Quantum Merlin-Arthur with an internally separable proof

Roozbeh Bassirian[1], Bill Fefferman[1], Itai Leigh[2], Kunal Marwaha[1], and Pei Wu[3]

[1]University of Chicago
[2]Tel Aviv University
[3]Penn State University

Extended abstract

Entanglement is a fundamental feature of quantum mechanics, and quantum proof systems offer a clean complexity-theoretic lens for isolating which aspects of entanglement matter computationally. A canonical open problem is to characterize the power of unentanglement in QMA(2), where two Merlins are required to send an unentangled witness across a fixed bipartition. Despite extensive work, our understanding remains limited. On the other hand, multipartite entanglement admits far richer structure than the binary distinction "entangled vs. unentangled," motivating a finer-grained study of the witness's entanglement structure. In this work, we take a first step exploring whether fine-grained entanglement promises can lead to a robust and analyzable refinement of QMA(2), or whether even very mild structural constraints on entanglemetn already trigger a dramatic complexity jumps to NEXP.

We study the natural promise of internal entanglement. We restrict Merlin to witnesses that are *internally separable*: the proof has a fixed tripartite form ρ_{ABC} in which C consists of $O(1)$ qubits and the reduced state ρ_{BC} is separable after tracing out A. This constraint is mild—the global state may still be entangled across every bipartition—but it fixes a separable marginal (equivalently, the witness is a partial purification of a separable state). Our main result shows a qualitative jump from one proof to two: with one internally separable proof the resulting class is simulable in EXP (even for inverse-exponentially small gaps), whereas with two unentangled internally separable proofs the class captures NEXP at a constant gap.

Beyond the separation itself, the proof exposes an unexpectedly narrow "use" of unentanglement: the second proof is needed only to perform a purity test, which lets the verifier treat the witness as effectively pure. In this way, our results isolate a sharp *pure-vs-mixed* distinction: once purity can be certified, the internal-separability promise suffices to enable NEXP-power verification.

Definitions. QMA is the class of decision problems that can be decided by a quantum computer ("Arthur") with help from a dishonest but all-powerful machine ("Merlin"). Merlin sends a quantum state ("proof") that is most likely to convince Arthur of a statement's veracity. If the statement is true, there is a proof that convinces Arthur to accept with high probability; if it is false, all proofs make Arthur reject with high probability. QMA(2) [19] is a variant of QMA where the quantum proof is guaranteed to be *not* entangled across a fixed bipartition. Although there is evidence that QMA(2) is more powerful than QMA [2, 10, 23, 15], we only know the trivial bounds $\mathsf{QMA} \subseteq \mathsf{QMA}(2) \subseteq \mathsf{NEXP}$.

We define the complexity class $\mathsf{QMA}_{\mathsf{IS}}$, a variant to QMA where the quantum proof must have a fixed, separable *subsystem*: that is, after tracing out all qubits beyond the subsystem, a predetermined set of $O(1)$ qubits are *not* entangled with the rest of the subsystem. Unlike in QMA(2), this guarantee refers to *internal* separability: the two parts of the subsystem can be entangled, but only if the entanglement disappears when the subsystem is isolated. See Figure 1 for a visual comparison.[1]

[1]We restrict one part of the subsystem to $O(1)$ qubits to isolate the effect of *internal* entanglement structure. Without the restriction, this class trivially contains QMA(2).

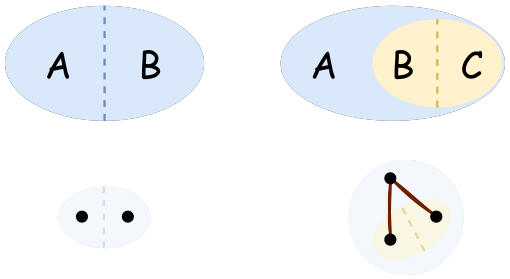

Figure 1: Cartoons of a separable state and a state with a separable subsystem. The left side depicts a separable state, where parts A and B share no entanglement. The right side depicts a state where *after* tracing out part A, parts B and C share no entanglement; this state is in general entangled across every bipartition. The lower cartoons each display a graph where every vertex is a part (A, B, or C), and an edge between two parts X, Y allows bipartite entanglement in the reduced state ρ_{XY}. On the right side, part A is entangled with both part B and part C.

