

Quantum Computation: A Brief Overview

Henan Huang

*School of Physical Science and Technology, Southwest Jiaotong University, Chengdu, China
15820446873@163.com*

Abstract: Quantum computation has teased scientific imagination ever since Richard Feynman dreamed in 1982 of quantum-mechanical computers, which could solve problems that are effectively out of reach of classical computation thanks to their ability to use superposition and entanglement. This critical survey recalls the field's journey from theoretical advances to present-day engineering challenges, highlighting the yawning gulf between quantum computing's lofty promises and its actual realizations. By examining three decades of developments, from Shor's integer factorization and Grover's search algorithms to recent demonstrations of quantum supremacy, this paper shows how idealized mathematical models interact with the noisy, resource-constrained realities of physical quantum systems. The author presents a literature review through critically analyzing key achievements in quantum computing research.. This paper concludes that quantum advantage will not arise from brute-force universality, but through application specific co-design, combining noise-adjusted algorithms to quantum hardware restrictions whilst mixing classical and quantum processing modes and fundamentally changing the way we think of error correction through the physics of qubits. This shift in paradigm from theoretical maximalism to engineering pragmatism embodies a realistic roadmap for practical quantum computation.

Keywords: Quantum computation, Quantum algorithms, Quantum error correction, NISQ era, Hybrid quantum-classical systems.

1. Introduction

Since Feynman's prescient proposal to leverage quantum mechanics to simulate physical systems, quantum computation has radically reshaped the landscape of computational science [1]. Decades have since then passed — the milestones of field evolution have been transformative: Shor's polynomial-time integer factorization algorithm overturned classical cryptography, Grover's quantum search acceleration repositioned information retrieval paradigms and surface code based error correction schemes laid the foundations of fault tolerance [2-4]. With the advent of Noisy Intermediate-Scale Quantum (NISQ) devices with 50–100 qubits, landmark quantum supremacy demonstrations have begun, signaling the transition from theory to practice [5-6]. Despite the burgeoning claims of quantum advantage, real-world quantum applications are limited by continuing discrepancies between idealized models of quantum operation and the physical reality.

This review critically examines the present state of quantum computation, interrogating three inconsistencies, including the gap between the assumptions of algorithmic complexity and error-prone quantum hardware, the oversimplification of scalability assumptions in error correction

protocols, and the mismatch between claims of quantum speedup and computational requirements in practice. More specifically, this research explores what needs to be addressed in order for foundational results, like Shor's algorithm needing 20 million physical qubits for factoring 2048-bit RSA, to not only be pushed into a theoretical realm, but also not remain untransformable to realized hardware within decades of effort developing hardware [7]. The investigation raises doubts about whether important issues such as NISQ-era benchmarks, including quantum supremacy experiments, contribute to practical computation or serve primarily to reveal scheduled quantum advantages [6].

This work methodologically synthesizes insights from three concurrent fields: algorithmic complexity theory, experimental quantum device characterization, and thermodynamic analyses of quantum systems. Cross-examining theoretical predictions with experimental data from superconducting qubit arrays and photonic quantum simulators, we pinpoint systemic oversights in current research trajectories [4,6]. This work focuses on some specific aspects of energy scaling laws that determine error correction and diminishing returns from variational quantum algorithms [8-9].

This critical appraisal is important because it calls for a re-allocating of research priorities. The review provides a framework for assessing technological readiness as the field nears possible inflection points from topological qubit realizations to hybrid quantum-classical architectures [10]. Through elucidating the limitations of the decoherence, the complexity of control, and the cost of thermodynamics, this paper seeks to guide the community towards co-design strategies that can shape the algorithmic innovation around physical qubit constraints, thereby accelerating the route to meaningful quantum advantage.

2. Theoretical foundations

2.1. Quantum algorithms

Two algorithmic discoveries were pivotal in establishing the theoretical underpinning of quantum computation, these being computational complexity boundary-shifting breakthroughs. In 1994, Shor discovered a polynomial-time algorithm for integer factorization, a task that classically seemed to require superpolynomial time [2]. The strength of the algorithm lies in the clever application of quantum phase estimation and the quantum Fourier transform (QFT):

$$\mathcal{F}_N |x\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i x k / N} |k\rangle \quad (1)$$

where the QFT allows for efficient period finding over modular arithmetic. Applying the above quantum method to the function $f(x) = ax \bmod N$ where a and N are coprime integers, the complexity of factorization is reduced from $O(e^{(\log N)^{1/3}})$ (classical number field sieve) to $O((\log N)^3)$. This exponential speedup, however, relies on perfect gates and dismisses the staggering penalty from error correction. The most recent analyses show that factoring 2048-bit RSA numbers requires concatenated surface codes protecting ~ 20 million physical qubits, corresponding to a logical qubit footprint exceeding $103\times$ the necessary physical qubit numbers [7].

