nature portfolio

Peer Review File

Unconditional advantage of noisy qudit quantum circuits over biased threshold circuits in constant depth

Corresponding Author: Mr Michael Oliveira

This file contains all reviewer reports in order by version, followed by all author rebuttals in order by version.

Version 0:

Reviewer comments:

Reviewer #1

(Remarks to the Author)
Noteworthy Results:

* This work unconditionally demonstrates that parallel quantum computation can exhibit greater computational power than previously believed/recognize.

* In particular, they show that there are certain problems solvable in QNC^0 (constant-depth quantum circuits with local gates), which are not solvable in poly-sized biased-PTC^0 (i.e. bPTC^0(k)).

* They identify a family of problems solvable by a constant-depth universal quantum computation over prime qudits (which are experimentally of interest because they appear to be more robust to noise) with bounded connectivity which is hard for poly-sized biased TC^0.

* They bridge high-dimensional non-local games with computational advantage on practically relevant/attainable architectures.

* They further show that the quantum advantages are robust to noise, making them even more practically plausible.

Significance to the field:

I enjoyed reading this paper and learned quite a bit about the unconditional quantum advantage literature. The paper does a good job of presenting novel, interesting theoretical results, while also motivating them very well from an experimental perspective - proving their robustness to noise and compatibility with current architectures. Therefore, the paper will be of interest to experimentalists in addition to theorists. In addition to the impact of the work - expanding the circuit class size for which unconditional quantum advantage exists - the work has a lot of technical novelty, introducing many new techniques (for example, novel qubit to qudit mappings/proofs and a new switching lemma for bPTC^0 circuits) that I believe will be of great interest/use for theorists working on related problems. Overall, the work is a very rigorous, comprehensive study of the proposal (studying, for example, robustness to noise and providing detailed resource estimates), offering justification for all the results/proofs and motivating them in comparison to the prior work. Overall, I think the paper makes many novel contributions, both technical and conceptual, and will be appealing to both the theory and experimental communities.

Comparison to established literature:

* Prior to this work, the largest classical circuit class for which unconditional quantum advantage was established was AC^0. However, note that AC^0 is a subset of bPTC^0(k), for bias k=O(1). However, for larger values of k, bPTC^0 contains circuits beyond AC^0. This work therefore expands the circuit classes for which unconditional quantum advantage exists.

* Interestingly their bPTC^0 proposal also encompasses problems which likely lie outside of TC^0. Since neural network architectures, such as LLMs are contained in TC^0, this suggests that there might be novel neural net architectures that lie within the computational power of shallow-depth noisy quantum circuits.

* Although they leverage non-local games, as has previously been done in the literature, they propose a new family of relational problems - ISMRP- which they show lies in QNC^0 and TC^0, but is strictly beyond bPTC^0.

* From the way the text is written on Lines 113-115, it is unclear if the authors are claiming to have proven the classical separation NC^0 < AC^0 < bPTC^0(k) for k=w(log n), or whether they are using this previously known fact to argue that the bPTC^0 circuit class is valuable in investigating quantum computational power. In the case of the former, they might want to make it more clear that they are actually proving this result (indicate where later in the paper/supplement this is shown). However, my impression is that it is the case of the latter - in which case, they should add citations to relevant prior works which showed these separations and also make it more explicit that they did not actually develop this hierarchy.

* The literature review could potentially be improved/expanded by citing the growing body of literature focused on proving separations for famous classical computations, such as computing Parity, in quantum classes beyond QNC^0. For example, there has been a lot of exciting recent work on proving explicit bounds on the number of ancilla needed to implement Parity in QAC^0 (e.g. [Rosenthal'20], [NPVY'24], [ADOY'24]) - motivated by the "quantum fanout is powerful" result [HS'05]. There is also a recent related result establishing the power of quantum threshold [GM'24].

Suggestions for Improving the Manuscript:

* On line 59, you refer to "parallel" quantum computation, but I don't think it is previously defined or explained why the relevant surrounding text describes "parallel" quantum computation. I think you could put more emphasis in the introduction on defining what "parallel" means in both the classical and quantum setting and explaining its significance, since it is pretty important to the text.

Potential Typos:

* Lines 24-25: "has quest the understanding if" - awkward/bad wording

* Lines 191-192: "with the extend to which"- awkward/bad wording

* Lines 267-271: I believe that there might be a grammatical typo or missing word (the sentence structure is strange and hard to follow)

* Line 596: "realizating" -> "realization"?