Main results. We first show that $\mathsf{QMA}_{\mathsf{IS}}(2)$ at a small promise gap can decide NEXP. A quantum verifier with a specific guarantee on entanglement structure is exponentially more powerful than a classical verifier.

Theorem 1. *There exist constants* $1 > c > s > 0$ *where* $\mathsf{QMA}_{\mathsf{IS}}^{c,s}(2) = \mathsf{NEXP}$.

Moreover, for any constant k, there exist constants $1 > c' > s' > 0$ where $\mathsf{QMA}_{\mathsf{IS}}^{c',s'}(k) = \mathsf{QMA}(k)$. As a result, gap amplification of $\mathsf{QMA}_{\mathsf{IS}}(2)$ would imply $\mathsf{QMA}(2) = \mathsf{NEXP}$.

Corollary 2. *If* $\mathsf{QMA}_{\mathsf{IS}}(2)$ *exhibits gap amplification, then* $\mathsf{QMA}(2) = \mathsf{NEXP}$.

Although the same is true of $\mathsf{QMA}^{+}(2)$ [17], the class QMA^{+} *cannot* have gap amplification unless $\mathsf{QMA} = \mathsf{NEXP}$ [7]. This limits the techniques available to prove gap amplification of $\mathsf{QMA}^{+}(2)$. By contrast, $\mathsf{QMA}_{\mathsf{IS}}$ even with inverse exponentially small promise gap is contained in EXP.

Theorem 3. *For any* $1 > c > s > 0$ *such that* $c - s = \Omega(\frac{1}{2^{\mathrm{poly}(n)}})$, *we have* $\mathsf{QMA}_{\mathsf{IS}}^{c,s} \subseteq \mathsf{EXP}$.

This means that gap amplification of $\mathsf{QMA}_{\mathsf{IS}}(2)$ can be plausibly found by studying gap amplification of $\mathsf{QMA}_{\mathsf{IS}}$, as the latter implies no such complexity collapse. This raises the exciting possibility of using Corollary 2 to fully characterize $\mathsf{QMA}(2)$. We summarize this in Table 1.

internal structure \ *external structure*	GENERAL	SEPARABLE BIPARTITION
GENERAL	QMA	$\mathsf{QMA}(2)$
SEPARABLE SUBSYSTEM	$\mathsf{QMA}_{\mathsf{IS}} \subseteq \mathsf{EXP}$	$\mathsf{QMA}_{\mathsf{IS}}(2) = \mathsf{NEXP}$

Table 1: Categorizing quantum verification protocols by the guaranteed entanglement structures in the proof.

Implications $\mathsf{QMA}(2)$ is concerned specifically with *bipartite* unentanglement. With $\mathsf{QMA}_{\mathsf{IS}}$, we can study one type of multipartite unentanglement known as *partial semi-separability* [11]. We also prove that restricting to quantum proofs that are pure and *multiseparable* [24] can decide NEXP. This motivates a general question about the power of QMA with other guarantees on multipartite entanglement:

Question 4. *Which notions of* multipartite unentanglement *are computationally strong? Why?*

Moreover, $\mathsf{QMA}_{\mathsf{IS}}(2)$ is no more powerful than $\mathsf{QMA}_{\mathsf{IS}}$ equipped with a purity test. This suggests that the power of *unentanglement* in $\mathsf{QMA}_{\mathsf{IS}}(2)$ arises from its ability to enforce purity. This is not coincidence: Many works [21, 15, 6, 25] use the fact that a protocol over separable states is equivalently a protocol over states with a purity constraint.