Grover's 1996 search algorithm provided a complementary quadratic speedup ($O(\sqrt{N})$ vs. classical $O(N)$) for unstructured databases through amplitude amplification [3]. The unitary operation:

$$G = (2|\psi\rangle\langle\psi| - I)O_f \quad (2)$$

where O_f is the mark's solutions operator, and $|\psi\rangle$ is the uniform superposition state; this iteration boosts the probability of target states. Though theoretically universal, its practical utility evaporates under decoherence: each Grover iteration requires error rates at 10^{-4} for searches at 1000 qubits—a threshold far beyond current thermal NISQ devices. These limitations illustrate a fundamental disconnection between asymptotic complexity claims and physical implementation constraints.

2.2. Quantum error correction

The threshold theorem forms the cornerstone of fault-tolerant quantum computation, asserting that arbitrary-length computations become feasible if physical error rates p satisfy $p < p_{\text{th}} \approx 10^{-3}$ for surface codes [4]. This threshold derives from the code's distance- d error suppression:

$$p_{\text{logical}} \approx C \left(\frac{p}{p_{\text{th}}} \right)^{(d+1)/2} \quad (3)$$

where C is a constant that depends on the topology. Surface codes implement this with stabilizer measurements on a 2D lattice of physical qubits and interrogate the qubit lattice by measuring end qubits to read out the syndrome cycle used to detect errors. Yet the assumptions of stochastic Pauli errors and scalable parity-check circuits inherent to the theorem conflict with experimental realities: cross-talk in superconducting qubits leads to correlated errors that invalidate independence assumptions, while the $O(d^3)$ temporal overhead required for syndrome processing surpasses NISQ-era coherence times [11].

Recent innovations attempt to circumvent these limitations through physical qubit engineering. Biased-noise qubits exploit asymmetric error channels (e.g., dominant dephasing in cat qubits) to simplify error correction [11]. By encoding logical qubits in coherent states $|\alpha\rangle + |-\alpha\rangle$ with phase-flip protection, the effective error rate becomes:

$$p_{\text{eff}} \propto e^{-2|\alpha|^2} \ll p_{\text{physical}} \quad (4)$$

reducing resource overheads by orders of magnitude. Similarly, dynamically protected logical qubits employ continuous driving fields to suppress relaxation errors, effectively "freezing" the qubit state within decoherence-free subspaces [12]. These approaches highlight the growing recognition that error correction must co-evolve with qubit physics rather than relying solely on abstract coding theory.

3. Current progress and critical challenges

3.1. The NISQ era

The Noisy Intermediate-Scale Quantum (NISQ) era, which was formally defined by Preskill in 2018, refers to the intermediate regime in which quantum devices will operate with on the order of 50–100 imperfect qubits with error rates above fault-tolerance limits [12]. The 2019 Sycamore processor demonstration was a watershed [6]: sampling outputs of a 53-qubit random circuit of depth 20, its claim was a task completion time of 200 seconds versus 10,000 years for classical supercomputers. This "quantum supremacy" was defined in terms of the exponential difficulty of simulating quantum systems:

$$\mathcal{C}_{\text{quantum}} = O(2^n \cdot d), \mathcal{C}_{\text{classical}} = O(2^{2n}) \quad (5)$$

where n is the qubit count and d circuit depth. However, subsequent classical optimizations using tensor network contractions reduced the simulated runtime to days, exposing the experiment's narrow specialization [13-14]. The Sycamore chip itself revealed fundamental NISQ limitations: single-qubit gate fidelities $\sim 99.85\%$ and two-qubit fidelities $\sim 99.4\%$ induce cumulative errors scaling as:

$$\epsilon_{\text{total}} \approx 1 - \prod_{k=1}^m (1 - \epsilon_k) \approx m \cdot \epsilon_{\text{avg}} \quad (6)$$

for m gates, making deep circuits unviable. In particular, NISQ applications such as the variational quantum eigensolver (VQE) and the quantum approximate optimization algorithm (QAOA) exhibit exponential scaling of resources. For molecular ground-state calculations, VQE needs $O(N^4)$ measurements for N -orbital systems, and QAOA requires $O(p \log p)$ layers to approximate MaxCut

for p vertices solutions, and therefore each layer is vulnerable to decoherence [9]. The size of such shallow circuits $d \lesssim 100$ is fundamentally limited by these constraints and the capability of NISQ to solve problems.