* Line 919: missing reference

REFERENCES
• Quantum Fan-out is Powerful -- Peter Høyer, Robert Spalek (2005)
• Bounds on the QAC0 Complexity of Approximating Parity -- Gregory Rosenthal (2020)
• On the Pauli Spectrum of QAC0 -- Shivam Nadimpalli, Natalie Parham, Francisca Vasconcelos, Henry Yuen (2024)
• On the Computational Power of QAC0 with Barely Superlinear Ancillae -- Anurag Anshu, Yangjing Dong, Fengning Ou, Penghui Yao (2024)
• Quantum Threshold is Powerful -- Daniel Grier, Jackson Morris (2024)

Reviewer #2

(Remarks to the Author)
The paper extends existing unconditional quantum advantage results to show that constant-depth noisy qudit circuits can beat constant-depth threshold circuits. Existing work had separated constant-depth quantum circuits (QNC^0) from constant-depth classical circuits with unbounded fan-in gates (AC^0). This work is similar, but against a slightly larger class of classical circuits, while maintaining noise robustness of the quantum circuit and an exponential separation in success probability. I think this paper represents the state of the art on this topic now.

Let's get into the technical details. The classical class in this paper is bPTC^0(k) for k = omega(log n), which is slight generalization of AC^0 (strictly larger, provably) but contained in TC^0. In bPTC^0(k), the circuit gets unbounded fan-in threshold gates which are arbitrary polynomials on inputs of Hamming weight <= k, and saturate to 1 above that threshold. Unbounded fan-in OR, for example, is in this class with k = 0. Conversely, for k = O(1), bPTC^0 = AC^0. This class appears to be a fairly recent idea, and one contribution of this paper is a tighter multi-switching lemma than what was previously known for this (or at least a very similar) complexity class.

The problem/non-local game that the main separation is built on has the same form as previous work: the Hamming weight of an output string should be determined modulo p by the Hamming weight of the input string. There are some complications from using qudits, like a non-uniform distribution of inputs and using quantum circuits outside the Clifford group, which subsequently require more work to make robust to noise.

Finally, the authors also make claims of a connection to neural networks, as complexity papers on threshold functions sometimes do. I find these entirely unconvincing, but whatever sells I guess. They also present resource estimates (Table I) for how many qudits would be required to demonstrate various levels of quantum advantage.

As I said before, I believe this paper represents the current state of the art on unconditional separations of quantum circuits from classical circuits. A lot of the ideas are recycled from earlier papers, but clearly significant technical work was necessary to put it all together. Finally, I'm sure it was decently written at some point, but the appendicization of this paper has not been artfully done. The authors list all these things about their main problem has --- it's a search problem, it involves high dimension qudits but it's over binary inputs, but the input distribution is/isn't uniform --- without ever actually defining their problem, not even implicitly by a quantum circuit that solves it.

Typos and corrections:
-- Missing citations starting in Table I. I counted 12 of them across both files. Always search for "??" in your final submission before you hit the button. That goes for the arXiv version too.
-- Line 67-70: "While certain quantum advantages offer computational benefits for parallel computations, these are relatively modest and largely pertain to classical circuit classes with limited practical applications." I'm struggling to understand what this sentence is supposed to mean.
-- Line 124-125: You've got two R's typeset differently in the same sentence.
-- Lines 234-237: "Additionally, it sidesteps the task of computing explicit success probability bounds for each game, while still achieving comparable separations." Again, I'm struggling to guess what was meant.
-- In Theorem 1 and 2, the problem is called \mathcal{R}. In Theorem 3, it's \mathfrak{R}. Are they actually different? Neither of them are properly defined in the main file (abstract?) so it's hard to say.
-- 707: "multi-swithching"
-- Supplement: "abritary" appears twice
-- [15] cites F. Gall and [63] cites F. Le Gall. I believe the latter is correct.
-- [26] and [81] contain complexity classes in the title which should be handled more carefully

Version 1:

Reviewer comments:

Reviewer #1

(Remarks to the Author)
Thanks to the authors for addressing my confusions, clarifying a few more subtle points, and making the recommended changes. The manuscript has improved following the rebuttal.

Reviewer #2

(Remarks to the Author)
I thank the authors for addressing my comments. I believe it has improved the paper and can now recommend accepting the paper.

