En Route to a Standard QMA_1 vs. QCMA Oracle Separation

David Miloschewsky
Department of Computer Science, Stony Brook University, NY, USA

Supartha Podder
Department of Computer Science, Stony Brook University, NY, USA

Dorian Rudolph
Department of Computer Science and Institute for Photonic Quantum Systems (PhoQS), Paderborn University, Germany

Abstract

We study the power of quantum witnesses under perfect completeness. We construct a classical oracle relative to which a language lies in QMA_1 but not in QCMA when the QCMA verifier is only allowed polynomially many adaptive rounds and exponentially many parallel queries per round. Additionally, we derandomize the permutation-oracle separation of Fefferman and Kimmel, obtaining an in-place oracle separation between QMA_1 and QCMA. Furthermore, we focus on QCMA and QMA with an exponentially small gap, where we show a separation assuming the gap is fixed, but not when it may be arbitrarily small. Finally, we derive consequences for approximate ground-state preparation from sparse Hamiltonian oracle access, including a bounded adaptivity frustration-free variant.

2012 ACM Subject Classification Theory of computation → Quantum complexity theory

Keywords and phrases Quantum complexity theory, Quantum Merlin-Arthur (QMA)

Digital Object Identifier 10.4230/LIPIcs.MFCS.2026.32

Related Version *Full Version*: https://arxiv.org/abs/2604.26921

Funding *Dorian Rudolph*: Funded by DFG Priority Programme 2514 (grant number 563388236).

Acknowledgements We thank Srinivasan Arunachalam, Sevag Gharibian, Srijita Kundu, Sinan Oral, and Nengkun Yu for helpful discussions. This work was done in part while the authors were visiting the Simons Institute for the Theory of Computing.

1 Introduction

The complexity class QMA (Quantum Merlin-Arthur, a quantum analogue of NP) was formally introduced by Kitaev [28] as the class of languages for which a polynomial-time quantum verifier can be convinced to accept yes-instances with high probability using a polynomial-size quantum witness, while rejecting no-instances regardless of the witness supplied. A natural variant of QMA, introduced by Aharonov and Naveh [4], is QCMA, where the verifier is quantum but the witness is restricted to be classical.

It is immediate that $\mathsf{QCMA} \subseteq \mathsf{QMA}$. A central question in quantum complexity theory is whether this inclusion is strict, i.e., whether quantum witnesses provide additional computational power over classical ones in the non-interactive setting. Despite significant effort, the status of this question in the unrelativized world remains open. Early intuition by Aharonov and Naveh [4] suggested that quantum witnesses might not be inherently more powerful, for instance, if ground states of local Hamiltonians were to admit efficient classical descriptions, then $\mathsf{QMA} = \mathsf{QCMA}$.

Considerable progress has been made in understanding this question in standard and relativized worlds. Watrous [48] showed that the Group Non-Membership problem separates QMA from MA with respect to an oracle and was one of the first candidates for understanding the power of classical and quantum witnesses [3, 20]. Aaronson and Kuperberg [3] gave the first separation between QMA and QCMA, albeit relative to a quantum oracle. Fefferman and Kimmel [17] later obtained separations using randomized in-place permutation oracles, and several subsequent works proposed alternative oracle constructions and candidate problems aimed at clarifying the source of quantum advantage [36, 33, 39]. More recent efforts pursued separations in increasingly standard oracle models [34, 42, 8, 50, 35]. In parallel, a line of work has investigated this question through the lens of uncloneability [43, 14, 13, 15], structural properties of QMA and its variants [23, 16, 40], as well as in communication complexity [45, 30, 29]. The longstanding question of whether QMA and QCMA can be separated relative to a standard classical oracle was ultimately resolved by [10, 11].

Thus a classical counterpart of the result of Aaronson and Kuperberg [3] was finally found. However, as noted by [10] (and also not achieved by [11]), neither of these classical oracle separations achieve perfect completeness. In contrast, [3] actually separates the class QMA$_1$ from QCMA with respect to a quantum oracle.

QMA with perfect completeness

QMA$_1$ is the variant of QMA in which the verifier must accept every YES instance with probability *exactly* 1 (while still accepting NO instances with probability at most 1/2). The class was formalized in [27] and gained prominence through the QMA$_1$-completeness of Quantum k-SAT [12, 22]. Whether QMA = QMA$_1$ remains open; Aaronson [2] gave a quantum oracle separation, and the answer is known to depend delicately on the verifier's gate set. Amplification and completeness techniques for one-sided-error QMA have been developed in [41, 31]. In contrast, the classical-witness analogue satisfies QCMA = QCMA$_1$ under standard gate sets [32]. This leaves open the following natural question.

▶ **Question 1.** *Is there a* standard classical *oracle separation between* QMA$_1$ *and* QCMA*?*

As our first result, we answer a bounded adaptivity analog of Question 1.

▶ **Result 2** (Theorem 25)**.** *For every polynomial R, there exists a classical oracle relative to which* QMA$_1 \not\subseteq$ QCMA*, assuming the* QCMA *verifier is restricted to R rounds of adaptive queries. Additionally, the language is in* coRP *with $R+1$ adaptive one-query rounds.*

By bounded adaptivity, we mean that the oracle calls are grouped into rounds. Each round of queries is performed in parallel and may only depend on the results of previous queries. Therefore, the restriction is on the depth of the oracle dependence, not on the total number of queries. In Result 2, the QCMA lower bound applies even when each round makes exponentially many queries. The regime described above is the same as in [8], who separated QCMA from QMA (but not QMA$_1$) with $o(\log n/\log\log n)$ adaptive rounds. In contrast, Theorem 25 separates QMA$_1$ from QCMA bounded to R rounds, where R is any fixed polynomial. On the other hand, the bounded round restriction is necessary in our problem as a coRP algorithm solves the problem with $R+1$ rounds, while the problem in [8] was used by [11] for the classical oracle separation.

In-place oracle separation

As discussed before, in the permutation oracle model, Fefferman and Kimmel [17] separated QMA from QCMA using *randomized* in-place permutation oracles. Despite the extensive line of work on the QMA versus QCMA question that followed [34, 42, 8, 50, 35, 10, 11],

derandomizing the [17] construction has remained elusive, and none of these works achieve perfect completeness in the in-place model. Furthermore, the in-place oracle model has been studied in other contexts as well [1, 26, 7, 25]. This motivates the following natural question.

▶ **Question 3.** *Can randomization be removed from the in-place oracle separation of Fefferman and Kimmel [17], and can the separation be strengthened to* QMA_1 *versus* QCMA*?*

We answer both parts affirmatively.

▶ **Result 4** (Theorem 22). *There exists a deterministic in-place permutation oracle relative to which* $\mathsf{QMA}_1 \not\subseteq \mathsf{QCMA}$*, even when the* QCMA *verifier is allowed* $2^{o(n)}$ *rounds of adaptivity and exponentially many queries per round.*

Viewed as a query problem, Result 4 is a set-preimage sampling lower bound. Formally defined in Problem 15, the problem is to estimate the parity bias of the preimage set $S_b = \pi^{-1}([N])$ where π is the given permutation. The QMA_1 witness is simply $|S_b\rangle$. Without a witness, one may sample S_b by drawing some $j \in [N]$ and applying π for $b-1$ steps. This differs from the standard permutation inversion problem, where given some y, one must find $\pi^{-1}(y)$, which has query complexity $\Theta(\sqrt{N})$ both in the standard XOR and in-place oracle models [24, 9, 17, 25]. Thus Result 4 shows that even when given a *classical witness*, the simple $b-1$ round sampling algorithm is optimal.

Witness verification with an exponentially small gap

A natural question in the study of verification classes with error is how they behave under various completeness-soundness gaps. For QMA and QCMA, standard error-reduction [37] shows that any inverse-polynomial gap can be amplified to a constant, meaning the specific choice of parameters is irrelevant. However, when the gap is allowed to shrink to $2^{-\mathrm{poly}(n)}$, no error-reduction techniques are known. The resulting classes $\mathsf{PreciseQMA}$ and $\mathsf{PreciseQCMA}$ have been characterized as PSPACE [18] and $\mathsf{NP}^{\mathsf{PP}}$ [38, 21], respectively.

▶ **Question 5.** *Is there a classical oracle separating* QMA *from* QCMA *when the completeness-soundness gap is exponentially small?*

We partially answer this question. Specifically, by tweaking the original proof technique of [11], we show that when the gap is fixed to $O(2^{-n})$, the classes may be separated. However, $\mathsf{PreciseQCMA}$, which considers the union over all $2^{-\mathrm{poly}(n)}$ gaps, solves the problem.

▶ **Result 6** (Theorem 31). *There exists a classical oracle relative to which a problem lies in* $\mathsf{QMA}(2^{-n})$ *and* $\mathsf{PreciseQCMA}$*, but not in* $\mathsf{QCMA}(2^{-n})$*.*

The $\mathsf{PreciseQCMA}$ inclusion holds due to the fact that the problem is in Π_2^{P}, which is in $\mathsf{NP}^{\mathsf{PP}}$ due to Toda's theorem [47]. In particular, this provides evidence against an efficient gap amplification procedure for $\mathsf{PreciseQMA}$ and $\mathsf{PreciseQCMA}$.

Circuit complexity of sparse Hamiltonian ground states

The No Low-Energy Trivial States (NLTS) theorem of Anshu, Breuckmann, and Nirkhe [5], resolving a conjecture of Freedman and Hastings [19], establishes that there exist families of local Hamiltonians whose low-energy states cannot be prepared by constant-depth quantum circuits. In an oracle setting, one can ask whether sparse Hamiltonians given via Hamiltonian query access O_H^{rc} have approximate ground states that provably require large circuits to prepare.