3.2. Quantum machine learning

Quantum machine learning (QML) proposals often hinge on the Harrow-Hassidim-Lloyd (HHL) algorithm for solving linear systems $Ax = b$ [15]. The quantum advantage ostensibly arises from the exponential speedup in state preparation:

$$|b\rangle = \sum_{i=1}^N b_i |i\rangle \xrightarrow{\text{QRAM}} O(\log N) \text{ time} \quad (7)$$

and eigenvalue inversion A^{-1} via quantum phase estimation. However, the algorithm's $O(\kappa^2 \log N / \epsilon)$ complexity (where κ is the condition number and ϵ precision) assumes fault-tolerant execution. In NISQ implementations, noisy quantum Fourier transforms and trotterized Hamiltonian evolution accumulate errors quadratically:

$$\| U_{\text{ideal}} - U_{\text{noisy}} \| \leq \Gamma \cdot t^2 \quad (8)$$

where t is the simulation time and Γ is the noise rate. Experimental studies demonstrate that quantum neural networks only reach 95% accuracy on MNIST classification tasks, compared to classical ones which give 99% accuracy, all while consuming $103\times$ more energy for cryogenic cooling [14]. And in quantum-enhanced applications, the best-known applications of quantum speedups, such as for portfolio optimization, the quadratic speedup of quantum amplitude estimation (QAE) disappears in the presence of data loading overheads (generally, any application which involves data loading). Compressed representations of classical tensor networks such as Tree Tensor Networks (TTN) provide similar performance to QML in $d \leqslant 10$ dimensional data:

$$\text{OTTN} = O(d \cdot \chi^3) \rightarrow \text{vs.* OQML} = O(2d) \quad (9)$$

where χ is a bond dimension, further questioning the necessity of quantum approaches in low- κ regimes. These realities demand rigorous resource-counting frameworks to assess QML's practical viability beyond asymptotic complexity claims.

4. Critical perspectives

4.1. The myth of universality

Despite its theoretical basis, the quest for quantum computers that can universally perform fault-tolerant calculations is deeply hindered by physical barriers that preclude the inevitability of its occurrence. Topological qubit architectures, including those based on Majorana fermions, exploit the braiding statistics of non-Abelian anyons to guarantee intrinsic error protection [9-10]. Nevertheless, experimental platform works are limited to sub-Kelvin region and ultra-clean semiconductor nanowires, so far obtaining ZBCPs (zero-bias conductance peaks) as a sufficient signature for the Majorana modes. Even if achieved, scaling to practical qubit counts is hindered by the "density problem": Majorana nanowires have $\sim 1 \mu\text{m}$ separation between anyons, with only $\sim 10^4$ qubits/cm 2 densities achievable in 2D arrays, (for reference) orders of magnitude too few compared to the $\sim 10^8/\text{cm}^2$ required for error corrected algorithms. Superconducting qubits have made rapid progress, but face frequency crowding as N , the number of qubits, scales (i.e., the spacing of the anharmonic oscillator Δ must satisfy:

$$\Delta > 5\sqrt{N} \cdot \kappa \quad (10)$$

where κ is the cavity linewidth, to avoid crosstalk. For $N = 1000$, this necessitates $\Delta/2\pi > 1$ GHz, exceeding current transmon designs ($\Delta/2\pi \approx 200$ MHz). These physical limits underscore the need for architecture-specific optimization over blind adherence to universal roadmaps.

4.2. Overlooking thermodynamic costs

Quantum computation's reversibility—often touted for energy efficiency—obscures the thermodynamic costs of error correction. Landauer's principle establishes a lower bound of $k_B T \ln 2$ per erased bit, but quantum error correction (QEC) cycles incur additional dissipation from syndrome measurement. For surface code cycles with $d \times d$ lattices, the energy per cycle scales as:

$$E_{\text{QEC}} \approx \frac{3}{2} k_B T d^2 \ln \left(\frac{1}{\epsilon_{\text{phys}}} \right) \quad (11)$$

where ϵ_{phys} is the physical error rate [8]. For example, a distance-25 code ($\epsilon_{\text{phys}} = 10^{-3}$) running at 10 mK thus dissipates $\sim 10^{-18}$ J/cycle, or ~ 1 kW power for a 10^6 qubit system, at 1 MHz cycles—comparable with classical supercomputers. Also, cryogenic cooling inefficiencies ($\eta \approx 10^{-4}$) multiply total energy expenses by $10^{4\times}$, negating the hypothetical quantum energy advantages. Such realities require QEC protocols to be co-designed to account for thermodynamic constraints.

