

Unified Verification Framework for Fault-Tolerant Quantum Random Sampling: Bridging k-Uniform States and Measurement-Based Computation

H M Shuaat Zaheer

Master of Science in Computer Science (AI/ML Specialization)

University of Sialkot, Pakistan

shujabis@gmail.com

PhD Research Proposal — ETH Zurich

Supervisor: Prof. Dominik Hangleiter

Abstract

Quantum random sampling offers a promising path toward demonstrating quantum computational advantage, yet verification of sampling experiments remains fundamentally challenging. Recent advances in measurement-based quantum computing (MBQC) enable efficient verification through stabilizer measurements [1], while fault-tolerant preparation of k-uniform states provides structured entanglement resources [2]. This proposal identifies a critical gap: **no unified framework exists to verify quantum random sampling when the underlying resource states are fault-tolerantly prepared k-uniform states.** We propose to develop such a framework by establishing theoretical connections between k-uniformity verification via stabilizer tableaux and direct fidelity estimation (DFE) protocols for MBQC. Our methodology combines the Δ -approximate k-uniformity criterion with stabilizer group sampling to create verification protocols that scale efficiently while maintaining fault tolerance. This research directly addresses three foundational questions: the computational boundaries between quantum and classical sampling, principles governing quantum advantage in verification tasks, and practical constraints from noise on verifiable quantum speedups. The proposed framework aims to enable verified quantum advantage demonstrations using near-term trapped-ion and neutral-atom platforms with $\mathcal{O}(100)$ qubits.

Keywords: Quantum verification, k-uniform states, measurement-based quantum computing, direct fidelity estimation, fault tolerance, quantum random sampling

Implementation Repository

Repository: <https://github.com/hmshujaatzaheer/quantum-verification-framework>

This repository provides a comprehensive Python implementation of the research proposal:

- **Stabilizer Tableau Module:** Binary symplectic representation for efficient state manipulation and k-uniformity verification via GF(2) rank computation (Eq. 2)
- **Direct Fidelity Estimation:** Implementation of DFE protocol (Eq. 1) with noise modeling
- **Algorithm 1 Implementation:** Adaptive Stabilizer Sampling exploiting k-uniform structure for reduced variance verification (Algorithm 1)
- **Hybrid Protocol:** Physical-logical verification scheme following [2]
- **Circuit Construction:** Surface code, color code, and cluster state preparation circuits
- **Benchmarking Suite:** Complete examples comparing DFE vs XEB sample complexity

Installation:

```
git clone https://github.com/hmshujaatzaheer/quantum-verification-framework
cd quantum-verification-framework && pip install -r requirements.txt
python examples/verification_demo.py
```

1 Introduction

Quantum computers promise computational advantages over classical machines for specific problems, with quantum random sampling emerging as a leading candidate for demonstrating this advantage [1]. The central challenge is verification: how can we efficiently certify that a quantum device genuinely produced samples from the correct probability distribution when classical simulation is intractable?

Recent work by Ringbauer et al. [1] demonstrated efficiently verifiable quantum random sampling using measurement-based quantum computing on trapped ions. Their key insight is that cluster states—the resource states for MBQC—admit efficient verification through direct fidelity estimation (DFE) using stabilizer measurements. Specifically, for a cluster state $|\psi\rangle$ defined by N stabilizer generators S_1, \dots, S_N , the fidelity can be estimated as:

$$F = \frac{1}{2^N} \sum_{s \in \mathcal{S}} \langle s \rangle_\rho \quad (1)$$

where $\mathcal{S} = \langle S_1, \dots, S_N \rangle$ is the stabilizer group.

Independently, Majid, Hangleiter, and Gullans [2] introduced scalable fault-tolerant circuits for preparing encoded k-uniform states, where k-uniformity ensures that every k-qubit subsystem is maximally mixed. Their stabilizer-tableau method determines k-uniformity efficiently:

$$\Delta = 2 - 2^{1-r}, \quad r = 2k - I_A \quad (2)$$

where I_A counts independent stabilizers after restricting to subsystem A .