With mild conditions on a general set of quantum states $\mathcal{W}$, we show how a $\mathsf{QMA}(2)$ protocol with each proof restricted to $\mathcal{W}$ can implement a QMA protocol with a proof restricted to *pure states* in $\mathcal{W}$. We use this as a recipe to generate other computational models that provably demonstrate the power of unentanglement, up to standard complexity-theoretic assumptions. As examples, we use the pure quantum proofs in QMA^+, and the *proper states* of [2, 9] as pure states of a larger set $\mathcal{W}$. Then, $\mathsf{QMA}_{\mathcal{W}}$ can be decided with a semidefinite program, but $\mathsf{QMA}_{\mathcal{W}}(2)$ can implement a SWAP test to restrict to the more capable pure states.

Techniques. To show Theorem 3, we rely on a well-known duality of membership testing of a convex set and optimizing a convex function over this set. We use this duality to reduce any $\mathsf{QMA}_{\mathsf{IS}}$ problem to membership testing of the set of internally separable quantum states $\mathcal{W}_{\mathsf{IS}}$. In order to use tools from convex optimization, we represent quantum states as vectors in a generalized Bloch sphere. We use a non-ellipsoidal reduction that permits an error analysis matching our setup [20, 14].

We then test membership of two convex sets whose intersection forms $\mathcal{W}_{\mathsf{IS}}$. Here, it is essential that only $O(1)$ qubits are unentangled from the rest of the subsystem. The first set represents all Bloch vectors of quantum states, which can be tested using exponentially many explicit conditions (e.g. [18]). The second set represents all vectors whose reduced density matrix on the subsystem is separable. This can be tested by solving the Doherty-Parrilo-Spedalieri SDP [12, 13, 22] which decides if a state has a *symmetric extension*. When one part of the subsystem contains $O(1)$ qubits, this SDP runs in exponential time.

To prove Theorem 1, we consider $\mathsf{QMA}_{|\mathsf{IS}\rangle}$, a variant of $\mathsf{QMA}_{\mathsf{IS}}$ where the proof must also be a *pure state*. Note that unlike QMA and $\mathsf{QMA}(2)$, restricting $\mathsf{QMA}_{\mathsf{IS}}$ to pure states can change the power of the complexity class, as an internally separable ensemble of pure states may not decompose into an *ensemble* of internally separable pure states. We then develop a $\mathsf{QMA}_{|\mathsf{IS}\rangle}$ protocol for an NEXP-complete problem, building on the proof of $\mathsf{QMA}^+ = \mathsf{NEXP}$ [10, 17, 7].

As in [17, 7], we consider a succinct constraint satisfaction problem (CSP) with constant promise gap, which is NEXP-hard by the PCP theorem [5, 4, 16]. In the QMA^+ protocol, one enforces a *rigidity* property of the quantum proof: the state must be close to $\frac{1}{\sqrt{R}} \sum_{j \in [R]} |j\rangle |a_j\rangle$. One can ensure that all constraints $j \in [R]$ are included in the state ("density"), but the positive-amplitude guarantee is used to ensure there is at most one assignment a_j per constraint ("validity"). We instead enforce validity using both internal separability and purity.

Lemma 5 (informal)**.** *There is a test A and a fixed quantum circuit C such that for any internally separable $|\psi\rangle$, if $A(|\psi\rangle) \geq 1 - \epsilon$, then $C|\psi\rangle$ has $1 - O(\epsilon)$ squared overlap with a* valid *state.*

In our $\mathsf{QMA}_{|\mathsf{IS}\rangle}$ protocol, the verifier enforces tripartite proofs of the form $\sum_{j,a} z_{ja} |j\rangle |a, j\rangle |a\rangle$. This can be done by measuring all registers and accepting iff we see two copies of the same constraint j, and two copies of the same assignment a. We then observe that having multiple assignments per constraint adds entanglement to the second and third registers, even after tracing out the first register. Thus, if the state is *internally separable*, it has high overlap with a state with one assignment a per constraint j. Notably, this test is inspired by recasting the QMA^+ protocol in the language of "superposition detection" and non-collapsing measurement [8, 3], an unphysical operation related to a problem of Aaronson [1].