Reply to Referee 1

We sincerely thank the referee for taking the time to review our manuscript and provide a detailed referee report. We have carefully read your comments, and we are glad that you have a positive impression of our work. Considering the suggestions you have noted, we have revised our manuscript appropriately. Thank you for triggering this revision and enabling us to significantly improve the presentation of our manuscript. Below, we present a point-by-point response addressing all the comments (quoted in blue, italicised text) raised in your report. We also adjoin the relevant edits we have made in the revised manuscript using green fonts below.

> *Noteworthy Results:*
>
> ** This work unconditionally demonstrates that parallel quantum computation can exhibit greater computational power than previously believed/recognize.*
>
> ** In particular, they show that there are certain problems solvable in QNC^0 (constant-depth quantum circuits with local gates), which are not solvable in poly-sized biased-PTC0 (i.e. $\mathsf{bPTC}^0(k)$).*
>
> ** They identify a family of problems solvable by a constant-depth universal quantum computation over prime qudits (which are experimentally of interest because they appear to be more robust to noise) with bounded connectivity which is hard for poly-sized biased TC^0.*
>
> ** They bridge high-dimensional non-local games with computational advantage on practically relevant/attainable architectures.*
>
> ** They further show that the quantum advantages are robust to noise, making them even more practically plausible.*

Thank you for summarising our contribution as a clear extension of the understanding of the power of parallel quantum computations. We are glad that you highlight our work beyond the standard qubit setting, and the consideration of noise, which makes our results more relevant to near-term experiments.

> *Significance to the field:*
>
> *I enjoyed reading this paper and learned quite a bit about the unconditional quantum advantage literature. The paper does a good job of presenting novel, interesting theoretical results, while also motivating them very well from an experimental perspective - proving their robustness to noise and compatibility with current architectures. Therefore, the paper will be of interest to experimentalists in addition to theorists. In addition to the impact of the work - expanding the circuit class size for which unconditional quantum advantage exists - the work has a lot of technical novelty, introducing many new techniques (for example, novel qubit to qudit mappings/proofs and a new switching lemma for bPTC^0 circuits) that I believe will be of great interest/use for theorists working on related problems. Overall, the work is a very rigorous, comprehensive study of the proposal (studying, for example, robustness to noise and providing detailed resource estimates), offering justification for all the results/proofs and motivating them in comparison to the prior work. Overall, I think the paper makes many novel contributions, both technical and conceptual, and will be appealing to both the theory and experimental communities.*

We appreciate your recognition of the novelty of our conceptual and technical contributions and their relevance to both theoretical and experimental researchers. It is also a pleasure to us that you have appreciated our efforts to clearly motivate our results, establish strong connections to prior work, and ensure the technical robustness of our approach.

Comparison to established literature:

** Prior to this work, the largest classical circuit class for which unconditional quantum advantage was established was AC^0. However, note that AC^0 is a subset of $\mathsf{bPTC}^0(k)$, for bias $k = O(1)$. However, for larger values of k, bPTC^0 contains circuits beyond AC^0. This work therefore expands the circuit classes for which unconditional quantum advantage exists.*

** Interestingly their bPTC^0 proposal also encompasses problems which likely lie outside of TC^0. Since neural network architectures, such as LLMs are contained in TC^0, this suggests that there might be novel neural net architectures that lie within the computational power of shallow-depth noisy quantum circuits.*

** Although they leverage non-local games, as has previously been done in the literature, they propose a new family of relational problems - ISMRP- which they show lies in QNC^0 and TC^0, but is strictly beyond bPTC^0.*

We are once again glad that the referee highlights our novel conceptual and technical contributions, in extending beyond the previous best unconditional classical-quantum separations. We are also happy to see interest in the classical circuit class we considered, and our definition and study of a new family of non-local games and relational problems used to establish the identified quantum advantage.

Here we would like to highlight a point in connection with the relation between neural network architectures and TC^0. As we have discussed in the manuscript, the expressivity of many important neural network architectures can be captured by TC^0 and this includes variants of the transformer architectures that form an important component of modern LLMs. Nevertheless, as we have further clarified in the revised manuscript, a full LLM may include more complex features such as feedback loops, which are not yet known to be simulatable using TC^0 circuits. However, as you have kindly noted, our work does suggest that there might be novel neural network architectures that lie within the computational power and expressivity of shallow-depth noisy quantum circuits, and we do believe that our results provide motivation and novel avenues for further work in this area.