4.3. Algorithmic relevance

The predominance of oracle-based algorithms in quantum computing literature, such as Grover's search and Deutsch-Jozsa, creates an illusion of broad applicability despite limited practical utility.

Grover's algorithm for unsorted database search: while achieving $O(\sqrt{N})$ queries versus classical $O(N)$, its real-world implementation requires:

$$N_{\text{phys}} = O \left(N_{\log} \cdot \log \left(\frac{1}{\epsilon_{\text{tot}}} \right) \right) \quad (12)$$

To build N_{\log} logical qubits, you need physical qubits to keep the total error $\epsilon_{\text{tot}} < 0.5$. This requires $> 10^4$ physical qubits for $N = 10^6$ database entries, even for gate errors of $\epsilon_{\text{gate}} = 10^{-4}$, exceeding NISQ capabilities. In contrast, quantum chemistry algorithms such as variational quantum eigensolvers carry real value [16]: FeMo-co (nitrogenase cofactor) can be simulated classically using $O(10^4)$ Pauli terms, but only $O(10^2)$ measurements quantumly. Nevertheless, existing hardware constraints limit simulations to ≤ 10 spin-orbitals while industrial catalysts need ≥ 100 . Closing that gap needs a coevolution of algorithms and hardware around domain-specific problems, not abstract SCF (speedup claims formulation).

5. Challenges and future directions

5.1. Key limitations

Three key limitations of existing work are as follows: Excessive focus on asymptotic complexity measures that decouple performance from physical resource limits, insufficient co-design between algorithmic and hardware engineering, and neglect of energy scaling laws in fault tolerance. Overcoming these barriers will require future work that is much more hardware-aware in algorithm design—for example designing surface code layouts specifically to optimize towards the particular lattice geometries available in molecular simulations—and that explores alternative paradigms, such as photonic GKP codes that suppress phase errors in principle. Hybrid classical-quantum architectures should capitalize on the use of tensor network decompositions to better distribute workloads while developing noise-adaptive compilers for more dynamic error mitigation.

5.2. Co-design algorithm-hardware optimization

Bridging the chasm between algorithmic theory and material hardware implies a systematic co-design paradigm workflow optimizing quantum circuits for particular qubit architectures. For superconducting qubit arrays with limited connectivity (e.g., IBM's heavy hex lattice), competitive gains can be achieved in SWAP gate overhead (30–40% reduction) using graph isomorphism-based qubit routing techniques in hardware-aware compilers. Noise-adaptive quantum error mitigation algorithms (e.g., probabilistic error cancellation (PEC)) can also dynamically prioritize gates expected to low-noise with respect to modern decoherence profiles. There is a need to integrate error correction capabilities directly into the design of algorithms—for instance, by designing surface code patches to conform to the calculations in quantum chemistry simulations to achieve a minimal spacetime overhead. However, recent studies have proposed co-design approaches that could bring the number of physical qubits required to factor 2048-bit RSA down from 20 million to 12 million under realistic error rates [7].

5.3. Hybrid classical-quantum systems

Near-term applications will be dominated by hybrid architectures in which classical processing like data truncation and quantization is done in advance before quantum execution. This enables each quantum tensor network to decompose a task into low entanglement subproblems that can be solved with classical resources (for example, deployment of TPUs for matrix product states) while still leaving quantum circuits for high-schmidt rank problem solving. By employing dynamic circuit cutting techniques based on Bayesian optimization, sub1000-qubit circuits can be decomposed into classically tractable fragments with < 50 qubits and < 5% fidelity loss. Moreover, classical meta-learning models trained on historical noise data can optimize variational quantum ansatzes, achieving $102\text{--}103\times$ reduction in quantum sampling rounds [9]. This conjugacy optimizes resource utilization at the smeared decoding noise and mitigates the decoherence impact, making it essential for the translation of quantum computing demonstrations of the NISQ-era into a practical quantum advantage.

