

Quantum Circuits surpass Biased Threshold Circuits in Constant-Depth

Min-Hsiu Hsieh ^{*} Leandro Mendes [†] Michael de Oliveira [‡]
Sathyawageeswar Subramanian [§]

Abstract

In this paper we study restricted classes of constant-depth threshold circuits recently introduced by [Kum23] as a family that generalizes AC^0 . Denoting these circuit families $bTC^0(k)$ for *biased threshold circuits* parameterised by an integer-valued bias k , we prove three hardness results separating these classes from constant-depth quantum circuits (QNC^0).

- We prove that the parity halving problem [WKS⁺19], which QNC^0 over qubits can solve with certainty, remains average-case hard for polynomial size $bTC^0(k)$ circuits for all $k = \mathcal{O}(n^{1/(5d)})$.
- We construct a new family of relation problems based on computing $\bmod p$ for each prime $p > 2$, and prove a separation of QNC^0 circuits over higher dimensional quantum systems ('qupits') against $bTC^0(k)$ for the same range of bias.

We also prove tighter lower bounds on the size of $bTC^0(k)$ circuits that are required to solve the relational problem with certainty, which we leverage to significantly reduce the estimated resource requirements for potential demonstrations of quantum advantage of this form.

$bTC^0(k)$ circuits can compute certain classes of Polynomial Threshold Functions (PTFs), which in turn serve as a natural model for neural networks and exhibit enhanced expressivity and computational capabilities. Furthermore, for large enough values of k , $bTC^0(k)$ contains TC^0 as a subclass. The main challenges arise in establishing the classical correlation lower bounds, and in designing non-local games with quantum-classical gaps in the winning probability in order to go beyond qubits to higher dimensions. We address the former challenge by developing new, tighter multi-switching lemmas for multi-output $bTC^0(k)$ circuits. We address the latter by analyzing a new family of non-local games defined in terms of $\bmod p$ computations, characterized by an exponential difference between their classical and quantum success probabilities. These technical tools may be of more general and independent interest.

Keywords. Quantum algorithms, Circuit complexity, Shallow-depth circuits, Non-local games, Resource Estimates.

1 Introduction

Realizing the theoretical gains promised by landmark quantum algorithms such as integer factorisation or search is challenged by the constraints of existing quantum hardware, requiring extensive resources and fault-tolerant operations for practical implementation. This challenge has shifted the focus towards the study of shallow-depth quantum circuits that can in principle be implemented on near term hardware. The seminal work of Bravyi et al. [BGK18] exhibited a relational problem that can be solved by constant-depth quantum circuits consisting only of 2-qubit Clifford gates, which no constant depth classical circuit with bounded fan-in gates can solve. This first *unconditional*, i.e. without any complexity theoretic assumptions, separation between QNC^0 and NC^0 spurred renewed interest in the field, and was followed by an extension of this result to a separation of QNC^0 against classical circuits of unbounded fan-in (AC^0) [WKS⁺19], average-case hardness [Gal19; WKS⁺19; CSV21], interactive protocols separating QNC^0 from classical logarithmic-depth circuits of bounded fan-in (NC^1) [GS20], the case of noisy quantum circuits requiring fault-tolerance and error correction [BGK⁺20; GJS21; CCK23], and sampling problems [WP23].

^{*}Hon Hai (Foxconn) Quantum Computing Research Center. Email: min-hsiu.hsieh@foxconn.com.

[†]Hon Hai (Foxconn) Quantum Computing Research Center. Email: leandro.rsm@foxconn.com.

[‡]International Iberian Nanotechnology Laboratory; LIP6, Sorbonne Universite. Email: michael.oliveira@inl.int.

[§]University of Cambridge. Email: ss2310@cam.ac.uk

A natural question that arises is whether quantum circuits of constant depth and fan-in can also perform tasks that classical constant-depth circuits of *threshold gates* cannot. Such threshold circuits form the class TC^0 , and are a canonical model for neural networks [SB91; MP69; Mur71]. Here we are faced with the frontier of classical theoretical computer science, where even cutting-edge circuit lower-bound techniques falter.

2 Background and context

In this paper we focus on constant-depth classical and quantum circuit classes with multiple output bits. In particular, our interest is in relational problems, wherein a circuit may map an n -bit input string to one of many possible valid m -bit output strings. We define QNC^0 to be the class of computational problems $R : \{0, 1\}^n \rightarrow \{0, 1\}^m$ solvable by quantum circuits with a constant depth using a polynomial number of gates of bounded fan-in (i.e. every gate has a fixed constant number of input and output wires) drawn from a finite, universal quantum gateset.