** From the way the text is written on Lines 113-115, it is unclear if the authors are claiming to have proven the classical separation $\mathsf{NC}^0 \subsetneq \mathsf{AC}^0 \subsetneq \mathsf{bPTC}^0(k)$ for $k = \omega(\log n)$, or whether they are using this previously known fact to argue that the bPTC^0 circuit class is valuable in investigating quantum computational power. In the case of the former, they might want to make it more clear that they are actually proving this result (indicate where later in the paper/supplement this is shown). However, my impression is that it is the case of the latter - in which case, they should add citations to relevant prior works which showed these separations and also make it more explicit that they did not actually develop this hierarchy.*

We thank the referee for pointing out this potential point of confusion. As you have correctly inferred, we are relying on a previously established result that was not clearly stated in our submission. We have now clarified this by explicitly acknowledging that this separation between classical circuit classes was known beforehand and by citing the relevant reference. Please see our revised text below for the correction.

Revised text: Notably, even a single biased threshold gate with bias $k = \omega(\log n)$ is known to require Boolean circuits of superpolynomial size (i.e., $\Omega(n^{\mathrm{polylog}(n)})$) using unbounded fan-in AND, OR, and NOT gates to simulate it [Kum23]. □

** The literature review could potentially be improved/expanded by citing the growing body of literature focused on proving separations for famous classical computations,* *such as computing Parity, in quantum classes beyond* QNC^0*. For example, there has been a lot of exciting recent work on proving explicit bounds on the number of ancilla needed to implement Parity in* QAC^0 *(e.g. [Rosenthal'20], [NPVY'24], [ADOY'24]) - motivated by the "quantum fanout is powerful" result [HS'05]. There is also a recent related result establishing the power of quantum threshold [GM'24].*

We sincerely thank the referee for highlighting this exciting and relevant body of literature on shallow-depth quantum circuit classes. However, due to space constraints and limitations on the number of references in the main document, we have introduced these references in our supplementary material, where these circuit classes are discussed in greater detail to provide context and establish a connection to this body of work. Please see the following text that has been added. Additionally, we gently note that including these references in the main text could distract from our goal of maintaining a concise and focused introduction to unconditional classical-quantum circuit separations.

Revised text: Our primary focus is QNC^0, the class of constant-depth quantum circuits built from a universal and finite set, often regarded in the literature as the quantum analogue of NC^0. ... It is worth mentioning that QAC^0 and QTC^0, which are defined as the quantum analogs of AC^0 and TC^0, have also been actively studied, yielding novel and unexpected results when multi-qubit gates are included [HŠ05; NPV+24; Ros21; ADO+24; GM24]. However, our discussion in this paper will focus on quantum classes without unbounded fan-in multi-qubit gates. □

Suggestions for Improving the Manuscript:

** On line 59, you refer to "parallel" quantum computation, but I don't think it is previously defined or explained why the relevant surrounding text describes "parallel" quantum computation. I think you could put more emphasis in the introduction on defining what "parallel" means in both the classical and quantum setting and explaining its significance, since it is pretty important to the text.*

We thank the referee for this important suggestion and have now provided a concrete definition of the term "parallel" computation for the specific context of shallow-depth circuits. Please see our revised text below addressing this issue.

Revised text: This first *unconditional* separation between shallow-depth quantum and classical circuits sparked renewed interest in the field. It underscored the potential for significant computational and practical advantages in *parallel* quantum computations. In both classical and quantum computing, circuit width is a good measure of parallelism (e.g. the number of processors) and depth is a good measure of runtime, with constant-depth circuits capturing the computations that can be performed by a polynomial number of processors running for a constant amount of time. □

Potential Typos:

** Lines 24-25: "has quest the understanding if" - awkward/bad wording*

** Lines 191-192: "with the extend to which"- awkward/bad wording*

** Lines 267-271: I believe that there might be a grammatical typo or missing word (the sentence structure is strange and hard to follow)*

** Line 596: "realizating"* $->$ *"realization"?*

** Line 919: missing reference*

We sincerely thank the referee for reading our manuscript carefully and pointing out typos, grammatical errors and other issues in the presentation. Based on this useful feedback we have re-read and corrected the presentation across the main manuscript as well as the supplementary material, and we thank you for triggering this wide revision and the opportunity to improve our paper. All of our revisions are set in blue font in the resubmitted manuscript.

Finally, we sincerely thank the referee once again for their valuable feedback, and for recognizing the impact and innovation of our work.