We then prove that $\mathsf{QMA}_{|\mathsf{IS}\rangle} \subseteq \mathsf{QMA}_{\mathsf{IS}}(2)$. The best proof Merlin can send in a $\mathsf{QMA}_{\mathsf{IS}}(2)$ protocol is a product state $\rho_1 \otimes \rho_2$. The SWAP test accepts a product state with probability $\frac{1}{2}(1 + \mathrm{Tr}[\rho_1 \rho_2])$: this is 1 only if ρ_1, ρ_2 are *pure*. The $\mathsf{QMA}_{\mathsf{IS}}(2)$ simulator thus applies a SWAP test with some probability, and otherwise applies the $\mathsf{QMA}_{|\mathsf{IS}\rangle}$ circuit.

References

[1] Scott Aaronson. *Quantum miscellany — Shtetl-Optimized*. 2023. URL: https://scottaaronson.blog/?p=7516.

[2] Scott Aaronson, Salman Beigi, Andrew Drucker, Bill Fefferman, and Peter Shor. "The Power of Unentanglement". In: *Theory of Computing* 5.1 (2009), pp. 1–42. DOI: 10.4086/toc.2009.v005a001. arXiv: 0804.0802.

[3] Scott Aaronson, Sabee Grewal, Vishnu Iyer, Simon C. Marshall, and Ronak Ramachandran. *PDQMA = DQMA = NEXP: QMA With Hidden Variables and Non-collapsing Measurements*. 2024. arXiv: 2403.02543.

[4] Sanjeev Arora, Carsten Lund, Rajeev Motwani, Madhu Sudan, and Mario Szegedy. "Proof Verification and the Hardness of Approximation Problems". In: *J. ACM* 45.3 (1998), pp. 501–555. DOI: 10.1145/278298.278306. URL: https://www.cs.umd.edu/~gasarch/TOPICS/pcp/ALMSS.pdf.

[5] Sanjeev Arora and Shmuel Safra. "Probabilistic Checking of Proofs; A New Characterization of NP". In: *33rd Annual Symposium on Foundations of Computer Science*. 1992. DOI: 10.1109/SFCS.1992.267824. URL: https://www.cs.umd.edu/~gasarch/TOPICS/pcp/AS.pdf.

[6] Boaz Barak, Pravesh K. Kothari, and David Steurer. "Quantum entanglement, sum of squares, and the log rank conjecture". In: *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*. 2017. DOI: 10.1145/3055399.3055488. arXiv: 1701.06321.

[7] Roozbeh Bassirian, Bill Fefferman, and Kunal Marwaha. "Quantum Merlin-Arthur and proofs without relative phase". In: *15th Innovations in Theoretical Computer Science Conference (ITCS 2024)*. 2023. DOI: 10.4230/LIPIcs.ITCS.2024.9. arXiv: 2306.13247.

[8] Roozbeh Bassirian and Kunal Marwaha. *Superposition detection and QMA with non-collapsing measurements*. 2024. arXiv: 2403.02532.

[9] Salman Beigi. *NP vs QMA_log(2)*. 2008. arXiv: 0810.5109.

[10] Hugue Blier and Alain Tapp. "A quantum characterization of NP". In: *Comput. Complex.* (Sept. 2012). DOI: 10.1007/s00037-011-0016-2. arXiv: 0709.0738.

[11] Gilles Brassard and Tal Mor. "Multi-particle entanglement via two-party entanglement". In: *Journal of Physics A: Mathematical and General* 34.35 (Aug. 2001). DOI: 10.1088/0305-4470/34/35/306. URL: https://csaws.cs.technion.ac.il/~talmo/CV/my-papers/BM01-multipartyEnt.pdf.