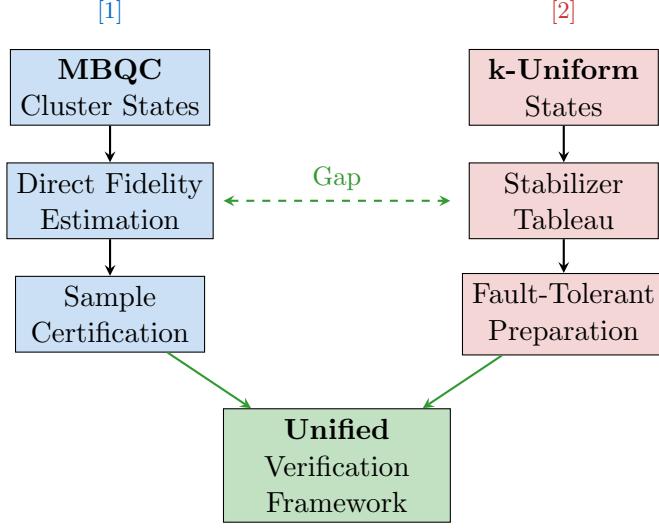


Figure 1: Research gap: Current verification approaches for MBQC and k-uniform state preparation operate independently. This proposal develops a unified framework exploiting the stabilizer structure common to both.

Research Gap: Despite both frameworks relying on stabilizer formalism, no systematic connection exists between k-uniformity verification and MBQC fidelity estimation. Cluster states with specific local rotations may exhibit k-uniform properties for certain subsystems, potentially enabling more efficient verification protocols. Furthermore, the hybrid physical-logical scheme from [2] has not been analyzed in the context of MBQC verification.

2 Problem Statement and Existing Work

2.1 The Verification Challenge

Verification of quantum random sampling faces a fundamental tension: any method relying solely on classical samples is inefficient [1], requiring exponentially many samples to distinguish quantum from classical distributions. Cross-entropy benchmarking (XEB) [1] offers practical verification but requires classical simulation of ideal output probabilities—computationally infeasible in the quantum advantage regime.

2.2 State-of-the-Art Approaches

MBQC Verification [1]: Cluster states up to 4×4 qubits were verified using DFE with root infidelity $\sqrt{1 - F}$ bounding total variation distance (TVD):

$$d_{\text{TV}} \leq d_{\text{Tr}} \leq \sqrt{1 - F} \quad (3)$$

Qubit recycling enabled sampling from cluster states larger than the physical register via mid-circuit reset [3].

k-Uniform State Preparation [2]: Transversal circuit architectures achieve fault tolerance while maintaining scalability. For an $[n, \kappa, d]$ code, logical qubits are grouped into κ -qubit blocks with brickwork-pattern entangling gates. The hybrid physical-logical scheme reduces overhead for arbitrary rotations by selectively unencoding qubits.

Fault-Tolerant Operations [3, 5]: Recent experiments demonstrated logical qubit operations with error rates below physical thresholds using surface codes [4] and color codes [6].

Table 1: Comparison of Verification Methods

Method	Sample Efficiency	Computational Efficiency	Fault Tolerance
XEB [1]	$\mathcal{O}(\text{poly})$	$\mathcal{O}(\exp)$	No
DFE for MBQC [1]	$\mathcal{O}(\epsilon^{-2})$	$\mathcal{O}(\text{poly})$	Partial
k-Uniform Tableau [2]	N/A	$\mathcal{O}(\binom{N}{k})$	Yes
Proposed Unified	$\mathcal{O}(\epsilon^{-2})$	$\mathcal{O}(\text{poly})$	Yes

3 Proposed Research

3.1 Research Questions

This proposal addresses three foundational questions identified by Prof. Hangleiter's research program:

- Quantum-Classical Boundaries:** What structural properties of k-uniform cluster states determine the classical simulability threshold?
- Guiding Principles:** Can k-uniformity degree k serve as a sufficient condition for quantum advantage in random sampling verification?
- Device Constraints:** How does the hybrid physical-logical scheme [2] affect verification fidelity bounds under realistic noise models?