References

[ADO+24] Anurag Anshu, Yangjing Dong, Fengning Ou, and Penghui Yao. *On the computational power of* QAC^0 *with barely superlinear ancillae*, 2024. arXiv: 2410.06499.

[GM24] Daniel Grier and Jackson Morris. *Quantum threshold is powerful*, 2024. arXiv: 2411.04953.

[HŠ05] Peter Høyer and Robert Špalek. "Quantum fan-out is powerful". *Theory of Computing*, 1(5):81–103, 2005.

[Kum23] Vinayak M. Kumar. "Tight correlation bounds for circuits between AC^0 and TC^0". *Proceedings of the Conference on Proceedings of the 38th Computational Complexity Conference*, CCC '23, Warwick, United Kingdom. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2023.

[NPV+24] Shivam Nadimpalli, Natalie Parham, Francisca Vasconcelos, and Henry Yuen. "On the pauli spectrum of qac0". *Proceedings of the 56th Annual ACM Symposium on Theory of Computing*, STOC 2024, pages 1498–1506, Vancouver, BC, Canada. Association for Computing Machinery, 2024.

[Ros21] Gregory Rosenthal. "Bounds on the QAC^0 complexity of approximating parity". James R. Lee, editor, *12th Innovations in Theoretical Computer Science Conference (ITCS 2021)*, volume 185 of *Leibniz International Proceedings in Informatics (LIPIcs)*, 32:1–32:20, Dagstuhl, Germany. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2021.

Reply to Referee 2

We sincerely thank the referee for taking the time to review our manuscript and provide a detailed referee report. We have carefully read your comments, and appreciate your useful and constructive feedback. Considering the suggestions you have noted, we have revised our manuscript appropriately. Thank you for triggering this revision and enabling us to significantly improve the presentation of our manuscript. Below, we present a point-by-point response addressing all the comments (quoted in blue, italicised text) raised in your report. We also adjoin the relevant edits we have made in the revised manuscript using green fonts below.

> *The paper extends existing unconditional quantum advantage results to show that constant-depth noisy qudit circuits can beat constant-depth threshold circuits. Existing work had separated constant-depth quantum circuits (QNC^0) from constant-depth classical circuits with unbounded fan-in gates (AC^0). This work is similar, but against a slightly larger class of classical circuits, while maintaining noise robustness of the quantum circuit and an exponential separation in success probability. I think this paper represents the state of the art on this topic now.*

We thank the referee for recognizing that our results improve upon the previous largest unconditional quantum-classical separation in the constant-depth circuit setting by considering a larger classical circuit class that models the power of threshold circuits. We appreciate the acknowledgment that our results represent the state of the art in this line of research.

> *Let's get into the technical details. The classical class in this paper is $\mathsf{bPTC}^0(k)$ for $k = \omega(\log n)$, which is slight generalization of AC^0 (strictly larger, provably) but contained in TC^0. In $\mathsf{bPTC}^0(k)$, the circuit gets unbounded fan-in threshold gates which are arbitrary polynomials on inputs of Hamming weight <= k, and saturate to 1 above that threshold. Unbounded fan-in OR, for example, is in this class with $k = 0$. Conversely, for $k = O(1)$, $\mathsf{bPTC}^0 = \mathsf{AC}^0$.*

We appreciate the referee's technical summary and largely agree with the contextualization of our results within the (evolving) landscape of circuit complexity classes. However, we would like to add that since AC^0 circuits of super-polynomial size are required to simulate even a *single gate* from most of those allowed in $\mathsf{bPTC}^0(\mathsf{k})$ for super-logarithmic values of the bias, $\mathsf{bPTC}^0(\mathsf{k})$ for $k = \omega(\log n)$ is a strict generalization of AC^0 and represents a family of circuit classes that are progressively significantly larger than AC^0; indeed, for bias values of order $n^{1/5d}$, much larger—*sub-exponential* size—AC^0 circuits are required to simulate most individual biased threshold gates. In both of our preceding statements the word "most" can be made mathematically precise in the sense that our assertion holds with high probability for a random gate drawn from the $\mathsf{bPTC}^0(\mathsf{k})$ gate set. This illustrates the strength of the separation results that we prove. We reiterate that our results are obtained even when saturating the bias parameter for the significantly larger values of k scaling polynomially in n, up to order $n^{1/5d}$, beyond which values small $\mathsf{bPTC}^0(\mathsf{k})$ circuits can easily solve the ISMR problems. We have made this clearer in the revised manuscript.

