

A Geometric Approach to Quantum Circuit Complexity

Research Proposal for DPhil in Computer Science
Word Count: 974

Yuhao Han

December 2, 2025

1 Background and Motivation

One of the most important tasks in the theory of computation is to determine what problems can be solved efficiently [19]. The consensus is that a problem, with input of n bits, can be solved efficiently if there exists an algorithm that can solve it in $S(n)$ steps, where $S(n)$ is bounded by a polynomial. Such problems belong to the \mathbf{P} complexity class [7].

An interpretation of the Extended Church-Turing thesis [26] states if a problem is not in \mathbf{P} , there exists no physically realisable machine whatsoever in the Universe that can solve it efficiently. This idea is profound, philosophical, and consequential. Importantly, recent advancements in quantum computation have challenged this view [8, 19]. Some quantum algorithms, including the Deutsch-Jozsa algorithm [9], quantum searching [13], and the Shor's algorithm for factoring [24], have been found to provide exponential or polynomial speedup over the best-known classical algorithms. These demonstrations of quantum computers' ability to outperform classical computers are called *quantum supremacy* [22]. Even physical realisations of quantum supremacy have been achieved in the task of quantum random circuit sampling [2].

These discoveries are promising, but they are far from practical. Designing robust quantum algorithms is extremely difficult due to the abstract nature of quantum mechanics. Many frameworks, to explain quantum algorithms and to aid their designs, have been developed, such as tensor-network methods [19], ZX calculus [15], and quantum information theory [1]. Here, I propose a geometric approach to quantum algorithms inspired by Nielsen's work [10, 20].

2 A Geometric Approach to Quantum Algorithms

Physical implementations of quantum computers use a set of universal gates, whose combinations can approximate any unitary operation with arbitrary precision [19]. The problem is, given a set of universal gates, what is the most efficient way to approximate any operation? This problem is difficult, and Nielsen presented the following approach [10, 18, 20].

Given an operator $U \in SU(2^n)$, suppose it is generated by Hamiltonian $H(t)$ satisfying the Schrödinger equation $\frac{dU}{dt} = -iHU$, with the requirement that $U(t_f) = U$. $H(t)$ has a Pauli operator expansion $H = \sum_{\sigma} h_{\sigma}\sigma + \sum_{\tau} h_{\tau}\tau$, where σ ranges over one and two body interactions, τ ranges over 3 or more body interactions, and h_{σ}, h_{τ} are real numbers. By

choosing a penalty, p , a cost function can be defined as

$$F(H) = \sqrt{\sum_{\sigma} h_{\sigma}^2 + p^2 \sum_{\tau} h_{\tau}^2}$$

The length of the path, $U(t) : [0, t_f] \rightarrow SU(2^n)$, with $U(0) = I$ and $U(t_f) = U$ is defined as

$$\int_0^{t_f} dt F(H(t))$$

$F(H)$ can be regarded as the norm associated with the metric on $SU(2^n)$ whose components are

$$g_{\sigma\tau} = \begin{cases} 0 & \text{if } \sigma \neq \tau \\ 1 & \text{if } \sigma = \tau \text{ is one or two-body interactions} \\ p^2 & \text{otherwise} \end{cases}$$

Let $d(I, U)$ denote the length of the minimal geodesic given by this metric between I and U . Nielsen showed that for any $U \in SU(2^n)$, $d(I, U)$, upto a constant, gives a lower bound to the number of one or two-body gates to precisely generate U [18]. He also showed that any U can be approximated with $d(I, U)$ number of gates with arbitrary precision upto a polynomial factor [20].

While these results are powerful, finding the minimal geodesic is difficult. Nielsen has pointed out according to the Razborov-Rudich theorem [23], if a classical pseudorandom generator exists, finding the minimal geodesic on $SU(2^n)$ is classically intractable [10].

I propose to consider the following question: *Is there a general method to find the minimal geodesic on a reduction of $SU(2^n)$ connecting I and U , either analytically or numerically?* By reduction, I mean

1. We may consider a small system with two or three qubits, or choose a special U that will reduce the difficulty of finding geodesics. If an analytical solution is difficult, an approximation by numerical method is definitely plausible. Investigations of geometry of one-qubit system has been done previously [4].
2. We may quotient $SU(2^n)$ by a subgroup of symmetry. One candidate for symmetry is permutation. Its plausibility is strengthened by recent research on permutation invariant quantum circuit [17] and the fact that reordering of qubits shall have no physical effects on quantum computers.
3. Since we are mostly interested in algorithms that exhibit quantum supremacy, we may reduce $SU(2^n)$ by quotienting the Clifford group. It is well known that elements of Clifford group can be simulated efficiently on classical computers [11, 12]. Since Clifford group is a Lie subgroup which fits into our theory nicely, our geometric method may reveal additional insights about the origin of quantum supremacy.