▶ **Question 7.** *Are there families of sparse Hamiltonians, given via oracle access, whose approximate ground states provably require large circuits to prepare?*

A natural question in a similar spirit is whether the oracle separations between QMA and QCMA yield circuit complexity lower bounds for ground states of sparse Hamiltonians given via Hamiltonian query access O_H^{rc}. To the best of our knowledge, this connection has not been made explicitly in prior work, although it follows relatively directly from applying the circuit-to-Hamiltonian construction [27] to the QMA verifiers in [10, 11].

▶ **Result 8** (Theorem 32)**.** *There exists a family of $O(1)$-sparse Hamiltonians $\{H_i\}$ on n_i qubits such that any state preparable by a circuit of size $2^{o(n_i^{1/3}/\log n_i)}$ which has access to H via the oracle $O_{H_i}^{\mathrm{rc}}$ has energy at least $\lambda_0(H_i) + 1/\mathrm{poly}(n_i)$.*

Furthermore, using Result 2, we are able to extend this to frustration-free Hamiltonians, except the circuit is restricted in adaptivity (see Theorem 33). Note that extending this without the restriction would resolve Question 1.

Techniques

The problem used to obtain Result 4 is a pointer-chasing permutation oracle instance. The permutation consists of disjoint chains through buckets $I_1, \ldots I_b$ with the first bucket being $[N]$ and the last bucket mapping to $[N]$. The problem is to decide whether parity of the items in I_b which map to $[N]$ is 0 or 1, given the promise that it is either 0 in all items, or only over half of them (for a formal definition, see Problem 15). In a YES instance, the QMA$_1$ witness is the uniform state on $S_b = \pi^{-1}([N])$, which is used to test the parity of S_b and whether it maps back to $[N]$, both of which are checked with perfect completeness.

The QCMA lower bound is as follows. Given a fixed verifier and classical witness, we record a transcript $\mathcal{T}^{(r)}$ of all the points of the oracle which the algorithm "knows" after r adaptive rounds of queries. Each round, $\mathcal{T}^{(r)}$ may only add points by either querying them with heavy weight or from the previous step in the chain. We describe a canonical permutation π' based on $\mathcal{T}^{(r)}$ and show that the verifier's state using π is close to that with π'. Assuming $\mathcal{T}^{(r)}$ satisfies several conditions which we call "good", which occurs with high probability, each YES instance may be transformed into a NO instance with the same canonical permutation by altering the last bucket I_b. A union bound over witnesses and diagonalization finishes the lower bound.

Result 2 uses the tools developed above. First, the QCMA lower bound applies using the standard XOR oracle. Second, the QMA$_1$ algorithm is obtained by considering the algorithm which uses $R + 1$ rounds of queries and parallelizing it using the Feynman-Kitaev history state. As we show, any R-round QMA (and QMA$_1$) algorithm may be parallelized to a single-round verifier with $O(R^4)$ parallel oracle queries.

We note that the oracle separations underlying Results 2 and 4 were developed independently of the two recent classical-oracle separations between QMA and QCMA [10, 11]. On the other hand, the results in Section 3.3 directly use the machinery developed in [11]. In Result 6, we solely modify the bias parameter. Furthermore, Result 8 is obtained by applying the circuit-to-Hamiltonian construction [27] to the QMA verifier in [11] and using sparse-Hamiltonian energy estimation. In the frustration-free case, we use the QMA$_1$ verifier for Problem 15.

2 Preliminaries

We assume the reader is familiar with standard quantum computing and complexity theory background. For introductions, see [44, 6]. We use the following notation. We use $[a]$ to denote the set $\{1, \dots a\}$ and $[a, b]$ to denote $\{a, a+1, \dots, b\}$. Given a set of integers S, let S^{even} and S^{odd} denote the subset of S which only contains its even or odd elements, respectively. For any finite non-empty set S, we let

$$|S\rangle = \frac{1}{\sqrt{|S|}} \sum_{s \in S} |s\rangle .$$

Given a matrix H, we let $\lambda_0(H)$ denote the smallest eigenvalue of H. Let us describe the oracle models we will use. For a string $x \in \{0,1\}^n$, the standard XOR oracle is,

$$O_x |i, b\rangle \coloneqq |i, b \oplus x_i\rangle ,$$

where $i \in [n]$ and $b \in \{0,1\}$. We call this a *classical oracle* as, when x represents a function $f : \{0,1\}^{\log n} \to \{0,1\}$, O_x is the associated unitary applied. A *forward in-place oracle* for a permutation π is the oracle O_π defined as,

$$O_\pi |x\rangle = |\pi(x)\rangle .$$

We emphasize that we do not provide access to the inverse of O_π. Lastly, we will use the Hamiltonian query model. We say a Hamiltonian H is *d-sparse* if for each row, there are at most d non-zero terms, while $H = \sum_i H_i$ is *frustration-free* if $H_i \succeq 0$ and $\lambda_0(H) = 0$. Consider a d-sparse Hamiltonian $H \in \mathbb{C}^{M \times M}$. Let $i, j \in [M]$, $k \in [d]$ and $f(i,k)$ be the kth column index of a non-zero term in row i of H. The O_H and O_f oracles are defined as,

$$\begin{aligned} O_H |i, j, z\rangle &\coloneqq |i, j, z \oplus H_{i,j}\rangle \\ O_f |i, k\rangle &\coloneqq |i, f(i,k)\rangle . \end{aligned}$$

We call the pair O_H and O_f the row-column oracle gates O_H^{rc}.

An algorithm A with R adaptive rounds of q queries to an arbitrary oracle O is a sequence of unitaries $A = (U_0, U_1, \dots, U_R)$ interlaced with parallel calls to O. On some input $|\psi\rangle$ it behaves as,

$$A |\psi\rangle \coloneqq U_R O^{\otimes q} U_{R-1} O^{\otimes q} \dots U_1 O^{\otimes q} U_0 .$$

2.1 Complexity Classes

▶ **Definition 9** (Variants of BQP). *A language $L \subseteq \{0,1\}^*$ is in $\mathsf{BQP}(c,s)$ where $c \geq s$ if there exists a uniform polynomial-time family of quantum circuits $Q = \{Q_n\}$ such that,*

$$\begin{aligned} x \in L &\implies \Pr[Q(x) = 1] \geq c \\ x \notin L &\implies \Pr[Q(x) = 1] \leq s. \end{aligned}$$

We define $\mathsf{BQP} = \mathsf{BQP}(\frac{2}{3}, \frac{1}{3})$, $\mathsf{RQP} = \mathsf{BQP}(\frac{1}{2}, 0)$ *and* $\mathsf{ZQP} = \mathsf{RQP} \cap \mathsf{coRQP}$.

Equivalently, ZQP is the class of zero-error quantum algorithms which may output $1, 0$ or "maybe", where the probability of "maybe" is at most $\frac{1}{2}$ and the algorithm never answers incorrectly. Lastly, RP is defined analogously to RQP, with the quantum circuit replaced by a probabilistic Turing machine.

▶ **Definition 10** (Witness classes). *A language $L \subseteq \{0,1\}^*$ is in $\mathsf{QMA}(c,s)$ where $c \geq s$ if there exist a uniform polynomial-time quantum verifier V and a polynomial p such that for every $x \in \{0,1\}^*$,*

$$x \in L \implies \exists\, |\psi\rangle \in (\mathbb{C}^2)^{\otimes p(|x|)} \colon \Pr\left[V(x,|\psi\rangle) = 1\right] \geq c$$
$$x \notin L \implies \forall\, |\psi\rangle \in (\mathbb{C}^2)^{\otimes p(|x|)} \colon \Pr\left[V(x,|\psi\rangle) = 1\right] \leq s.$$

$\mathsf{QCMA}(c,s)$ is the restriction of $\mathsf{QMA}(c,s)$ in which the witness is a classical string $y \in \{0,1\}^{p(|x|)}$. We define the following classes,

$$\mathsf{QMA} = \bigcup_{c-s \geq \frac{1}{\mathrm{poly}(n)}} \mathsf{QMA}(c,s),$$
$$\mathsf{QCMA} = \bigcup_{c-s \geq \frac{1}{\mathrm{poly}(n)}} \mathsf{QCMA}(c,s),$$
$$\mathsf{QMA}_1 = \bigcup_{s \leq 1-\frac{1}{\mathrm{poly}(n)}} \mathsf{QMA}(1,s),$$
$$\mathsf{PreciseQMA} = \bigcup_{c-s \geq 2^{-\mathrm{poly}(n)}} \mathsf{QMA}(c,s),$$
$$\mathsf{PreciseQCMA} = \bigcup_{c-s \geq 2^{-\mathrm{poly}(n)}} \mathsf{QCMA}(c,s),$$

where the parameters c, s are functions of the input length.

By standard completion and soundness gap amplification techniques [37], $\mathsf{QMA} = \mathsf{QMA}(\frac{2}{3}, \frac{1}{3})$, $\mathsf{QCMA} = \mathsf{QCMA}(\frac{2}{3}, \frac{1}{3})$ and $\mathsf{QMA}_1 = \mathsf{QMA}(1, \frac{1}{2})$. However, the same techniques are not known to apply to $\mathsf{PreciseQMA}$ and $\mathsf{PreciseQCMA}$.

▶ **Definition 11** (Bounded adaptivity oracle classes). *Let $O = \{O_n\}_n$ be a family of oracles and $R, q \colon \mathbb{N} \to \mathbb{N}$ be query bounds. A language $L \subseteq \{0,1\}^*$ is in $\mathsf{QMA}^O[R,q]$ if there exist a uniform quantum verifier V and a polynomial p such that V makes at most $R(|x|)$ adaptive rounds of $q(|x|)$ parallel queries to O and for every $x \in \{0,1\}^*$,*

$$x \in L \implies \exists\, |\psi\rangle \in (\mathbb{C}^2)^{\otimes p(|x|)} \colon \Pr\left[V^O(x,|\psi\rangle) = 1\right] \geq \frac{2}{3},$$
$$x \notin L \implies \forall\, |\psi\rangle \in (\mathbb{C}^2)^{\otimes p(|x|)} \colon \Pr\left[V^O(x,|\psi\rangle) = 1\right] \leq \frac{1}{3}.$$

The classes $\mathsf{QCMA}^O[R,q]$ and ${\mathsf{QMA}_1}^O[R,q]$ are defined analogously.