This result was already established in prior work, and to ensure this distinction is clear, we have now explicitly added the following text to the manuscript:

Revised text: Notably, even a single biased threshold gate with bias $k = \omega(\log n)$ is known to require Boolean circuits of superpolynomial size (i.e., $\Omega(n^{\mathrm{polylog}(n)})$) using unbounded fan-in AND, OR, and NOT gates to simulate it [Kum23]. □

This class appears to be a fairly recent idea, and one contribution of this paper is a tighter multi-switching lemma than what was previously known for this (or at least a very similar) complexity class.

We again acknowledge the referee's recognition of our technical contribution in developing a tighter multi-switching lemma. However, we would like to highlight that our main contribution is in fact a *multi-output* multi-switching lemma of which the tighter multi-switching lemma is a corollary. Multi-output multi-switching lemmas must be specifically constructed for each circuit class (in case it admits it), and this did not exist in prior work for $\mathsf{bPTC}^0(k)$. This is crucial because locality ensures that (via lightcone arguments) QNC^0 cannot be separated from NC^0 for decision/single-bit-output problems, and quantum advantages only manifest in the multi-output setting. In other words, previously known single-output multi-switching lemmas alone are insufficient to establish any separation between the considered circuit classes, even if they were tighter.

We noticed some inconsistencies in how we referred to our multi-output multi-switching lemma and have revised relevant passages, such as the following one, to clearly reflect this distinction and align with our clarification above: "Our approach introduces a novel multi-output multi-switching technique that serves as a reduction tool, breaking down multi-output biased polynomial threshold circuits into simpler classical computational models".

We also thank the referee for acknowledging the conceptual interest and novelty of comparing the relatively new family of circuit classes $\mathsf{bPTC}^0(k)$ to quantum circuits.

The problem/non-local game that the main separation is built on has the same form as previous work: the Hamming weight of an output string should be determined modulo p by the Hamming weight of the input string. There are some complications from using qudits, like a non-uniform distribution of inputs and using quantum circuits outside the Clifford group, which subsequently require more work to make robust to noise.

Again, we appreciate the referee's correct interpretation of our technical contributions. We emphasize that, while our definition of ISMR problems is inspired by the parity halving problem (for p=2, i.e. qubits) and corresponding non-local game from prior work, it is one of several possible extensions. We justify this particular extension based on its natural definition and useful properties that enable our results.

As the referee notes, our approach requires a range of non-trivial technical extensions to prior work, which are significant and substantial. Previous results resorted to an established separation between the optimal classical and quantum correlations in specific multi-party non-local games. In contrast, we define an entire infinite family of such games and explicitly prove the differences between optimal quantum and classical strategies. Additionally, as the referee notes, we address a key challenge: these non-local games are naturally defined for non-binary inputs, an issue that only arises when one considers the extension to prime qudit dimensions larger than 2. Without additional work to establish suitable mappings between p-dimensional and binary alphabets and associated transformations of the input distributions and so on, a fair assessment of the computational capacity of classical Boolean circuits vis-à-vis qudit quantum circuits would not be possible. Our work provides the necessary transformations to analyze them in the binary setting, ensuring a meaningful comparison even in the context of average-case hardness.

Furthermore, the need for non-Clifford gates to achieve noise robustness posed a fundamental and considerable challenge. Standard magic state teleportation gadgets are inadequate in this case, as adaptive corrections are unavailable in the constant-depth setting. Instead, we had to analyze the specific structure of the problem to derive an alternative equivalent gadget that operates without adaptive corrections. We also reiterate that our generalization of the approach to prime qudit dimensions involves extensive technical developments, as previous results had not established whether such an extension was possible. In particular, we highlight our single-shot state preparation for higher-dimensional Bell pairs (GHZ_2 states), which plays a crucial role in our proofs.

Finally, the authors also make claims of a connection to neural networks, as complexity papers on threshold functions sometimes do. I find these entirely unconvincing, but whatever sells I guess. They also present resource estimates (Table I) for how many qudits would be required to demonstrate various levels of quantum advantage.

We appreciate that the referee highlights our improved resource estimates for experimental demonstrations of quantum advantage. Regarding the connection to neural networks, we emphasize that we have been careful in discussing only connections that have been well-received in *both* the computational complexity theory and neural network communities. Moreover, we only cite well-established, peer-reviewed references with formal mathematical proofs describing these connections, which are primarily concerned with capturing the expressivity of certain classes of neural network architectures in terms of circuit complexity classes such as AC^0 and TC^0.