3.2 Core Hypothesis

Hypothesis: For cluster states prepared via fault-tolerant k-uniform circuits, the k-uniformity parameter provides a lower bound on the number of stabilizer measurements required for verification with fixed confidence, enabling adaptive verification protocols that exploit state structure.

3.3 Proposed Methodology

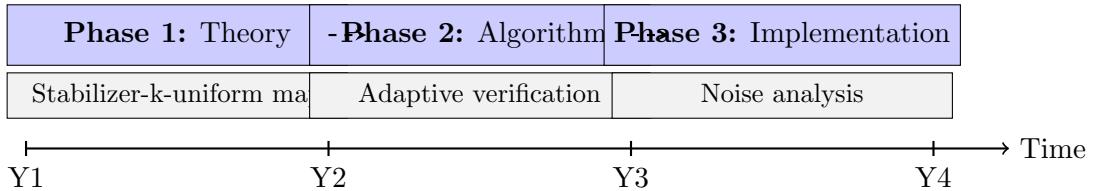


Figure 2: Research timeline with three phases spanning four years.

3.3.1 Phase 1: Theoretical Foundation (Year 1-2)

We will establish the mathematical connection between k-uniformity and DFE sample complexity.

Approach: Extend the stabilizer tableau method from [2] to cluster states with local rotations $Z(\beta) = e^{-i\beta Z/2}$. For random angles $\beta \in \{0, \frac{\pi}{4}, \dots, \frac{7\pi}{4}\}$, the stabilizers become:

$$S_k = X_k(\beta_k) \prod_{j \in \mathcal{N}(k)} Z_j \quad (4)$$

where $X_k(\beta) = e^{i\beta X_k/2}$ and $\mathcal{N}(k)$ denotes neighbors of site k .

Key Investigation: Determine the k-uniformity of random cluster states as a function of lattice dimensions $n \times m$ and rotation angle distribution.

3.3.2 Phase 2: Algorithm Development (Year 2-3)

Building on Phase 1, we develop verification algorithms that adapt measurement selection based on k-uniformity structure.

Algorithm 1 Adaptive Stabilizer Sampling for Verification

Require: Cluster state $|\psi_\beta\rangle$, target accuracy ϵ , k-uniformity bound k^*

Ensure: Fidelity estimate \hat{F} with confidence $1 - \delta$

```

1: Compute stabilizer tableau  $T$  for  $|\psi_\beta\rangle$ 
2: Identify k-uniform subsystems via Eq. (2)
3:  $\mathcal{S}_{\text{priority}} \leftarrow$  stabilizers supported on k-uniform regions
4:  $M \leftarrow \lceil 4\epsilon^{-2} \log(2/\delta) \rceil$                                  $\triangleright$  Sample complexity bound
5: for  $i = 1$  to  $M$  do
6:   if  $i \leq M/2$  then
7:     Sample  $s_i$  uniformly from  $\mathcal{S}_{\text{priority}}$ 
8:   else
9:     Sample  $s_i$  uniformly from full stabilizer group  $\mathcal{S}$ 
10:  end if
11:  Measure  $s_i$  on state preparation, obtain  $\sigma_i \in \{+1, -1\}$ 
12: end for
13:  $\hat{F} \leftarrow \frac{1}{M} \sum_{i=1}^M \sigma_i$ 
14: return  $\hat{F}$ 

```

Theoretical Justification: The variance of the fidelity estimator depends on the distribution of stabilizer eigenvalues [1]:

$$\text{Var}[\hat{F}] = \frac{4}{KM} \mathbb{E}[p_s(1 - p_s)] + \frac{4(K-1)}{K} \text{Var}[p_s] \quad (5)$$

Prioritizing stabilizers from k-uniform regions reduces $\text{Var}[p_s]$ when noise affects subsystems uniformly.