▶ **Definition 12** (Advice classes). *A language $L \subseteq \{0,1\}^*$ is in $\mathsf{BQP}_{/\mathsf{qpoly}}$ if there is a polynomial-time family of quantum circuits $Q = \{Q_n\}$, a polynomial $p(n)$ and a family of quantum states $\{|\psi_n\rangle \in (\mathbb{C}^2)^{\otimes p(n)}\}$ such that,*

$$x \in L \implies \Pr\left[Q(x, |\psi_{|x|}\rangle) = 1\right] \geq \frac{2}{3},$$
$$x \notin L \implies \Pr\left[Q(x, |\psi_{|x|}\rangle) = 1\right] \leq \frac{1}{3}.$$

$\mathsf{BQP}_{/\mathsf{poly}}$ is defined analogously, except the advice states $|\psi_n\rangle$ are replaced by classical strings $y \in \{0,1\}^{p(n)}$. Similarly, $\mathsf{ZQP}_{/\mathsf{qpoly}}$ is defined as $\mathsf{BQP}_{/\mathsf{qpoly}}$ with the zero-error semantics of ZQP.

2.2 Tools

We will use a parallel-query hybrid method [9].

▶ **Lemma 13** (Parallel-query hybrid method). *Let π, π' be permutations over $[M]$, $|\phi\rangle$ an arbitrary state over q query registers, Π be projector $\Pi \coloneqq \sum_{x:\pi(x)\neq\pi'(x)} |x\rangle\langle x|$ and Π_j be Π over the query register $j \in [q]$. Furthermore, define $p_j = \langle\phi| \Pi_j |\phi\rangle$. Then,*

$$\left\| \left(O_\pi^{\otimes q} - O_{\pi'}^{\otimes q}\right) |\phi\rangle \right\| \leq 2\sqrt{\sum_{j\in[q]} p_j}.$$

▶ **Lemma 14.** *Let U be a finite set such that $|U| = B$ and let $S \subset U$ be uniformly random subset of size N. Letting μ be an arbitrary distribution on U and $H = \{x \in U : \mu(x) \geq \epsilon/N\}$,*

$$\Pr_{S\sim\text{unif}}[|S \cap H| \geq \delta N] \leq \left(\frac{eN}{\delta\epsilon B}\right)^{\delta N}. \tag{1}$$

3 Results

Let us formally list the results of the paper.

3.1 In-place oracle separation via pointer-chasing

Let us begin by fixing multiple variables we will use throughout the section. Fix some constants $l \geq 4$ and $\alpha \in (0, \frac{1}{2})$. For any $n \in \mathbb{N}$, let $N \coloneqq 2^n$, $M \coloneqq 2^{ln}$, $b = \lceil 2^{\alpha n} \rceil$ and $B \coloneqq 2\lfloor \frac{M-N}{2(b-1)} \rfloor$.[1] Lastly, for $i \in [b]$, define the buckets I_i as,

$$I_i = \begin{cases} [N] & \text{if } i = 1 \\ [N + (i-2)B + 1, N + (i-1)B] & \text{if } i \geq 2. \end{cases}$$

Therefore, for $i \geq 2, |I_i| = B$. Lastly, $I_{\text{junk}} = [M] \setminus \bigcup_i I_i$. Let us define the problem we will analyze.

▶ **Problem 15** (Permutation pointer-chasing). *For $i \in [b]$, let $S_i \subseteq [M]$ be a set such that $|S_i| = N$ and $S_i \subseteq I_i$, and $f_i : [N] \to S_i$ be a bijection. Let us fix the permutation $\pi : [M] \to [M]$, defined as,*

$$\pi(x) = \begin{cases} f_{i+1}(j) & \text{if } x = f_i(j) \text{ for } j \in [N], i \in [b-1] \\ j & \text{if } x = f_b(j) \text{ for } j \in [N] \\ x & \text{if } x \notin \bigcup_i S_i. \end{cases} \tag{2}$$

The problem is to decide whether (YES) $|S_b^{\text{even}}| = N$ or (NO) $|S_b^{\text{even}}| \leq \frac{N}{2}$.

Let us show that the problem is in QMA_1.

▶ **Lemma 16** (QMA_1 algorithm). *For any in-place oracle $\Pi = \{\pi_n\}_n$ where π_n are instances of Problem 15, the language $L \coloneqq \{1^n : \pi_n \text{ is a YES instance}\}$ is in $\mathsf{QMA}_1^{\Pi}[1, 1]$.*

Next, we show a QCMA lower bound on the problem.

[1] Although all the variables are functions in terms of n, we omit writing the input n.

▶ **Lemma 17** (QCMA lower bound). *Fix $l \geq 4$, $\alpha \in (0, \frac{1}{2})$, and $\beta \geq 0$ such that,*

$$\beta + 5\alpha < l - 2. \tag{3}$$

There exists an in-place oracle $\Pi = \{\pi_n\}_n$ such that the language $L \coloneqq \{1^n : \pi_n$ is a YES instance$\}$ is not in $\mathsf{QCMA}^{\Pi}[b(n) - 2, q(n)]$ where $q(n) \leq 2^{\beta n}$.

Proof. Let us fix some instance n. We first fix an in-place algorithm V which takes in some witness $v \in \{0,1\}^{w(n)}$ and makes $R \coloneqq b - 2$ rounds of q parallel queries per round. Let $|\psi_0\rangle = |0\rangle |v\rangle$ be the initial state and for any permutation σ and $r \in [R]$, let $|\psi_r^\sigma\rangle$ denote the state right before the $r+1$ query,

$$|\psi_r^\sigma\rangle \coloneqq U_r O_\sigma^{\otimes q} \dots O_\sigma^{\otimes q} U_0 |\psi_0\rangle .$$

The distribution D_n^{YES} over YES instances of PC_n is defined as follows. First, set $S_1 = [N]$ and $f_1(j) = j$. For $i \in [2, b-1]$, draw S_i uniformly from $\binom{I_i}{N}$ and f_i be a uniformly-random bijection. Last, S_b is uniformly-drawn from $\binom{I_b^{\mathrm{even}}}{N}$ and f_b is uniformly-random. Given a fixed element from D_n^{YES}, we may define π_n using Equation (2).

Next, we define the *transcript* and its *canonical completion*. For each round $r \in [R]$, the transcript $\mathcal{T}^{(r)}$ tracks the known and unknown parts of each set S_i of an oracle. It consists of the following parts:

(a) *Discovered* sets $D_i^{(r)} \subseteq S_i$,
(b) *Commited* sets $Q_i^{(r)} \subseteq S_i$ and their associated commited values $\pi(x)$ for all $x \in Q_i^{(r)}$,
(c) *Frontier* sets $F_i^{(r)} \coloneqq D_i^{(r)} \setminus Q_i^{(r)}$,
(d) *Unexplored* sets $U_i^{(r)} \subseteq I_i \setminus D_i^{(r)}$,
(e) *Excluded* sets $E_i^{(r)} \coloneqq I_i \setminus (U_i^{(r)} \cup D_i^{(r)})$.

We initialize $\mathcal{T}^{(0)}$ as follows,

$$D_1^{(0)} = F_1^{(0)} = [N] \qquad U_1^{(0)} = Q_1^{(0)} = E_1^{(0)} = \emptyset,$$
$$\forall i \geq 2,\ U_i^{(0)} = I_i \qquad D_i^{(0)} = Q_i^{(0)} = E_i^{(0)} = F_i^{(r)} = \emptyset.$$

Notice that we may use $\mathcal{T}^{(r)}$ to partition I_i as follows,

$$I_i = Q_i^{(r)} \sqcup F_i^{(r)} \sqcup U_i^{(r)} \sqcup E_i^{(r)}. \tag{4}$$

Assuming $\left|\bigcup_i F_i^{(r)}\right| = \left|[N] \setminus \pi(Q_b^{(r)})\right|$, we define the root function $f^{(r)}(x) : \bigcup_i F_i^{(r)} \to [N] \setminus \pi(Q_b^{(r)})$ to be the first bijection from an enumerated list of functions. The *canonical completion* $\tilde{\pi}_r$ is defined as,

$$\tilde{\pi}_r(x) \coloneqq \begin{cases} \pi(x) & \text{if } x \in \bigcup_i Q_i^{(r)}, \\ f^{(r)}(x) & \text{if } x \in \bigcup_i F_i^{(r)}, \\ x & \text{if } x \in I_{\mathrm{junk}} \cup \bigcup_i E_i^{(r)} \cup \bigcup_i U_i^{(r)}. \end{cases} \tag{5}$$

Intuitively, each point $x \in \bigcup_i F_i^{(r)}$ is at the end of a known chain from $[N]$. Using $f^{(r)}$, we ensure that $\tilde{\pi}_r(x)$ is a permutation.

▷ Claim 18. Assume that for a $\mathcal{T}^{(r)}$ based on permutation π and for all $x \in \bigcup_i F_i^{(r)}$, there exists some sequence of points $x_0, \dots x_{i-1}, x$ such that for all $t \in [i-1]$, $x_t \in Q_t^{(r)}$. Then,

1. there exists a bijection $f^{(r)}(x) : \bigcup_i F_i^{(r)} \to [N] \setminus \pi(Q_b^{(r)})$,
2. $\tilde{\pi}_r$ is a permutation and,
3. for all $x \in [M]$, $\pi(x) = x \implies \tilde{\pi}_r(x) = x$.