Nevertheless, we have taken this opportunity to revise the text regarding the connection to neural networks in our manuscript, to dispel confusions that we were able to anticipate and address the suggestion of reducing the space and emphasis devoted to this discussion. We would like to point out that AC^0 and TC^0 circuits capture neural networks in the constant-depth setting and not more complex architectures, which could for instance include feedback loops—a potential source of confusion. We have addressed this concern by further clarifying the precise mathematical settings in which the connection is valid. We have removed speculative connections, either by omitting them entirely or by moving them to the discussion section and clearly phrasing them as mathematical conjectures. Additionally, to avoid over-representing the neural network connection, we have reduced its overall emphasis throughout the text.

We believe this is a natural connection and motivation to study the classical circuit classes we have analyzed, and an enriching component of the manuscript for both the classical and quantum communities working on related topics, therefore of considerable interest to the wide readership of Nature Communications (as also hinted by Referee 1).

As I said before, I believe this paper represents the current state of the art on unconditional separations of quantum circuits from classical circuits. A lot of the ideas are recycled from earlier papers, but clearly significant technical work was necessary to put it all together.

We sincerely thank the referee for recognizing that our work represents the state of the art in unconditional separations of quantum circuits from classical circuits. We also appreciate the acknowledgment that significant technical development in conjunction with a synthesis of techniques from a wide variety of past work was required to achieve our results.

Finally, I'm sure it was decently written at some point, but the appendicization of this paper has not been artfully done.

– Missing citations starting in Table I. I counted 12 of them across both files. Always search for "??" in your final submission before you hit the button. That goes for the arXiv version too.

We thank the referee for pointing out the lapses in presentation, and the inconsistencies and missing references between the main text and the supplementary material. We have resolved all 12 missing links, and ensured that there are no further broken links as well. We have also introduced new additional references from the results sections to the methods and from the main manuscript to the supplementary material. This ensures that readers are correctly directed to further details when needed while improving consistency across all main and supplementary sections.

The authors list all these things about their main problem has — it's a search problem, it involves high dimension qudits but it's over binary inputs, but the input distribution *is/isn't uniform — without ever actually defining their problem, not even implicitly by a quantum circuit that solves it.*

– In Theorem 1 and 2, the problem is called $\mathcal{R}$. In Theorem 3, it's $\mathfrak{R}$. Are they actually different? Neither of them are properly defined in the main file (abstract?) so it's hard to say.

We thank the referee for pointing out that we missed out including a proper definition of our ISMR problems in the main text. We have now introduced an explicit definition in the background section, making the connection with our non-local games clearer as well. Also, this now provides the correct references for the relation problems in Theorems 1 and 2, which we have also rephrased based on the concrete relation problems now explicitly presented in the text. We reproduce the added text below.

Revised text: Finally, we focus on relational or search problems, where the inputs x are n-bit strings, and the outputs y are m-bit strings. Formally, we have valid input-output pairs $(x, y) \in \mathcal{R}$ for some relation $\mathcal{R} \subset \{0,1\}^n \times \{0,1\}^m$. As in previous results, these relations will have non-local games embedded into them. In this paper, we introduce the family of qudit XOR non-local games, designated Modular XOR games, described in Figure 3. Building on this class of multi-party non-local games, we introduce a corresponding family of relational problems, that we term Inverted Strict Modular Relation Problems (ISMRP). For any prime p, the ISMR problem $\mathcal{R}_p$ is defined as follows. Given an input $x \in \mathbb{F}_2^n$ such that $|x| \bmod p = 0$, the goal is to output a string from the set

$$\mathcal{R}_p(x) := \left\{ y \;\middle|\; y \in \mathbb{F}_2^m : \; |y| = -\left(\frac{|x|}{p}\right) \bmod p \right\}, \tag{1}$$

where $|z| = \sum_{i=1}^{n} z_i$ is the ℓ_1-norm for any string $z \in \mathbb{F}_p^m$, which is equal to the Hamming weight in the case of bitstrings. We typically choose the output length m to be slightly larger than n. □

We note that we did not include the circuit solving the relation problem in the main text due to space restrictions, but have added reference to the exact subsections of the supplementary material, where these circuits are explicitly explained and illustrated.