[12] Andrew C. Doherty, Pablo A. Parrilo, and Federico M. Spedalieri. "Distinguishing Separable and Entangled States". In: *Phys. Rev. Lett.* 88 (18 Apr. 2002). DOI: 10.1103/PhysRevLett.88.187904. arXiv: quant-ph/0112007.

[13] Andrew C. Doherty, Pablo A. Parrilo, and Federico M. Spedalieri. "Complete family of separability criteria". In: *Physical Review A* 69.2 (Feb. 2004). DOI: 10.1103/physreva.69.022308. arXiv: quant-ph/0308032.

[14] Sevag Gharibian. "Strong NP-Hardness of the Quantum Separability Problem". In: *Quantum Info. Comput.* 10.3 (Mar. 2010), pp. 343–360. DOI: 10.5555/2011350.2011361. arXiv: 0810.4507.

[15] Aram W. Harrow and Ashley Montanaro. "Testing product states, quantum Merlin-Arthur games and tensor optimization". In: *Journal of the ACM (JACM)* 60.1 (2013), pp. 1–43. DOI: 10.1145/2432622.2432625. arXiv: 1001.0017.

[16] Prahladh Harsha. "Robust PCPs of proximity and shorter PCPs". PhD thesis. Massachusetts Institute of Technology, 2004. URL: https://dspace.mit.edu/bitstream/handle/1721.1/26720/59552830-MIT.pdf.

[17] Fernando Granha Jeronimo and Pei Wu. "The Power of Unentangled Quantum Proofs with Non-negative Amplitudes". In: *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*. 2023. DOI: 10.1145/3564246.3585248. arXiv: 2402.18790.

[18] Gen Kimura. "The Bloch vector for N-level systems". In: *Physics Letters A* 314.5–6 (Aug. 2003), pp. 339–349. DOI: 10.1016/s0375-9601(03)00941-1. arXiv: quant-ph/0301152.

[19] Hirotada Kobayashi, Keiji Matsumoto, and Tomoyuki Yamakami. "Quantum Merlin-Arthur Proof Systems: Are Multiple Merlins More Helpful to Arthur?" In: *Algorithms and Computation*. 2003. DOI: 10.1007/978-3-540-24587-2_21. arXiv: quant-ph/0306051.

[20] Yi-Kai Liu. "The Complexity of the Consistency and N-representability Problems for Quantum States". PhD thesis. University of California, San Diego, 2007. arXiv: 0712.3041.

[21] Yi-Kai Liu, Matthias Christandl, and F. Verstraete. "N-representability is QMA-complete". In: *Physical Review Letters* 98.11 (Mar. 2007). DOI: 10.1103/physrevlett.98.110503. arXiv: quant-ph/0609125.

[22] Miguel Navascués, Masaki Owari, and Martin B. Plenio. "Power of symmetric extensions for entanglement detection". In: *Physical Review A* 80.5 (Nov. 2009). DOI: 10.1103/physreva.80.052306. arXiv: 0906.2731.

[23] Attila Pereszlényi. *Multi-Prover Quantum Merlin-Arthur Proof Systems with Small Gap*. 2012. arXiv: 1205.2761.

[24] Ashish V. Thapliyal. "Multipartite pure-state entanglement". In: *Physical Review A* 59.5 (May 1999), pp. 3336–3342. DOI: 10.1103/physreva.59.3336. arXiv: quant-ph/9811091.

[25] Xiao-Dong Yu, Timo Simnacher, H. Chau Nguyen, and Otfried Gühne. "Quantum-Inspired Hierarchy for Rank-Constrained Optimization". In: *PRX Quantum* 3.1 (Mar. 2022). DOI: 10.1103/prxquantum.3.010340. arXiv: 2012.00554.