Proof. Based on Equation (5), partition $[M] = A \sqcup B \sqcup C$ where $A \coloneqq \bigcup_i Q_i^{(r)}$, $B \coloneqq \bigcup_i F_i^{(r)}$, and $C \coloneqq I_{\text{junk}} \cup \bigcup_i E_i^{(r)} \cup \bigcup_i U_i^{(r)}$.

Due to the assumption on $x \in \bigcup_i F_i^{(r)}$, we have that $x \in \bigcup_i F_i^{(r)}$ if and only if for all $z \in [b-i]$, $\pi^z(x) \in U_i^{(i+z)}$.[2] As the number of such points is $\left|[N] \setminus \pi(Q_b^{(r)})\right|$, Item 1 follows.

Let us show Item 2. As elements in C are mapped to themselves in $\tilde{\pi}_r$, it suffices to show that $\tilde{\pi}_r|_{A\cup B}$ is a bijection on $A \cup B$. By definition of A, the only points $x \in A$ for which there does not exist a $y \in A$ such that $x = \tilde{\pi}_r(y) \in A$ are in $[N] \setminus \pi(Q_b^{(r)})$. Similarly, all points in $x \in A$ such that $\tilde{\pi}_r(x) \notin A$ are in $\bigcup_i F_i^{(r)}$. Per Item 1 combined with the fact that π is a permutation, $\tilde{\pi}_r|_{A\cup B}$ is a permutation.

By Equation (2), $\pi(x) = x$ implies that $x \notin \bigcup_i S_i$, so $x \notin \bigcup_i D_i^{(r)} = A \cup B$. Therefore, $x \in C$, proving Item 3. ◁

The canonical state $|\psi'_r\rangle$ is defined to be,

$$|\psi'_r\rangle = U_r O_{\tilde{\pi}_r}^{\otimes q} U_{r-1} O_{\tilde{\pi}_{r-1}}^{\otimes q} \dots O_{\tilde{\pi}_1}^{\otimes q} U_0 |\psi_0\rangle ,$$

which depends on the transcripts $\mathcal{T}^{(i)}$ for $i \in [r]$. We say that a permutation σ is *consistent* with $\mathcal{T}^{(r)}$ if $\mathcal{T}^{(r)}$ is its transcript after r rounds under a verifier V. Furthermore, we define heavy sets, the sets which have a large weight in the query registers of $|\psi_r^\pi\rangle$ (i.e. right before the oracle call $O_\pi^{\otimes q}$). Formally, let $r \in [R]$, $i \in [b]$ and $j \in [q]$ be some variables. Letting X_j denote the j-th query register and $\Pi_S^{(j)} \coloneqq \mathbf{I}^{\otimes(j-1)} \otimes \left(\sum_{x\in S} |x\rangle\langle x|\right) \otimes \mathbf{I}^{\otimes(q-j)}$ the projector onto $S \subseteq [M]$ acting on the j-th query register, consider the following variables,

$$\begin{aligned} p_{i,j}^{(r)} &\coloneqq \langle \psi'_{r-1} | \, \Pi_{I_i}^{(j)} \, |\psi'_{r-1}\rangle \\ p_i^{(r)} &\coloneqq \sum_{j\in[q]} p_{i,j}^{(r)} \\ \mu_i^{(r)}(S) &\coloneqq \frac{1}{p_i^{(r)}} \sum_{j\in[q]} \langle \psi'_{r-1} | \, \Pi_S^{(j)} \, |\psi'_{r-1}\rangle \qquad (S \subseteq I_i). \end{aligned}$$

Note that when $p_i^{(r)} = 0$, we let $\mu_i^{(r)}(S) = 0$. The *heavy* set $H_i^{(r)}$ is defined as,

$$H_i^{(r)} \coloneqq \left\{ x \in I_i : \mu_i^{(r)}(\{x\}) \geq \frac{\epsilon}{N} \right\},$$

where ϵ is a variable we will set later. Next, let us define how the transcript is *updated* each round. For $r \geq 1$, let the undiscovered part of S_i be $S_i^{(r)} \coloneqq S_i \cap U_i^{(r-1)}$ and the heavy hits be $G_i^{(r)} \coloneqq H_i^{(r)} \cap S_i^{(r)}$.

For each $g \in G_i^{(r)}$, let $\text{chain}(g)$ denote the following maximal sequence,

$$\text{chain}(g) = g, g^{-1}, \dots, g^{-k} : \forall m \in [k-1] : \pi^{-1}(g^{-m}) = g^{-(m+1)} \text{ and } g^{-k} \in S_1.$$

Essentially, $\text{chain}(g)$ represents the sequence of steps of π which bring us from g back to S_1. The *path points* at level i are elements of $\text{chain}(g)$ lying in I_i that have not yet been committed,

$$P_i^{(r)} \coloneqq \left\{ z : \exists\, k > i, \exists\, g \in G_k^{(r)} \text{ s.t. } z \in \text{chain}(g) \cap I_i \right\}.$$

[2] By $\pi^z(x)$, we mean applying the permutation on input x z-times.

We commit these path points to the transcript in order to ensure that we may define a valid root function $f^{(r)}$ and completion $\tilde{\pi}_r$ in Equation (5). For $i \geq 2$ and going from round $r-1$ to r, the transcript is updated as follows,

$$Q_i^{(r)} \coloneqq Q_i^{(r-1)} \cup D_i^{(r-1)} \cup G_i^{(r)} \cup P_i^{(r)} \tag{6}$$

$$D_i^{(r)} \coloneqq D_i^{(r-1)} \cup G_i^{(r)} \cup P_i^{(r)} \cup \pi\big(Q_{i-1}^{(r)}\big) \tag{7}$$

$$U_i^{(r)} \coloneqq U_i^{(r-1)} \setminus \big(H_i^{(r)} \cup D_i^{(r)}\big). \tag{8}$$

Note that for $i = 1$ and $r > 0$, the committed set is $Q_1^{(r)} = [N]$. One may see that the condition in Claim 18 is satisfied for all r.

▷ Claim 19 (Transcript indistinguishability). For any pair of oracles π_1, π_2 consistent with the same transcript history $\mathcal{T}^{(t)}$ for $t \in [r]$,

$$\| |\psi_r^{\pi_1}\rangle - |\psi_r^{\pi_2}\rangle \| \leq 4r\sqrt{q\epsilon}.$$

Proof. To show the statement, it suffices to show that for any permutation σ consistent with $\mathcal{T}^{(r)}$,

$$\| |\psi_r^{\sigma}\rangle - |\psi_r'\rangle \| \leq 2r\sqrt{q\epsilon}, \tag{9}$$

as applying Equation (9) to π_1 and π_2 and using the triangle inequality gives the claim. We prove Equation (9) by induction on $t \in [0, r]$. The base case $t = 0$ is immediate since the witness and verifier are fixed. For the inductive step,

$$\begin{aligned} \| |\psi_t^{\sigma}\rangle - |\psi_t'\rangle \| &= \big\| O_{\sigma}^{\otimes q} \big|\psi_{t-1}^{\sigma}\big\rangle - O_{\tilde{\pi}_t}^{\otimes q} \big|\psi_{t-1}'\big\rangle \big\| \\ &\leq \big\| \big|\psi_{t-1}^{\sigma}\big\rangle - \big|\psi_{t-1}'\big\rangle \big\| + \big\| (O_{\sigma}^{\otimes q} - O_{\tilde{\pi}_t}^{\otimes q}) \big|\psi_{t-1}'\big\rangle \big\| \\ &\leq 2(t-1)\sqrt{q\epsilon} + \big\| (O_{\sigma}^{\otimes q} - O_{\tilde{\pi}_t}^{\otimes q}) \big|\psi_{t-1}'\big\rangle \big\|, \end{aligned} \tag{10}$$

where the equality follows due to unitarity of U_t and the inequality is an application of the triangle inequality and inserting $O_{\sigma}^{\otimes q} \big|\psi_{t-1}'\big\rangle$.

We claim that σ and $\tilde{\pi}_t$ may disagree only on $\bigcup_i (S_i^{(t)} \setminus H_i^{(t)})$. This can be shown case by case. First, if $x \in I_{\text{junk}}$, both oracles are the identity. Let us check each part of the partition of I_i in Equation (4),

1. If $x \in Q_i^{(t)}$, then by Equation (5) both σ and $\tilde{\pi}_t$ agree with $\pi(x)$.
2. If $x \in F_i^{(t)} = D_i^{(t)} \setminus Q_i^{(t)}$, then $x \in S_i^{(t)} \setminus H_i^{(t)}$. This is due to the fact that since $D_i^{(t)} \setminus Q_i^{(t)} \subseteq \pi(Q_{i-1}^{(t)}) \setminus Q_i^{(t)} \subseteq S_i \setminus D_i^{(t-1)}$, we have $x \in U_i^{(t-1)} \cap S_i = S_i^{(t)}$. Furthermore, $x \notin H_i^{(t)}$ as otherwise $x \in G_i^{(t)} \subseteq Q_i^{(t)}$, contradicting $x \in F_i^{(t)}$.
3. If $x \in U_i^{(t)}$, then σ and $\tilde{\pi}_t$ may only disagree on $U_i^{(t)} \cap S_i$ as all other points are self-loops. As $U_i^{(t)} \subseteq U_i^{(t-1)}$, $D_i^{(t)} \cap U_i^{(t)} = \emptyset$ and $G_i^{(t)} \subseteq D_i^{(t)}$, we have $U_i^{(t)} \cap S_i \subseteq S_i^{(t)} \setminus H_i^{(t)}$ (the $H_i^{(t)}$ elements in $U_i^{(t-1)}$ were added to $G_i^{(t)} \subseteq Q_i^{(t)} \subseteq D_i^{(t)}$, so they left $U_i^{(t)}$).
4. If $x \in E_i^{(t)}$, there is no disagreement as $\pi(x) = x = \tilde{\pi}_r(x)$.