Our contributions start by comparing QNC^0 and a newly introduced classical circuit class [Kum23] that interpolates between AC^0 and beyond TC^0 through the use of an integer parameter k . More specifically, defining k -biased Polynomial Threshold Functions (PTFs) as boolean functions of the form

$$f(x) = \begin{cases} P(x), & \sum_{i=1}^n x_i \leq k; \\ 1, & \sum_{i=1}^n x_i > k \end{cases}; \quad \text{with } P : \mathbb{F}_2^n \rightarrow \mathbb{F}_2 \text{ a polynomial over } \mathbb{F}_2 = \{0, 1\}, \quad (2.1)$$

we set $\text{bTC}^0(k)$ to be the class of constant depth circuits composed of unbounded fan-in gates each of which may compute a k -biased PTF. k defines the activation region of the PTF or neuron. When $k = 0$, we recover unbounded fan-in AND and OR gates, and $\text{bTC}^0(0)$ corresponds to AC^0 .

3 Main results

Our first result is an unconditional separation between constant-depth quantum circuits and biased polynomial threshold circuits, both in the exact and average-case hardness scenarios.

Theorem 3.1 (Informal, see formal version in the full text.). *For every large enough input size $n \in \mathbb{N}$, there exists a relation $R \subset \{0, 1\}^n \times \{0, 1\}^m$ with $m = \mathcal{O}(n \log n)$ such that on input any $x \in \{0, 1\}^n$, a QNC^0 circuit consisting of only subquadratically many ($o(n^2)$) gates can output $y \in \{0, 1\}^m$ such that $(x, y) \in R$ with certainty. Conversely, the size s of any $\text{bTC}^0(k)/\text{rpoly}$ circuit of depth d that outputs any valid y is lower bounded as shown in the table below, for both exact solutions and for arbitrary success probabilities, in the context of average-case hardness. Here $/\text{rpoly}$ means the circuit is randomised, i.e. has access to polynomially many random input bits.*

$\text{bTC}^0(k)/\text{rpoly}$	$k = 0$ ($\equiv \text{AC}^0/\text{rpoly}$)	$k = n^{1/5d}$
Exact hardness	$s = \Omega \left(\exp \left(\left(\frac{\sqrt{n}}{(\log n)^{3/2 + \mathcal{O}(1)}} \right)^{\frac{1}{d-1}} \right) \right)$	$s = \Omega \left(\exp \left(\left(\frac{n^{3/10}}{(\log n)^{3/2 + \mathcal{O}(1)}} \right)^{\frac{1}{d-1}} \right) \right)$
Average-case hardness	-	$\Pr[\text{Success}] \leq \frac{1}{2} + \exp \left(-\Omega \left(\frac{n^{3/5 - \mathcal{O}(1)}}{(\log s)^{2d-1}} \right) \right)$

The standout consequence of theorem 3.1 is that $\text{bTC}^0(k)/\text{rpoly}$ with $k = \mathcal{O}(n^{1/d})$ requires superpolynomial size circuits to solve a relational problem that QNC^0 circuits solve efficiently. The class $\text{bTC}^0(k)/\text{rpoly}$ not only serves as a model for neural networks, but even a *single gate* of such a circuit (i.e. a single k -biased PTF), with $k = \text{polylog}(n)$, would also require superpolynomial (i.e. $\Omega(n^{\text{polylog}(n)})$) size AC^0 circuits to emulate it; hence $\text{AC}^0 \subsetneq \text{bTC}^0(k)$ for $k = \omega(\log n)$ [Kum23]. Notably, our results do achieve a super-polylogarithmic value for k —demonstrating that theorem 3.1 extends separations against AC^0 from prior work to genuinely new and larger circuit classes. Furthermore, we remark that it is the largest possible k for the type of relation problems considered—because for any

larger k , $\text{bTC}^0(k)$ can in fact solve the problem with high probability and small circuit size. This hints that we need completely new approaches in future work to improve our results.

The ‘exact case’ in theorem 3.1 refers to the scenario where we impose the $\text{bTC}^0(k)$ circuit to solve the problem with certainty, matching the performance of the quantum circuit. For $k = 0$, this case further yields us a new separation against AC^0/rpoly with the tightest bounds demonstrated yet.

Our second contribution is to extend all the foregoing results beyond qubits to higher dimensions.