If the minimal geodesic has been found, Nielsen's results show that it gives a lower bound for quantum complexity. I further ask: *is it possible to construct the minimal circuit to generate U , given the minimal geodesic $d(I, U)$?* Nielsen has hinted its possibility, without any further investigations [20].

This project will mostly rely on tools from differential geometry, Lie groups, and quantum information theory. Since an explicit metric on $SU(2^n)$ has been constructed, we follow the approach of General Relativity by studying connections, Christoffel symbols, and geodesic differential equation, similar to those used by Nielsen [20]. We will also

follow the modern approach to Clifford algebra [16]. Since $SU(2^n)$ has rich algebraic properties, we may also use modern computer algebra tools to aid our investigation, including Macaulay 2 and Lean. Besides these, we will also apply numerical simulations in Python, C++, or Rust.

3 Proposed Supervisor and Conclusion

I identify Dr Sathya Subramanian as my potential supervisor. His research on rigorous mathematical aspects of quantum systems, quantum algorithms and complexity theory [21, 14, 3], quantum catalytic space [5], and quantum information [25, 6, 27] are closely related to my interest, and my proposed research will be a direct continuation of some of his works.

Previously at Edinburgh, I had conducted algebraic geometry research on hypertoric varieties and Linux kernel research on computer-expressed link. Currently, I am collaborating on a deep learning paper on unifying supervised and unsupervised learning via free energy principle, which is relevant to my proposed research project via quantum information theory. Quantum computation is an interdisciplinary subject connecting pure mathematics, physics, and computer science. Therefore, my background in pure mathematics, practical skills in programming, and past research experience will make me a good fit.

My reasons for applying to DPhil at Oxford to study quantum computation are three-fold. Firstly, I find quantum computation an extremely interesting subject, combining the abstract structural beauty of mathematics with practical applications to solve consequential real-world problems. Secondly, Dr Subramanian’s expertise closely fits my interest, and it would be my pleasure to study under his supervision. Lastly, as a current Oxford student, I greatly enjoy Oxford’s academic environment and its resources that facilitate research, and I would like to continue my study at Oxford.

References

- [1] In: *Quantum Information Theory*. Cambridge University Press, Nov. 2016, pp. xi–xii. DOI: [10.1017/9781316809976.001](https://doi.org/10.1017/9781316809976.001). URL: <http://dx.doi.org/10.1017/9781316809976.001>.
- [2] F. Arute et al. “Quantum supremacy using a programmable superconducting processor”. In: *Nature* 574 (2019), pp. 505–510. DOI: <https://doi.org/10.1038/s41586-019-1666-5>.
- [3] Vahid R. Asadi et al. “Quantum Worst-Case to Average-Case Reductions for All Linear Problems”. In: *Proceedings of the 2024 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pp. 2535–2567. DOI: [10.1137/1.9781611977912.90](https://doi.org/10.1137/1.9781611977912.90). eprint: <https://epubs.siam.org/doi/pdf/10.1137/1.9781611977912.90>. URL: <https://epubs.siam.org/doi/abs/10.1137/1.9781611977912.90>.
- [4] Adam R. Brown and Leonard Susskind. “Complexity geometry of a single qubit”. In: *Physical Review D* 100.4 (Aug. 2019). ISSN: 2470-0029. DOI: [10.1103/PhysRevD.100.046020](https://doi.org/10.1103/PhysRevD.100.046020). URL: <http://dx.doi.org/10.1103/PhysRevD.100.046020>.
- [5] Harry Buhrman et al. *Quantum Catalytic Space*. 2025. arXiv: [2506.16324](https://arxiv.org/abs/2506.16324) [quant-ph]. URL: <https://arxiv.org/abs/2506.16324>.