In all cases, potential disagreement is contained in $S_i^{(t)} \setminus H_i^{(t)}$. Letting p_j be the probability that the j-th query register holds a value in $\bigcup_{i \in [b]} (S_i^{(t)} \setminus H_i^{(t)})$ and using the fact that each $x \notin H_i^{(t)}$ has $\mu_i^{(t)}(\{x\}) < \epsilon/N$,

$$\mu_i^{(t)}(S_i^{(t)} \setminus H_i^{(t)}) \leq \left|S_i^{(t)}\right| \cdot \frac{\epsilon}{N} \leq \epsilon,$$

we have that,

$$\sum_{j\in[q]} p_j = \sum_{i\in[b]} p_i^{(t)}\mu_i^{(t)}(S_i^{(t)} \setminus H_i^{(t)})$$
$$\leq \epsilon \sum_{i\in[b]} p_i^{(t)} \leq \epsilon q.$$

By Lemma 13, the second term of Equation (10) is bounded by $2\sqrt{q\epsilon}$, finishing the proof. ◁

Let $\delta \in (0,1]$ be a constant we fix later. We say a transcript $\mathcal{T}^{(r)}$ is *good* if,

$\forall i \in [r+2, b] : |D_i^{(r)}| \leq 4rb\delta N$

$\forall i \in [r+1, b] : |Q_i^{(r)}| \leq 4rb\delta N.$

If $\mathcal{T}^{(r)}$ does not satisfy the criteria above, we call it *bad*.

▷ Claim 20 (Probability of a bad transcript). Assume $4rb\delta \leq 1$ and $\left(\frac{1}{\epsilon} + 4b\delta\right) rN \leq \frac{B}{4}$. Then for a fixed verifier V and witness v,

$$\Pr_{\pi\sim D_n^{\text{YES}}}\left[\mathcal{T}^{(r)} \text{ is bad}\right] \leq rb\left(\frac{4eN}{\delta\epsilon B}\right)^{\delta N}. \tag{11}$$

Proof. We prove this by induction on $r \in [R]$. The base case holds as, except for $D_1^{(0)}$, $D_i^{(0)} = Q_i^{(0)} = \emptyset$. For the inductive step, assume that $\mathcal{T}^{(r-1)}$ is good and fix some $i \in [r+1, b]$. As $i \geq r+1 \geq (r-1)+2$, goodness of $\mathcal{T}^{(r-1)}$ and the condition $\left(\frac{1}{\epsilon} + 4b\delta\right)(r-1)N \leq B/4$ imply $\left|U_i^{(r-1)}\right| \geq \frac{3B}{4}$.

If $i \leq b-1$, then $S_i^{(r)} = S_i \cap U_i^{(r-1)}$ is a uniformly-random subset of $U_i^{(r-1)}$ of size $N - \left|D_i^{(r-1)}\right| \leq N$. For $i = b$, $S_b^{(r)}$ is uniform over $U_b^{(r-1)} \cap [M]^{\text{even}}$; since I_b has $\geq B/2$ even elements and at most $B/4$ total have been removed, $\left|U_b^{(r-1)} \cap [M]^{\text{even}}\right| \geq \frac{B}{4}$. In both cases, as $H_i^{(r)}$ is determined by $\mathcal{T}^{(r-1)}$ (as the verifier and witness are fixed), $S_i^{(r)}$ is stochastically dominated by a uniformly-chosen set of size N from a universe of size at least $\frac{B}{4}$. By Lemma 14,

$$\Pr\left[\left|G_i^{(r)}\right| \geq \delta N \mid \mathcal{T}^{(r-1)}\right] \leq \left(\frac{4eN}{\delta\epsilon B}\right)^{\delta N}. \tag{12}$$

Let E denote the event that for all $t \leq r$ and $i \geq t+1$, $\left|G_i^{(t)}\right| < \delta N$. Next, we show that if E occurs, then $\mathcal{T}^{(r)}$ is good. Let,

$$J^{(r)} \coloneqq \{j \in [N] : \exists t \leq r, k > t \text{ s.t. } f_k(j) \in G_k^{(t)}\},$$

denote the indices of *paths* which were guessed earlier than expected. Under the assumption on $\left|G_i^{(t)}\right|$, we have that $\left|J^{(r)}\right| \leq rb\delta N$. We claim that every point in $D_i^{(r)}$ with $i \geq r+2$ and $Q_i^{(r)}$ with $i \geq r+1$ has a label in $J^{(r)}$. We prove this by induction on r. The claim is immediate for $r = 0$. For the inductive step, consider $Q_i^{(r)}$ with $i \geq r+1$. By Equation (6),

$$Q_i^{(r)} \subseteq Q_i^{(r-1)} \cup D_i^{(r-1)} \cup G_i^{(r)} \cup P_i^{(r)}.$$

By the inductive hypothesis, the terms $Q_i^{(r-1)}$ and $D_i^{(r-1)}$ have labels in $J^{(r-1)} \subseteq J^{(r)}$. The terms $G_i^{(r)}$ have labels in $J^{(r)}$ as $i \geq r+1$, while a label j in $P_i^{(r)}$ implies that it is in some $G_k^{(r)}$ where $k > i$. By similar reasoning, we find the same for $D_i^{(r)}$. Therefore $\left|J^{(r)}\right|$ bounds the size of all $D_i^{(r)}$ and $Q_i^{(r)}$ we care about, meaning $\mathcal{T}^{(r)}$ is good.

All that remains is bounding the probability of event E. Applying Equation (12), union-bounding over b buckets with $i \geq r+1$ and applying the chain rule over r rounds,

$$\Pr_{\pi \sim D_n^{\mathrm{YES}}}\left[\mathcal{T}^{(r)} \text{ is bad}\right] \leq rb\left(\frac{4eN}{\delta\epsilon B}\right)^{\delta N}. \qquad \triangleleft$$

▷ Claim 21 (NO-instance transformation). Suppose that for all $r \in [R]$, $\mathcal{T}^{(r)}$ is good for $\pi \in \mathrm{supp}(D_n^{\mathrm{YES}})$ where $R = b-2$, $8Rb\delta \leq \frac{1}{4}$ and $(\frac{1}{\epsilon} + 4b\delta)RN \leq \frac{B}{4}$. Then there exists a NO instance π_{NO} of PC_n which is consistent with $\mathcal{T}^{(r)}$.

Proof. We may entirely describe the permutation π using $f_1, \ldots f_b$. Notice that by definition, B is always even. As $\pi \in \mathrm{supp}(D_n^{\mathrm{YES}})$, $f_b([N]) = S_b \subseteq I_b^{\mathrm{even}}$. Let J_{fix} denote the fixed points which certify that some $x \in S_b$ is even,

$$J_{\mathrm{fix}} \coloneqq \left\{j : f_{b-1}(j) \in Q_{b-1}^{(R)}\right\} \cup \left\{j : f_b(j) \in D_b^{(R)}\right\}.$$

As $\mathcal{T}^{(R)}$ is good, $|J_{\mathrm{fix}}| \leq 8Rb\delta N \leq \frac{N}{4}$. Let $F \coloneqq \{f_b(j) : j \in J_{\mathrm{fix}}\} \subseteq I_b^{\mathrm{even}}$. Per our assumption, elements leave U_b by entering D_b or H_b. Over R rounds, at most $\left|D_b^{(R)}\right| + \sum_{r\in[R]}\left|H_b^{(r)}\right| \leq 4Rb\delta N + RN/\epsilon \leq \left(\frac{1}{\epsilon} + 4b\delta\right)RN \leq \frac{B}{4}$ elements have been removed, so $\left|U_b^{(R)}\right| \geq \frac{3B}{4}$. Since B is even, I_b is an interval of size B with exactly $B/2$ even elements and $B/2$ odd elements. At most $B/4$ elements in total have been removed, so at most $B/4$ even (resp. odd) elements were removed. Hence $\left|U_b^{(R)} \cap I_b^{\mathrm{even}}\right| \geq \frac{B}{2} - \frac{B}{4} = \frac{B}{4}$ and similarly $\left|U_b^{(R)} \cap I_b^{\mathrm{odd}}\right| \geq \frac{B}{4}$. Note also $F \cap U_b^{(R)} = \emptyset$ since $F \subseteq D_b^{(R)}$.

Choose $O' \subseteq U_b^{(R)} \cap I_b^{\mathrm{odd}}$ and $E' \subseteq U_b^{(R)} \cap I_b^{\mathrm{even}}$ such that $|O'| = \frac{N}{2}$ and $|E'| = \frac{N}{2} - |F|$ (feasible since both sets have size $\geq B/4 \geq N$). Then we set $S_b^{\mathrm{NO}} \coloneqq F \cup E' \cup O'$, giving $\left|S_b^{\mathrm{NO}}\right| = N$ and $\left|(S_b^{\mathrm{NO}})^{\mathrm{odd}}\right| = N/2$.

Define $f_b^{\mathrm{NO}} : [N] \to S_b^{\mathrm{NO}}$ by $f_b^{\mathrm{NO}}(j) = f_b(j)$ for all $j \in J_{\mathrm{fix}}$ and bijectively assigning the remaining indices to $S_b^{\mathrm{NO}} \setminus F$ (feasible since $\left|S_b^{\mathrm{NO}} \setminus F\right| = N - |J_{\mathrm{fix}}|$). We define π_{NO} using $f_1, \ldots, f_{b-1}$ unchanged and replacing f_b with f_b^{NO}.