Theorem 3.2 (Informal, see formal version in the full text.). *For every prime $p \in \mathbb{N}$, there exists a relation $\mathcal{R}_p : \mathbb{Z}_p^n \rightarrow \mathbb{Z}_p^m$ such there is a constant depth quantum circuit over $(\mathbb{C}^p)^{\otimes n}$ (i.e. n ‘qubits’) that has constant correlation with \mathcal{R}_p , but in contrast only has exponentially small correlation $\exp(-\mathcal{O}(n^{3/5}))$ with any polynomial size $\text{bTC}^0(n^{1/5d})$ circuit.*

Previous studies have suggested that non-local games with significant quantum-classical winning probability gaps could give rise to computational separations between quantum and classical circuit classes [Aas21]. However, such separations were not explicitly demonstrated. By proving theorem 3.2 we establish the existence of such a non-local game for each prime dimension and make use of them to explicitly construct relational problems and quantum circuits that solve them with high correlation. Our correlation measure is a generalisation of the usual correlation between Boolean functions to \mathbb{Z}_p , taking into account ‘how wrong’ an output is: if $R(x) = 2$, then $\tilde{R}(x) = 3$ should intuitively be a worse guess than $\tilde{R}(x) = 4$ (figure 5). These explicit separations not only clarify the theoretical landscape but also hold practical relevance, as many quantum computing platforms naturally operate in higher dimensions [RMP+22; GZC+22] offering promising avenues for demonstrating quantum advantage. In addition, we note that these non-local games might be of independent interest as they could be used in other quantum information processing tasks.

Resource estimation. In physical experiments that test this kind of unconditional separation, it is important to pin down at what values of depth d and width n (i.e. number of input qubits) we observe a transition in the circuit size; that is, at what depths and input sizes do the quantum advantages kick in?

We leverage our exact-case hardness bound in theorem 3.1 to provide such estimates, bringing theoretical predictions closer to the capabilities of current quantum devices. For context, the transition point for Shor’s algorithm is estimated to be $\sim 1,700$ qubits, 10^{36} Toffoli gates, and a circuit depth of 10^{25} [CFS24], while for the HHL algorithm it is roughly 10^8 qubits and a depth of 10^{29} [SVM+17]. Recent advancements in quantum hardware favors larger devices (i.e. more qubits) over those with prolonged coherence, and so there is a push towards shallower circuits [LJV+23; BEG+23]. Separations against NC^0 are the most viable for near-term quantum devices, plausible with only hundreds to thousands of qubits. The separation against AC^0 circuit under average-case conditions and 2D architectures in [WKS+19] could need roughly 10^{97} qubits to observe quantum advantage, diminishing its near-term feasibility. However, by bounding the constant factors, optimizing the parameters and considering all-to-all qubit connectivity, this requirement could drop to 10^{21} qubits with depth-3 quantum circuits. For $\text{bTC}^0(n^{1/5d})$ circuits, the requirement is 10^{40} qubits. Our exact hardness results demonstrate that circuits with 10^{11} and 10^{22} qubits at depth 3 can establish quantum advantages over AC^0 and $\text{bTC}^0(n^{1/5d})$ circuits respectively, significantly lowering circuit requirements and paving the way for a progression of quantum advantage experiments. Our estimates do not represent lower bounds, as better proof methods and parameter optimization remain possible.

Technical contributions. We develop a novel multi-switching lemma for $\text{bTC}^0(k)$ circuits (theorem 3.1) which we derive by inductive methods, as an application we prove depth reduction lemmas for relation-type problems. While we use these technical tools to prove our lower bounds in theorem 3.1, they could be of independent interest, as they apply to circuit models of neural networks with real-world applications involving string-to-string mappings.

Note that the essence of switching lemmas has remained unchanged since their introduction in the 80s, primarily addressing separations within the AC^0 class. The significance of our work is underscored

by the fact although Kumar’s introduction of a class between AC^0 and beyond TC^0 [Kum23] offered new possibilities, the switching lemmas in that paper are insufficient for relation-type problems, and in fact do not even yield separations between QNC^0 and AC^0 .


For our new exact-case hardness results in theorem 3.1, we start by reducing the initial bTC^0 circuit to m independent decision trees of depth d , each corresponding to an output bit. Our innovation is to consider all valid outcomes of the output bits in our candidate relational problem, described by Algebraic Normal Forms [Don14], and then lower bound the number of degree-two terms in this representation. We then limit the number of terms each local decision tree can generate, setting bounds on their expressivity and exact problem-solving ability, which reflects the capacity of the initial circuit to solve the problem exactly.