- [6] Matthias C Caro et al. “Information-theoretic generalization bounds for learning from quantum data”. In: *The Thirty Seventh Annual Conference on Learning Theory*. PMLR. 2024, pp. 775–839.
- [7] Stephen A Cook. “The complexity of theorem-proving procedures”. In: *Logic, automata, and computational complexity: The works of Stephen A. Cook*. 2023, pp. 143–152.
- [8] David Deutsch. “Quantum theory, the Church–Turing principle and the universal quantum computer”. In: *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences* 400.1818 (1985), pp. 97–117. DOI: [10.1098/rspa.1985.0070](https://doi.org/10.1098/rspa.1985.0070). eprint: <https://royalsocietypublishing.org/doi/pdf/10.1098/rspa.1985.0070>. URL: <https://royalsocietypublishing.org/doi/abs/10.1098/rspa.1985.0070>.
- [9] David Deutsch and Richard Jozsa. “Rapid solution of problems by quantum computation”. In: *Proceedings of the Royal Society of London. Series A: Mathematical and Physical Sciences* 439.1907 (1992), pp. 553–558. DOI: [10.1098/rspa.1992.0167](https://doi.org/10.1098/rspa.1992.0167). eprint: <https://royalsocietypublishing.org/doi/pdf/10.1098/rspa.1992.0167>. URL: <https://royalsocietypublishing.org/doi/abs/10.1098/rspa.1992.0167>.
- [10] Mark R. Dowling and Michael A. Nielsen. *The geometry of quantum computation*. 2006. arXiv: [quant-ph/0701004](https://arxiv.org/abs/quant-ph/0701004) [quant-ph]. URL: <https://arxiv.org/abs/quant-ph/0701004>.
- [11] Daniel Gottesman. *Stabilizer Codes and Quantum Error Correction*. 1997. arXiv: [quant-ph/9705052](https://arxiv.org/abs/quant-ph/9705052) [quant-ph]. URL: <https://arxiv.org/abs/quant-ph/9705052>.
- [12] Daniel Gottesman. *The Heisenberg Representation of Quantum Computers*. 1998. arXiv: [quant-ph/9807006](https://arxiv.org/abs/quant-ph/9807006) [quant-ph]. URL: <https://arxiv.org/abs/quant-ph/9807006>.
- [13] 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. Philadelphia, Pennsylvania, USA: Association for Computing Machinery, 1996, pp. 212–219. ISBN: 0897917855. DOI: [10.1145/237814.237866](https://doi.org/10.1145/237814.237866). URL: <https://doi.org/10.1145/237814.237866>.
- [14] Christian Ikenmeyer and Sathyawageeswar Subramanian. “Kronecker Coefficients in BQP”. In: *ACM Transactions on Quantum Computing* 6.4 (2025). DOI: [10.1145/3762673](https://doi.org/10.1145/3762673). URL: <https://doi.org/10.1145/3762673>.
- [15] Aleks Kissinger and John van de Wetering. *Picturing Quantum Software: An Introduction to the ZX-Calculus and Quantum Compilation*. Preprint, 2024.
- [16] Douglas Lundholm and Lars Svensson. *Clifford algebra, geometric algebra, and applications*. 2009. arXiv: [0907.5356](https://arxiv.org/abs/0907.5356) [math-ph]. URL: <https://arxiv.org/abs/0907.5356>.
- [17] Maximilian Balthasar Mansky et al. *Permutation-invariant quantum circuits*. 2023. arXiv: [2312.14909](https://arxiv.org/abs/2312.14909) [quant-ph]. URL: <https://arxiv.org/abs/2312.14909>.
- [18] Michael A. Nielsen. *A geometric approach to quantum circuit lower bounds*. 2005. arXiv: [quant-ph/0502070](https://arxiv.org/abs/quant-ph/0502070) [quant-ph]. URL: <https://arxiv.org/abs/quant-ph/0502070>.
- [19] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

- [20] Michael A. Nielsen et al. “Quantum Computation as Geometry”. In: *Science* 311.5764 (Feb. 2006), pp. 1133–1135. ISSN: 1095-9203. DOI: [10.1126/science.1121541](https://doi.org/10.1126/science.1121541). URL: <http://dx.doi.org/10.1126/science.1121541>.
- [21] Marcelo de Oliveira et al. “Unconditional advantage of noisy qudit quantum circuits over biased threshold circuits in constant depth”. In: *Nature Communications* 16.1 (Aug. 2025). ISSN: 2041-1723. DOI: [10.1038/s41467-025-58545-4](https://doi.org/10.1038/s41467-025-58545-4). URL: <http://dx.doi.org/10.1038/s41467-025-58545-4>.
- [22] John Preskill. *Quantum computing and the entanglement frontier*. 2012. arXiv: [1203.5813](https://arxiv.org/abs/1203.5813) [quant-ph]. URL: <https://arxiv.org/abs/1203.5813>.
- [23] Alexander A Razborov and Steven Rudich. “Natural proofs”. In: *Proceedings of the twenty-sixth annual ACM symposium on Theory of computing*. 1994, pp. 204–213.
- [24] Peter W. Shor. “Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer”. In: *SIAM Journal on Computing* 26.5 (Oct. 1997), pp. 1484–1509. ISSN: 1095-7111. DOI: [10.1137/S0097539795293172](https://doi.org/10.1137/S0097539795293172). URL: <http://dx.doi.org/10.1137/S0097539795293172>.
- [25] Sathyawageeswar Subramanian and Min-Hsiu Hsieh. “Quantum algorithm for estimating α -Renyi entropies of quantum states”. In: *Phys. Rev. A* 104 (2 Aug. 2021), p. 022428. DOI: [10.1103/PhysRevA.104.022428](https://doi.org/10.1103/PhysRevA.104.022428). URL: <https://link.aps.org/doi/10.1103/PhysRevA.104.022428>.
- [26] Alan Mathison Turing et al. “On computable numbers, with an application to the Entscheidungsproblem”. In: *J. of Math* 58.345-363 (1936), p. 5.
- [27] Hayata Yamasaki et al. “Quantum ridgelet transform: winning lottery ticket of neural networks with quantum computation”. In: *International Conference on Machine Learning*. PMLR. 2023, pp. 39008–39034.