We claim that π_{NO} generates the identical transcript to π through every round $r \in [R]$. Since $f_1, \ldots, f_{b-1}$ are unchanged, the heavy-hit sets $G_i^{(r)}$ and path points $P_i^{(r)}$ for buckets $i \leq b-1$ are identical for π and π_{NO} at every round. For bucket b: every point of $U_b^{(R)}$ avoided $D_b^{(r)}$ and $H_b^{(r)}$ for all $r \leq R$ (otherwise it would have left U_b before round R). Since $E', O' \subseteq U_b^{(R)}$, replacing elements of S_b inside $U_b^{(R)}$ by other elements of $U_b^{(R)}$ cannot change any $G_b^{(r)}$ or $D_b^{(r)}$ for $r \leq R$. Moreover, for $j \in J_{\mathrm{fix}}$, we have $f_b^{\mathrm{NO}}(j) = f_b(j)$, preserving all committed values. It follows inductively on r that the entire transcript $\mathcal{T}^{(r)}$ is identical for π and π_{NO} for every $r \in [R]$. $\triangleleft$

With the claims above, we may finally set the parameters ϵ and δ,

$$\epsilon \coloneqq \frac{1}{10^4 qb^2}, \quad \delta \coloneqq \frac{1}{64b^2}.$$

With these assignments, the conditions of Claims 20 and 21 are satisfied. The first condition holds as $8Rb\delta \leq 8b^2 \cdot \frac{1}{64b^2} \leq \frac{1}{4}$. The second condition follows since $\left(\frac{1}{\epsilon} + 4b\delta\right) RN \leq 2 \cdot 10^4 qb^3 N$, so it suffices to show $2 \cdot 10^4 qb^3 N \leq \frac{B}{4}$. For large n, $B \geq \frac{M-N}{b-1} \geq \frac{M}{2b}$, so it suffices to show $16 \cdot 10^4\, qb^4 N \leq M$. Substituting $q \leq 2^{\beta n}$, $b \leq 2^{\alpha n+1}$, and $N = 2^n$,

$$16 \cdot 10^4 qb^4 N \leq 256 \cdot 10^4 \cdot 2^{(\beta+4\alpha+1)n}.$$

As $M = 2^{ln}$, this holds whenever $256 \cdot 10^4 \cdot 2^{(\beta+4\alpha+1)n} \leq 2^{ln}$, meaning for all n such that,

$$n \geq n_1 \coloneqq \left\lceil \frac{\log_2(256 \cdot 10^4)}{l - 1 - \beta - 4\alpha} \right\rceil, \tag{13}$$

which is finite since $l - 1 - \beta - 4\alpha > 0$ by Equation (3). Therefore, for all $n \geq n_1$, the conditions of the claims are satisfied. Furthermore, these variables mean that $4R\sqrt{q\epsilon}$ is always bounded by $\frac{1}{25}$. Lastly, we bound the bad transcript probability in Equation (11). The base is bounded by,

$$\begin{aligned} \frac{4eN}{\delta\epsilon B} &\leq 512e \cdot 10^4 \cdot \frac{qb^5 N}{M} \\ &\leq 512 \cdot 32 \cdot e \cdot 10^4 \cdot 2^{(\beta+5\alpha+1-l)n} \leq C \cdot 2^{-\lambda n}, \end{aligned}$$

where $C = 16384 \cdot e \cdot 10^4$ is a constant and $\lambda = l - 1 - \beta - 5\alpha$. By Equation (3), $\lambda > 1$. Therefore for $n \geq n_2 = \lceil (\log_2 C + 1)/\lambda \rceil$, the base is bounded by $\frac{1}{2}$. Therefore,

$$\Pr_{\pi \sim D_n^{\mathrm{YES}}} \left[\mathcal{T}^{(r)} \text{ is bad} \right] \leq rb \cdot 2^{-\delta N}. \tag{14}$$

Let us show argue for the QCMA hardness. Fix any QCMA verifier V with $R = b - 2$ rounds of q queries and a witness of size $w = \mathrm{poly}(n)$. By taking the union bound over Equation (14), we have that,

$$\Pr_{\pi \sim D_n^{\mathrm{YES}}} [\exists v \in \{0,1\}^w : \mathcal{T}_v^{(r)} \text{ is bad}] \leq 2^w \cdot Rb \cdot 2^{-\delta N},$$

where $\mathcal{T}_v^{(r)}$ denotes the transcript using verifier V and witness v. Let $w \leq c \cdot n^d$ for some constants c, d and notice that,

$$\delta N = \frac{N}{64b^2} \geq \frac{2^{(1-2\alpha)n}}{256}.$$

Therefore,

$$2^w \cdot Rb \cdot 2^{-\delta N} \leq 2^{2+2\alpha n + cn^d} \cdot 2^{-\frac{2^{(1-2\alpha)n}}{256}}. \tag{15}$$

We have that this quantity is strictly less than 1 for all n such that,

$$n > n_3 \coloneqq \frac{256(c + 2\alpha + 2)(d+1)!}{(1-2\alpha)^{d+1} (\ln 2)^{d+1}}.$$

Therefore, for all $n \geq \max(n_1, n_2, n_3)$, there exists a yes-instance $\pi^*_{\mathrm{YES}} \in \mathrm{supp}(D_n^{\mathrm{YES}})$ such that $\mathcal{T}_v^{(R)}$ is good for every witness v. However, by Claims 19 and 21, V cannot distinguish π^*_{YES} from a no-instance π^*_{NO} consistent with $\mathcal{T}^{(R)}$ of π^*_{YES} with probability above $\frac{1}{25}$. Therefore, the completeness condition is not satisfied for π^*_{YES}, or soundness for π^*_{NO}. Letting π^*_n being one of these, by standard diagonalization techniques, we may create the oracle family $\Pi = \{\pi^*_n\}$ such that $L \notin \mathsf{QCMA}^{\Pi}[b(n) - 2, q(n)]$. ◀

Combining the two results above, we obtain the following theorem.

▶ **Theorem 22** (In-place oracle separation between QCMA and QMA_1). *There exists an in-place oracle* Π *with respect to which,* $\mathsf{QMA}_1{}^{\Pi} \not\subseteq \mathsf{QCMA}^{\Pi}$.

3.2 Bounded adaptivity standard oracle separation

One may observe that the proof of Lemma 17 works using classical oracles.

▶ Remark 23. Define the oracle family $O = \{O_n\}$ as the family of instances of Problem 15 π_n where,

$$O_n |x, y\rangle \coloneqq |x, y \oplus \pi_n(x)\rangle \tag{16}$$

There exists an oracle O such that the language $L \coloneqq \{1^n : \pi_n \text{ is a YES instance}\}$ is not in $\mathsf{QCMA}^O[b(n) - 2, q(n)]$, where $b(n)$ and $q(n)$ are as in Lemma 17.

Next, we show that any QMA^O query protocol can be parallelized by using Kitaev's proof that the Local Hamiltonian problem is QMA-complete. [27].

▶ **Lemma 24.** *For any unitary O, $\mathsf{QMA}^O = \mathsf{QMA}^{\|O}$ and $\mathsf{QMA_1}^O = \mathsf{QMA_1}^{\|O}$. In terms of the number of rounds, $\mathsf{QMA}^O[R, 1] \subseteq \mathsf{QMA}^O[1, O(R^4)]$ and $\mathsf{QMA_1}^O[R, 1] \subseteq \mathsf{QMA_1}^O[1, O(R^4)]$.*

Therefore, we may obtain a bounded adaptivity oracle separation using Problem 15 with respect to classical oracles. We emphasize that the restriction is important as allowing even a single additional round of queries puts the problem into QCMA. Thus, even when $R(n) = n^k$, this is not an oracle separating $\mathsf{QMA_1}$ from unrestricted QCMA.

▶ **Theorem 25** (Lifting to unitary oracles)**.** *For any fixed $R \in \mathrm{poly}(n)$ and $q(n) \leq 2^{\beta n}$ where $\beta \geq 0$, there exists a unary language L and an oracle $O = \{O_n\}$ such that, $L \in \mathsf{coRP}^O[R, 1]$, $L \in \mathsf{QMA_1}^O[1, O(R^4)]$, but $L \notin \mathsf{QCMA}^O[R - 1, q(n)]$.*

3.3 Extensions of prior results

Below, we focus on extending the results of [11]. Let us first fix the key terminology. We will use λ as the input size. Fix q to be the smallest prime with $\lambda^5 < q \leq 2\lambda^5$ and set $C_\lambda \coloneqq \mathsf{Mult}_{s,\mathbb{F}_q,k}$ (an error-correcting code) with $k = \lambda^3$, $s = \lambda$, $\Sigma \coloneqq \mathbb{F}_q^s$. For a function $H : [q] \times \Sigma \to \{0, 1\}$. The relation $R_{C_\lambda, H}$ associated with the *code intersection problem* is,

$$R_{C_\lambda,H} \coloneqq \{(x, v) \in \{0, 1\}^q \times \Sigma^q : v \in C_\lambda,\ \forall j \in [q],\ H(j, v_j) = x_j\},$$

Based on [49], it was shown that there exists a state $|\mathsf{adv}_H\rangle$ and an algorithm BiasYZ which, given some input x, finds a v such that $(x, v) \in R_{C_\lambda,H}$ with high probability [11]. In their proof, the function H is drawn from a biased distribution, meaning that the random function drawn will output 1 with probability p^* as opposed to $\frac{1}{2}$.

We define the distribution $\mathsf{Bias}_{q,p,\Sigma}$ over functions H as the product of q distributions $\mathsf{Bias}_{p,\Sigma}$ over functions H_i from Σ to $\{0, 1\}$ where $\Pr[H_i(y) = 1] = p$. Let $\mathsf{Good} \subseteq \mathrm{supp}(\mathsf{Bias}_{q,p,\Sigma})$ be a subset which we define later.

3.3.1 Zero error advice separation

We first strengthen the advice separation result of [11]. As $\mathsf{ZQP} \subseteq \mathsf{BQP_1}$, this affirmatively answers a variant of Question 1 where the witness is replaced with advice.