6. Conclusion

This extensive analysis has exhibited that, if quantum computation is to emerge as a practically useful technology, there must be a fundamental rethink of the theoretical foundations and engineering practice. This review identifies systemic tensions that need to be addressed in the three tensions we discussed in the introduction: mismatch between algorithms and hardware, simplified error correction scalability, and unrealistic speedup claims and find systemic bottlenecks currently restricting implementations. Although Shor's and Grover's algorithms are nonclassical in nature, as they provide exponential and quadratic speedups respectively, and theoretically their speeds can be achieved, the realization of this has been accompanied by a significant order of magnitude challenge—the proposal for RSA-2048 factoring requires at least 20 million physical qubit, and 10^{-4} error rate threshold for Grover's search which lies beyond the physical capabilities of even the NISQ. Even the quantum supremacy milestone, while symbolically powerful, emphasizes narrow quantum dynamics more than general computing advantage.

The study also highlights important blind spots in current paradigms of research. First, the assumption of independent errors made by the threshold theorem does not take into account superconducting qubit cross-talk, which requires the use of adaptive error correction codes such as biased-noise cat qubits. Second, thermodynamic studies show that surface code error correction for 10^6 qubit systems generates 1 kW of power just in dissipation, similar to classical supercomputers—while considering cryogenic overhead. Third, state-of-the-art oracle-based algorithms, such as Grover's search, require $> 10^4$ physical qubits to be implemented for databases with practical sizes,

and domain-specific applications (indeed quantum chemistry simulations) remain constrained to toy models due to hardware constraints.

In the end, the field's evolution from laboratory curiosities to technological revolution awaits through the rejection of universal quantum computing as a goal to be attained in the short run. Rather, concentrated investments in application specific co-design, low-energy error correction, and hybrid system integration are likely to produce the first generation of practical quantum advantage. Such engineering, pragmatic, informed by physics, is the only way that quantum computation is ever going to realize its transformative promise.

Although the fundamental problems of quantum computation are critically examined in this review, new developments such as breakthroughs in topological qubits, synergies in quantum machine learning, and recent advances in error-correction (e.g., Floquet codes) are not adequately covered. Future research will employ hybrid approaches that combine theoretical criticisms with experimental benchmarking, as well as structured literature mining, to methodically monitor state-of-the-art developments. By addressing this dynamic landscape, the roadmap will become more relevant and help close gaps between engineering frameworks and quickly changing research.

References

- [1] R. P. Feynman, "Simulating physics with computer", *International Journal of Theoretical Physics*, vol. 21, no. 6, pp. 467–488, 1982.
- [2] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring", in *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 1994, pp. 124–134.
- [3] L. K. Grover, "A fast quantum mechanical algorithm for database search", in *Proceedings of the 28th Annual ACM Symposium on Theory of Computing*, 1996, pp. 212–219.
- [4] J. Preskill, "Fault-tolerant quantum computation", *arXiv:quant-ph/9712048*, 1998.
- [5] A. W. Harrow and A. Montanaro, "Quantum computational supremacy", *Nature*, vol. 549, no. 7671, pp. 203–209, 2017.
- [6] F. Arute et al., "Quantum supremacy using a programmable superconducting processor", *Nature*, vol. 574, no. 7779, pp. 505–510, 2019.
- [7] C. Gidney and M. Eker a, "How to factor 2048-bit RSA integers in 8 hours using 20 million noisy qubits", *Quantum*, vol. 5, p. 433, 2021.
- [8] D. Reeb and M. M. Wolf, "Improved Landauer principle with finite-size bath", *New Journal of Physics*, vol. 16, no. 10, p. 103011, 2014.
- [9] M. Cerezo et al., "Variational quantum algorithms", *Nature Reviews Physics*, vol. 3, no. 9, pp. 625–644, 2021.
- [10] D. Aasen et al., "Milestones toward Majorana-based quantum computing", *Physical Review X*, vol. 6, no. 3, p. 031016, 2016.
- [11] J. Guillaud and M. Mirrahimi, "Repetition cat qubits for fault-tolerant quantum computation", *Physical Review X*, vol. 9, no. 4, p. 041053, 2019.
- [12] J. Preskill, "Quantum computing in the NISQ era and beyond", *Quantum*, vol. 2, p. 79, 2018.
- [13] E. Pednault et al., "Leveraging secondary storage to simulate deep 54-qubit Sycamore circuits", *arXiv:1910.09534*, 2019.
- [14] F. Pan and P. Zhang, "Simulating the Sycamore quantum supremacy circuits", *Physical Review Letters*, vol. 129, no. 5, p. 050502, 2022.
- [15] J. Biamonte et al., "Quantum machine learning", *Nature*, vol. 549, no. 7671, pp. 195–202, 2017.
- [16] S. McArdle et al., "Quantum computational chemistry", *Reviews of Modern Physics*, vol. 92, no. 1, p. 015003, 2020.