Finally, we have added the following text in the explanations following the theorem to provide the reader with an intuition of how the more complex search problems $\mathfrak{R}$ referenced in Theorem 3 are defined. Also, in the methods section, we now include a reference for the reader to the relevant subsection of the Supplementary Information with the full and formal definition of these problems.

Revised text: Additionally, as part of Theorem 3, we design new quantum circuits in the form of non-adaptive Clifford circuits with input-independent advice states to solve ISMR problems fault-tolerantly. These quantum circuits essentially give rise to our definition of the $\mathfrak{R}_p$ search problems □

Typos and corrections:

– Line 67-70: "While certain quantum advantages offer computational benefits for parallel computations, these are relatively modest and largely pertain to classical circuit classes with limited practical applications." I'm struggling to understand what this sentence is supposed to mean.

We thank the referee for pointing out this confusing phrasing. Our intention in this sentence was to highlight that while previously proven separations between constant-depth classical and quantum circuits are unconditional and intrinsically interesting, the largest classical circuit class against which they had been proven, viz. AC^0, is of limited practical applicability, although it has theoretical applications to certain algebraic problems for instance. Our goal is to clarify that demonstrating separations for larger circuit classes with greater practical relevance provides stronger evidence for the advantage and utility of quantum circuits, particularly those implementable on near-term devices, which is a central focus of research in the quantum computing community.

To improve clarity, we have rephrased the sentence as follows:

Revised text: While this prior work has established that parallel quantum computations can show advantages over comparable parallel classical computations, these advantages have only been demonstrated for classical circuit classes with limited practical applicability. □

– Lines 234-237: "Additionally, it sidesteps the task of computing explicit success probability bounds for each game, while still achieving comparable separations." Again, I'm struggling to guess what was meant.

We thank the referee for pointing out that this sentence was unclear. We have revised the text as follows, which we believe better conveys our intended ideas.

Revised text: Additionally, it avoids the need to compute explicit success probability bounds for each game. In particular, we show that for our family of games parameterized by a prime p, the correlation of any classical strategy with a winning answer decreases exponentially with the number of parties in the game (see Section IVA). This correlation decay alone is sufficient to achieve comparable separations. We thus sidestep the obstacle of explicitly computing bounds on winning *probabilities*: this has been emphasised in prior research, which predominantly relied on established quantum-classical distinctions in the winning probabilities for non-local games [BGK18; WKS+19]. Few developments beyond the conventional qubit setting were considered or achieved previously [Law17]. Finally, our search problems $\mathcal{R}_p$ remain binary, aligning naturally with Boolean circuits. They do not impose hardness by making clever use of arithmetic operations over other prime fields, making traditional Razborov-Smolensky type lower bounds inapplicable to this classical Boolean gate setting. □

– Line 124-125: You've got two R's typeset differently in the same sentence.

– 707: "multi-swithching"

– Supplement: "abritary" appears twice

– [15] cites F. Gall and [63] cites F. Le Gall. I believe the latter is correct.

– [26] and [81] contain complexity classes in the title which should be handled more carefully

We sincerely thank the referee for reading our manuscript carefully and pointing out typos, grammatical errors and other issues in the presentation. Based on this useful feedback we have re-read and corrected the presentation across the main manuscript, bibliography, and supplementary material. We thank the referee for triggering this wide revision and for the opportunity to improve our manuscript. All the revisions that we have made appear in blue font in the resubmitted manuscript.

Finally, we sincerely thank the referee once again for the valuable constructive feedback, which has helped us improve the quality and presentation of our manuscript.

References

[BGK18] Sergey Bravyi, David Gosset, and Robert König. "Quantum advantage with shallow circuits". *Science*, 362(6412):308–311, 2018.

[Kum23] Vinayak M. Kumar. "Tight correlation bounds for circuits between AC^0 and TC^0". *Proceedings of the Conference on Proceedings of the 38th Computational Complexity Conference*, CCC '23, Warwick, United Kingdom. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2023.

[Law17] Jay Lawrence. "Mermin inequalities for perfect correlations in many-qutrit systems". *Physical Review A*, 95(4):042123, 2017.

[WKS+19] Adam Bene Watts, Robin Kothari, Luke Schaeffer, and Avishay Tal. "Exponential separation between shallow quantum circuits and unbounded fan-in shallow classical circuits". *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*, pages 515–526. Association for Computing Machinery, 2019.