▶ **Theorem 26** (Extension of Theorem 7.5 in [11])**.** *There exists a classical oracle O such that $\mathsf{ZQP}^O_{/\mathsf{qpoly}} \not\subseteq \mathsf{BQP}^O_{/\mathsf{poly}}$.*

3.3.2 Precise verification

The oracle separation of [11] gives a separation between classes which have a constant completeness and soundness gap. We show that their argument extends to the setting where the gap is $2^{-\mathrm{poly}(n)}$ when this gap is fixed. The proof is the same, except we make a slight modification to the bias parameter p^*. The result uses the following problem.

▶ **Problem 27** (Code Intersection Subset Size CISS_σ)**.** *Let $H \in \mathsf{Good}$ be a random function, $\sigma : \mathbb{N} \to \mathbb{N}$ a function and $E \subseteq \{0,1\}^\lambda$. Given access to the following oracle,*

$$O[H,E](x,v) = \begin{cases} 1 & \text{if } x \in E \text{ and } (x,v) \in R_{C_\lambda,H}. \\ 0 & \text{otherwise,} \end{cases}$$

decide whether (YES) $|E| = 2^\lambda$ or (NO) $|E| \leq 2^\lambda - \sigma(\lambda)$.

The original problem [11] set $\sigma(n) = \frac{2^{\lambda+1}}{3}$. Instead, we will use $\sigma(n) = 2$. For simplicity of notation, in this section we will write that $\mathsf{QCMA}(2^{-n}) = \mathsf{QCMA}(1-2^{-n}, 1-2^{-n+1})$ and $\mathsf{QMA}(2^{-n}) = \mathsf{QMA}(1-2^{-n}, 1-2^{-n+1})$. Let us show that CISS_2 is in $\mathsf{QMA}(2^{-n})$.

▶ **Lemma 28.** CISS_2 *may be solved by* $\mathsf{QMA}(2^{-n})$.

Next, we will show the $\mathsf{QCMA}(2^{-n})$ lower bound. The main argument in [11] is that the existence of a QCMA algorithm which makes r queries and runs unitaries $\{U_i\}_{i\in[r]}$ implies the existence of a $\mathsf{Guesser}$ algorithm, a zero-query algorithm which can guess elements $(x,v) \in R_{C_\lambda,H}$ without making any queries to $O[H,E]$. In the algorithm below, we will use O_S to denote the unitary which, given a set S, behaves as follows,

$$O_S |x,y\rangle \coloneqq |x, y \oplus \mathbb{1}[x \in S]\rangle .$$

Algorithm 1 $\mathsf{Guesser}$.

Input: String 1^l and unitaries $\{U_i\}_{i\in[r]}$.
Sample $y \leftarrow \{0,1\}^w$ and set $S_0 = \emptyset$;
for $i \in [l]$ **do**
  Sample $j \leftarrow [0, r-1]$;
  Compute $|\psi_j\rangle = U_j O_{S_{i-1}} \dots O_{S_{i-1}} U_0 |y, 0\rangle$;
  Measure the query register of $|\psi_j\rangle$ to get some (x,v);
  Set $S_j \coloneqq S_{j-1} \cup \{(x,v)\}$;
Output: $\{(x_{[1,\lambda]}, v) : (x,v) \in S_l\}$

The following statements are directly from [11], except we parametrized the soundness and completeness gap as δ. The first is a lower bound on the success probability of $\mathsf{Guesser}$.

▶ **Lemma 29** ($\mathsf{Guesser}$ lower bound; Lemma 6.4 in [11])**.** *Let $\delta > 0$ and suppose there exists a $\mathsf{QCMA}(c, c-\delta)$ algorithm $\mathcal{A}$ that uses a $t(\lambda)$-bit classical witness, $Q(\lambda)$ oracle queries solving CISS_2. Then for all $l \leq 2^\lambda - 1$, there exists a no-query $\mathsf{Guesser}$ such that for every $H \in \mathsf{Good}$,*

$$\Pr\left[\begin{matrix}\forall i \neq j,\ (x_i,v_i) \neq (x_j,v_j) \\ \wedge\ (x_i \| 0^{q-\lambda}, v_i) \in R_{C_\lambda,H}\end{matrix} : \{(x_i,v_i)\}_{i=1}^l \leftarrow \mathsf{Guesser}(1^l)\right] \geq 2^{-t(\lambda)} \cdot \left(\frac{\delta^2}{16\,Q(\lambda)^2}\right)^l .$$

Below is the upper bound on the success of $\mathsf{Guesser}$, which will be used for a contradiction of the existence of $\mathcal{A}$.

▶ **Lemma 30** (Guesser upper bound; Lemma 6.6 in [11]). *For all sufficiently large λ and any algorithm* Guesser *making no oracle queries, for all $l \leq 2^\lambda$,*

$$\Pr_{H \leftarrow \mathsf{Bias}_{q,p^*,\mathbb{F}_q^s}}\left[\begin{array}{l}\{(x_i,v_i)\}_{i=1}^{l} \leftarrow \mathsf{Guesser}(1^l): \\ \forall i \neq j,\ (x_i,v_i) \neq (x_j,v_j) \text{ and } (x_i \| 0^{q-\lambda}, v_i) \in R_{C_\lambda,H}\end{array}\right] \leq 2^{-\lambda^2 l/32}.$$

With the results above, we may show the main result.

▶ **Theorem 31.** *There exists a classical oracle O such that,*

$$\Pi_2^{\mathsf{P}^O} \cap \mathsf{PreciseQCMA}^O \cap \mathsf{QMA}^O(2^{-n}) \not\subseteq \mathsf{QCMA}^O(2^{-n}).$$

3.3.3 Circuit complexity of sparse Hamiltonian ground states

Suppose that, for some sparse Hamiltonian, we are given oracle access via O_H^{rc}. Can we lower-bound the circuit complexity of preparing an approximate ground state of H? As we will show below, this is a straightforward consequences of the classical oracle separation between QMA and QCMA [10, 11]. Nonetheless, to the best of our knowledge, this connection has not been established yet in prior literature, and shows an interesting parallel to the NLTS theorem [5].

In our proofs, we will assume that verifiers are using the gate set $\mathcal{G} = \{\mathrm{X}, \mathrm{CNOT}, \mathrm{Toffoli}, \mathrm{H} \otimes \mathrm{H}\}$, which is computationally universal as it can simulate H [46].

▶ **Theorem 32.** *There exists a family of $O(1)$-sparse Hamiltonians $\mathcal{H} = \{H_i\}_{i\in\mathbb{N}}$ on $n_i > n_{i-1}$ qubits with integer entries bounded by $O(1)$ such that for all i, any state $|\psi\rangle$ generated by a circuit with $2^{o(n_i^{1/3}\log(n_i)^{-1})}$ gates (using $\mathcal{G}$ and $O_{H_i}^{\mathrm{rc}}$),*

$$\langle\psi| H_i |\psi\rangle \geq \lambda_0(H_i) + \tfrac{1}{\mathrm{poly}(n_i)}.$$

We note that one may obtain a similar result using the classical oracle separation in [10]. With our work, we can extend Theorem 32 to frustration-free Hamiltonians in the bounded adaptivity parallel-query setting. Note that extending Theorem 32 to the frustration-free setting without query restrictions would imply a classical oracle separation between QCMA and QMA$_1$, an open problem.

▶ **Theorem 33.** *For any $k \in \mathbb{N}$, there exists a family of $O(1)$-sparse frustration-free Hamiltonians $\mathcal{H} = \{H_i\}_{i\in\mathbb{N}}$ on $n_i > n_{i-1}$ qubits with integer entries bounded by $O(1)$, such that for all i, any state $|\psi\rangle$ generated by a circuit with $2^{o(n_i)}$ gates (using $\mathcal{G}$ and O_H^{rc}) using n^k rounds of queries to O_H^{rc} has*

$$\langle\psi| H_i |\psi\rangle \geq \tfrac{1}{\mathrm{poly}(n_i)}.$$

Additionally, the ground state of H_i may be prepared using $n_i^k + O(1)$ adaptive queries to O_H^{rc}.

References

1 Scott Aaronson. Quantum lower bound for the collision problem. In *Proceedings of the Thiry-Fourth Annual ACM Symposium on Theory of Computing*, STOC '02, pages 635–642, New York, NY, USA, 2002. Association for Computing Machinery. doi:10.1145/509907.509999.

2 Scott Aaronson. On perfect completeness for QMA. *Quantum Information & Computation*, 9(1):81–89, 2009. doi:10.26421/QIC9.1-2-5.

3 Scott Aaronson and Greg Kuperberg. Quantum versus classical proofs and advice. In *Twenty-Second Annual IEEE Conference on Computational Complexity (CCC'07)*, pages 115–128. IEEE, 2007. doi:10.1109/CCC.2007.27.

4 Dorit Aharonov and Tomer Naveh. Quantum NP-a survey. *quant-ph/0210077*, 2002.

5 Anurag Anshu, Nikolas P. Breuckmann, and Chinmay Nirkhe. Nlts hamiltonians from good quantum codes. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*, STOC '23, pages 1090–1096. ACM, June 2023. doi:10.1145/3564246.3585114.

6 Sanjeev Arora and Boaz Barak. *Computational Complexity: A Modern Approach*. Cambridge University Press, USA, 1st edition, 2009.

7 Roozbeh Bassirian, Bill Fefferman, and Kunal Marwaha. On the Power of Nonstandard Quantum Oracles. In Omar Fawzi and Michael Walter, editors, *18th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2023)*, volume 266 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 11:1–11:25, Dagstuhl, Germany, 2023. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. doi:10.4230/LIPIcs.TQC.2023.11.