Finally, for all prime qudit dimensions, we constructively prove the existence of non-local games that classical strategies can solve, at best, with an exponentially lower success probability compared to their quantum counterparts. Our approach accommodates non-uniform input distributions and circumvents the intricate task of computing explicit bounds for each game while providing equivalent separations. This challenge is highlighted in previous studies, which relied on established quantum-classical separations in non-local games [BGK18; WKS⁺19], fundamental for the type of computational separations presented in this text and previous work in the average-case hardness setting. Additionally, very few extensions of the qubit case to higher dimensions were known before our work [Law17].

In our correctness proof of the candidate quantum circuit that solves the qudit relational problem, we have incorporated a technique to efficiently describe the support of standard measurement outcomes of local unitary (LU)-equivalent generalized (p -dimensional) GHZ states with a dependence on the phases (lemma 4.21). This allowed us to incorporate a correction function for the output string, and ascertain the success probability of the quantum circuits in an elegant manner.

4 Related work

In the table below, we present a comparison to some of the prior work on unconditional separations between classical and quantum circuit classes that we outlined in the introduction.

	Problem	Advantage against	Geometry	Higher dimensions	Average c. hardness	Noise resilience
[BGK18]	2D HLF	NC^0/rpoly	2D	\times	\times	\times
[WKS ⁺ 19]	PHP	AC^0/rpoly	2D	\times	\checkmark	\times
[BGK ⁺ 20]	MSP	NC^0/rpoly	1D	\times	\checkmark	\checkmark
[CCK23]	TELEP	AC^0/rpoly	1D	\times	\checkmark	\checkmark
Our work	ISM RP	$\text{bTC}^0(k)/\text{rpoly}$	2D, 3D, ...	\checkmark	\checkmark	

5 Outlook

Our work extends previously known results on unconditional shallow-depth circuit separations to larger classical circuit classes and higher dimensions (qupits), while also pointing out potential quantum advantage experiments. It naturally raises many interesting questions for further work. In particular, there are problems that $\text{bTC}^0(k)$ circuits for $k = n^{1/d}$ can solve but $\text{AC}^0[p]$ circuits cannot, such as MOD p operations over $n^{1/d}$ bits [Smo87]. This indicates the potential for establishing unconditional separations between QNC^0 circuits and $\text{AC}^0[p]$ for any prime p . Our results might simplify existing conditional results by eliminating the necessity for interactivity or advice in proving such separations.

Furthermore, our work achieves near-optimal separations concerning the circuit class considered using non-adaptive MBQC-type quantum circuits. This suggests that to attain larger separations, such as with TC^0 , we must either identify harder problems solvable in this setting or consider more advanced QNC^0 circuits, such as constant-depth adaptive MBQC circuits [BKM⁺24].

Additionally, we highlight the potential of investigating novel higher-dimensional error-correcting codes (i.e., beyond the qubit case) [ABC⁺14] to understand the noise resilience of theorem 3.2.

References

- [Aas21] Sivert Aasnæss. *Comparing two cohomological obstructions for contextuality, and a generalised construction of quantum advantage with shallow circuits*. PhD thesis, University of Oxford, Oxford, UK, 2021 (page 3).
- [ABC⁺14] Hussain Anwar, Benjamin J Brown, Earl T Campbell, and Dan E Browne. “Fast decoders for qudit topological codes”. *New Journal of Physics*, 16(6):063038, 2014 (page 4).
- [BEG⁺23] Dolev Bluvstein, Simon J Evered, Alexandra A Geim, Sophie H Li, Hengyun Zhou, Tom Manovitz, Sepehr Ebadi, Madelyn Cain, Marcin Kalinowski, Dominik Hangleiter, et al. “Logical quantum processor based on reconfigurable atom arrays”. *Nature*:1–3, 2023 (page 3).
- [BGK⁺20] Sergey Bravyi, David Gosset, Robert Koenig, and Marco Tomamichel. “Quantum advantage with noisy shallow circuits”. *Nature Physics*, 16(10):1040–1045, 2020 (pages 1, 4).
- [BGK18] Sergey Bravyi, David Gosset, and Robert König. “Quantum advantage with shallow circuits”. *Science*, 362(6412):308–311, 2018. eprint: <https://www.science.org/doi/pdf/10.1126/science.aar3106> (pages 1, 4).
- [BKM⁺24] Alex Bredariol Grilo, Elham Kashefi, Damian Markham, and Michael de Oliveira. “The power of shallow-depth Toffoli and qudit quantum circuits”. *arXiv e-prints*:arXiv:2404.18104, arXiv:2404.18104, April 2024. arXiv: [2404.18104 \[quant-ph\]](https://arxiv.org/abs/2404.18104) (page 4).
- [CCK23] Libor Caha, Xavier Coiteux-Roy, and Robert Koenig. “A colossal advantage: 3d-local noisy shallow quantum circuits defeat unbounded fan-in classical circuits”. *arXiv preprint arXiv:2312.09209*, 2023 (pages 1, 4).
- [CFS24] Clémence Chevignard, Pierre-Alain Fouque, and André Schrottenloher. “Reducing the number of qubits in quantum factoring”. *Cryptology ePrint Archive*, 2024 (page 3).
- [CSV21] Matthew Coudron, Jalex Stark, and Thomas Vidick. “Trading locality for time: certifiable randomness from low-depth circuits”. *Communications in mathematical physics*, 382:49–86, 2021 (page 1).
- [Don14] Ryan O’ Donnell. *Analysis of boolean functions*. Cambridge University Press, 2014 (page 4).
- [Gal19] François Le Gall. “Average-case quantum advantage with shallow circuits”. *34th Computational Complexity Conference (CCC 2019)*. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2019 (page 1).
- [GZC⁺22] Daniel González-Cuadra, Torsten V. Zache, Jose Carrasco, Barbara Kraus, and Peter Zoller. “Hardware efficient quantum simulation of non-abelian gauge theories with qudits on rydberg platforms”. *Phys. Rev. Lett.*, 129:160501, 16, 2022 (page 3).
- [GJS21] Daniel Grier, Nathan Ju, and Luke Schaeffer. “Interactive quantum advantage with noisy, shallow clifford circuits”. *arXiv preprint arXiv:2102.06833*, 2021 (page 1).
- [GS20] Daniel Grier and Luke Schaeffer. “Interactive shallow clifford circuits: quantum advantage against nc^1 and beyond”. *Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2020, pages 875–888, Chicago, IL, USA. Association for Computing Machinery, 2020 (page 1).
- [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 (pages 1, 2, 4).
- [Law17] Jay Lawrence. “Mermin inequalities for perfect correlations in many-qudit systems”. *Physical Review A*, 95(4):042123, 2017 (page 4).

- [LJV⁺23] Thomas Lubinski, Sonika Johri, Paul Varosy, Jeremiah Coleman, Luning Zhao, Jason Necaie, Charles H Baldwin, Karl Mayer, and Timothy Proctor. “Application-oriented performance benchmarks for quantum computing”. *IEEE Transactions on Quantum Engineering*, 2023 (page 3).
- [MP69] Marvin Minsky and Seymour Papert. “An introduction to computational geometry”. *Cambridge tiass., HIT*, 479(480):104, 1969 (page 2).
- [Mur71] Saburo Muroga. “Threshold logic and its applications”, 1971 (page 2).
- [RMP⁺22] Martin Ringbauer, Michael Meth, Lukas Postler, Roman Stricker, Rainer Blatt, Philipp Schindler, and Thomas Monz. “A universal qudit quantum processor with trapped ions”. *Nature Physics*, 18(9):1053–1057, 2022 (page 3).
- [SVM⁺17] Artur Scherer, Benoit Valiron, Siun-Chuon Mau, Scott Alexander, Eric Van den Berg, and Thomas E Chapuran. “Concrete resource analysis of the quantum linear-system algorithm used to compute the electromagnetic scattering cross section of a 2d target”. *Quantum Information Processing*, 16:1–65, 2017 (page 3).
- [SB91] Kai-Yeung Siu and Jehoshua Bruck. “On the power of threshold circuits with small weights”. *SIAM Journal on Discrete Mathematics*, 4(3):423–435, 1991 (page 2).
- [Smo87] R. Smolensky. “Algebraic methods in the theory of lower bounds for boolean circuit complexity”. *Proceedings of the Nineteenth Annual ACM Symposium on Theory of Computing*, STOC ’87, pages 77–82, New York, New York, USA. Association for Computing Machinery, 1987 (page 4).
- [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 (pages 1, 3, 4).
- [WP23] Adam Bene Watts and Natalie Parham. “Unconditional quantum advantage for sampling with shallow circuits”. *arXiv preprint arXiv:2301.00995*, 2023 (page 1).