8 Shalev Ben-David and Srijita Kundu. Oracle Separation of QMA and QCMA with Bounded Adaptivity. In *51st International Colloquium on Automata, Languages, and Programming (ICALP 2024)*, volume 297 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 21:1–21:18. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2024. doi:10.4230/LIPIcs.ICALP.2024.21.

9 Charles H. Bennett, Ethan Bernstein, Gilles Brassard, and Umesh Vazirani. Strengths and weaknesses of quantum computing. *SIAM Journal on Computing*, 26(5):1510–1523, 1997. doi:10.1137/S0097539796300933.

10 John Bostanci, Jonas Haferkamp, Chinmay Nirkhe, and Mark Zhandry. Separating QMA from QCMA with a classical oracle, 2026. doi:10.48550/arXiv.2511.09551.

11 John Bostanci, Andrew Huang, and Vinod Vaikuntanathan. Separating quantum and classical advice with good codes, 2026. doi:10.48550/arXiv.2602.09385.

12 Sergey Bravyi. Efficient algorithm for a quantum analogue of 2-sat, 2006. arXiv:quant-ph/0602108.

13 Anne Broadbent, Alex B Grilo, Supartha Podder, and Jamie Sikora. The role of piracy in quantum proofs. In *International Conference on Cryptology and Information Security in Latin America*, pages 267–295. Springer, 2025. doi:10.1007/978-3-032-06754-8_10.

14 Alper Cakan, Vipul Goyal, and Omri Shmueli. Public-key quantum fire and key-fire from classical oracles. *arXiv preprint*, 2025. arXiv:2504.16407.

15 Rohit Chatterjee, Srijita Kundu, and Supartha Podder. Uncloneable quantum states are necessary as proofs and advice. In *Proceedings of the 57th Annual ACM Symposium on Theory of Computing*, pages 1817–1827, 2025. doi:10.1145/3717823.3718226.

16 Friederike Anna Dziemba. Robustness of QMA against witness noise. *Quantum Information & Computation*, 17(13-14):1167–1190, 2017. doi:10.26421/QIC17.13-14-6.

17 Bill Fefferman and Shelby Kimmel. Quantum vs. Classical Proofs and Subset Verification. In Igor Potapov, Paul Spirakis, and James Worrell, editors, *43rd International Symposium on Mathematical Foundations of Computer Science (MFCS 2018)*, volume 117 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 22:1–22:23, Dagstuhl, Germany, 2018. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. doi:10.4230/LIPIcs.MFCS.2018.22.

18 Bill Fefferman and Cedric Yen-Yu Lin. A Complete Characterization of Unitary Quantum Space. In Anna R. Karlin, editor, *9th Innovations in Theoretical Computer Science Conference (ITCS 2018)*, volume 94 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 4:1–4:21, Dagstuhl, Germany, 2018. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. doi:10.4230/LIPIcs.ITCS.2018.4.

19 Michael H. Freedman and Matthew B. Hastings. Quantum systems on non-k-hyperfinite complexes: A generalization of classical statistical mechanics on expander graphs. *Quantum Information & Computation*, 14(1–2):144–180, 2014. doi:10.26421/QIC14.1-2-9.

20 François Le Gall, Harumichi Nishimura, and Dhara Thakkar. Group order is in qcma. In *2025 IEEE 66th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 1128–1143, 2025. doi:10.1109/FOCS63196.2025.00059.

21 Sevag Gharibian, Miklos Santha, Jamie Sikora, Aarthi Sundaram, and Justin Yirka. Quantum generalizations of the polynomial hierarchy with applications to QMA(2). *Computational Complexity*, 31(2):13, 2022. doi:10.1007/s00037-022-00231-8.

22 David Gosset and Daniel Nagaj. Quantum 3-SAT is QMA_1-complete. *SIAM J. Comput.*, 45(3):1080–1128, January 2016. doi:10.1137/140957056.

23 Alex Bredariol Grilo, Iordanis Kerenidis, and Jamie Sikora. QMA with subset state witnesses. In *International Symposium on Mathematical Foundations of Computer Science*, pages 163–174. Springer, 2015. doi:10.1007/978-3-662-48054-0_14.

24 Lov K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, STOC '96, pages 212–219, New York, NY, USA, 1996. Association for Computing Machinery. doi:10.1145/237814.237866.

25 Blake Holman, Ronak Ramachandran, and Justin Yirka. Quantum Search with In-Place Queries. In Bill Fefferman, editor, *20th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2025)*, volume 350 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 1:1–1:18, Dagstuhl, Germany, 2025. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. doi:10.4230/LIPIcs.TQC.2025.1.

26 Elham Kashefi, Adrian Kent, Vlatko Vedral, and Konrad Banaszek. Comparison of quantum oracles. *Phys. Rev. A*, 65:050304, May 2002. doi:10.1103/PhysRevA.65.050304.

27 A. Yu. Kitaev, A. H. Shen, and M. N. Vyalyi. *Classical and Quantum Computation*. American Mathematical Society, USA, 2002.

28 Alexei Kitaev. Quantum NP. *Talk at AQIP*, 99, 1999.

29 Hartmut Klauck. The Complexity of Quantum Disjointness. In *42nd International Symposium on Mathematical Foundations of Computer Science (MFCS 2017)*, volume 83 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 15:1–15:13. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2017. doi:10.4230/LIPIcs.MFCS.2017.15.

30 Hartmut Klauck and Supartha Podder. Two results about quantum messages. In *International Symposium on Mathematical Foundations of Computer Science*, pages 445–456. Springer, 2014. doi:10.1007/978-3-662-44465-8_38.

31 Hirotada Kobayashi, François Le Gall, and Harumichi Nishimura. Stronger methods of making quantum interactive proofs perfectly complete. In *Proceedings of the 4th conference on Innovations in Theoretical Computer Science*, pages 329–352, 2013. doi:10.1145/2422436.2422475.

32 Hirotada Kobayashi, Daniel Nagaj, and Harumichi Nishimura. Achieving perfect completeness in classical-witness quantum merlin-arthur proof systems. *Quantum Information and Computation*, 12(5&6):0461–0471, 2012. doi:10.26421/QIC12.5-6-7.

33 Nicholas Laracuente. Quantum oracle separations from complex but easily specified states. *arXiv:2104.07247*, 2021.

34 Xingjian Li, Qipeng Liu, Angelos Pelecanos, and Takashi Yamakawa. Classical vs Quantum Advice and Proofs Under Classically-Accessible Oracle. In *15th Innovations in Theoretical Computer Science Conference (ITCS 2024)*, volume 287 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 72:1–72:19. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2024. doi:10.4230/LIPIcs.ITCS.2024.72.

35 Jiahui Liu, Saachi Mutreja, and Henry Yuen. QMA vs QCMA and pseudorandomness. In *Proceedings of the 57th Annual ACM Symposium on Theory of Computing*, pages 1520–1531, 2025. doi:10.1145/3717823.3718296.

36 Andrew Lutomirski. Component mixers and a hardness result for counterfeiting quantum money. *arXiv:1107.0321*, 2011.

37 Chris Marriott and John Watrous. Quantum Arthur–Merlin games. *Computational Complexity*, 14(2):122–152, June 2005. doi:10.1007/s00037-005-0194-x.

38 Tomoyuki Morimae and Harumichi Nishimura. Merlinization of complexity classes above BQP. *Quantum Info. Comput.*, 17(11-12):959–972, September 2017. doi:10.26421/QIC17.11-12-3.

39 Dimitrios I Myrisiotis. *Quantum Complexity, Relativized Worlds*. PhD thesis, National and Kapodistrian University of Athens, 2016.

40 Daniel Nagaj, Dominik Hangleiter, Jens Eisert, and Martin Schwarz. Pinned quantum merlin-arthur: The power of fixing a few qubits in proofs. *Physical Review A*, 103(1):012604, 2021.

41 Daniel Nagaj, Pawel Wocjan, and Yong Zhang. Fast amplification of QMA. *Quantum Information & Computation*, 9(11–12):1053–1068, 2011. arXiv:0904.1549.

42 Anand Natarajan and Chinmay Nirkhe. A distribution testing oracle separation between QMA and QCMA. *Quantum*, 8:1377, 2024. doi:10.22331/Q-2024-06-17-1377.

43 Barak Nehoran and Mark Zhandry. A Computational Separation Between Quantum No-Cloning and No-Telegraphing. In *15th Innovations in Theoretical Computer Science Conference (ITCS 2024)*, volume 287 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 82:1–82:23. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2024. doi:10.4230/LIPIcs.ITCS.2024.82.

44 Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010.

45 Ran Raz and Amir Shpilka. On the power of quantum proofs. In *Proceedings. 19th IEEE Annual Conference on Computational Complexity, 2004.*, pages 260–274. IEEE, 2004. doi:10.1109/CCC.2004.1313849.

46 Yaoyun Shi. Both toffoli and controlled-not need little help to do universal quantum computing. *Quantum Info. Comput.*, 3(1):84–92, January 2003. doi:10.26421/QIC3.1-7.

47 Seinosuke Toda. Pp is as hard as the polynomial-time hierarchy. *SIAM Journal on Computing*, 20(5):865–877, 1991. doi:10.1137/0220053.

48 John Watrous. Succinct quantum proofs for properties of finite groups. In *Proceedings 41st Annual Symposium on Foundations of Computer Science*, pages 537–546. IEEE, 2000. doi:10.1109/SFCS.2000.892141.

49 Takashi Yamakawa and Mark Zhandry. Verifiable quantum advantage without structure. *J. ACM*, 71(3), June 2024. doi:10.1145/3658665.

50 Mark Zhandry. Toward Separating QMA from QCMA with a Classical Oracle. In *16th Innovations in Theoretical Computer Science Conference (ITCS 2025)*, volume 325 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 95:1–95:19. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2025. doi:10.4230/LIPIcs.ITCS.2025.95.