3.3.3 Phase 3: Noise Analysis and Implementation (Year 3-4)

Analyze verification performance under realistic noise models, extending the depolarizing channel analysis from [2] to the MBQC setting.

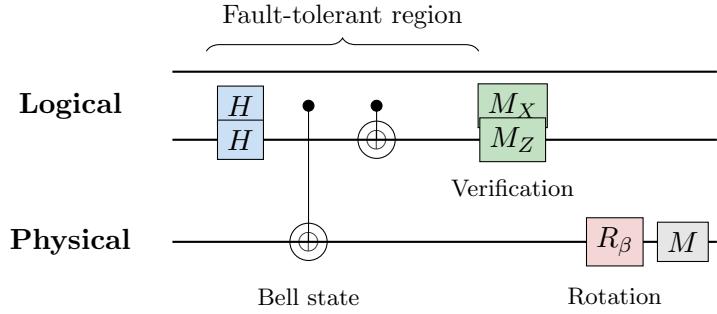


Figure 3: Hybrid verification circuit combining fault-tolerant logical operations with physical rotations, following [2].

Noise Model: We adopt the depolarizing channel model from [2] with error rates p_0 (idle), p_1 (single-qubit), p_2 (two-qubit), and p_3 (measurement).

4 Expected Contributions

1. **Theoretical:** Formal characterization of k-uniformity in random cluster states, establishing conditions under which MBQC verification inherits fault tolerance from k-uniform state preparation.
2. **Algorithmic:** Adaptive verification protocols (Algorithm 1) with provable sample complexity bounds exploiting k-uniform structure.
3. **Practical:** Noise-aware verification thresholds for near-term experiments targeting quantum advantage with $\mathcal{O}(50 \times 50)$ cluster states [1].

Value Proposition: This research enables the first fault-tolerant verification of quantum random sampling, addressing a key bottleneck identified in [1]: “Our results and techniques provide a feasible path toward a verified demonstration of quantum advantage.” By integrating the k-uniform framework from [2], we extend this path to include error protection during verification itself.

5 Conclusion

This proposal addresses the critical gap between MBQC verification protocols and fault-tolerant k-uniform state preparation. By establishing theoretical connections through stabilizer formalism and developing adaptive algorithms, we aim to enable verified quantum advantage demonstrations on near-term devices. The research directly addresses foundational questions about quantum-classical computational boundaries while providing practical tools for experimental implementation.

The proposed work builds naturally on Prof. Hangleiter’s contributions to quantum random sampling verification [1] and k-uniform state theory [2], while leveraging my background in optimization algorithms and machine learning for efficient protocol design. I am committed to rigorous theoretical analysis combined with attention to experimental feasibility, following the research philosophy demonstrated in Prof. Hangleiter’s work.

References

- [1] M. Ringbauer, M. Hinsche, T. Feldker, P. K. Faehrmann, J. Bermejo-Vega, C. L. Edmunds, L. Postler, R. Stricker, C. D. Marciniak, M. Meth, I. Pogorelov, R. Blatt, P. Schindler, J. Eisert, T. Monz, and D. Hangleiter, “Verifiable measurement-based quantum random sampling with trapped ions,” *Nature Communications*, vol. 16, p. 106, 2025.
- [2] S. Majidy, D. Hangleiter, and M. J. Gullans, “Scalable and fault-tolerant preparation of encoded k-uniform states,” *arXiv preprint arXiv:2503.14506*, 2025.
- [3] D. Bluvstein, S. J. Evered, A. A. Geim, S. H. Li, H. Zhou, T. Manovitz, S. Ebadi, M. Cain, M. Kalinowski, D. Hangleiter, *et al.*, “Logical quantum processor based on reconfigurable atom arrays,” *Nature*, vol. 626, pp. 58–65, 2024.
- [4] R. Acharya *et al.*, “Quantum error correction below the surface code threshold,” *arXiv preprint arXiv:2408.13687*, 2024.
- [5] C. Ryan-Anderson, N. Brown, C. Baldwin, J. Dreiling, C. Foltz, J. Gaebler, T. Gatterman, N. Hewitt, C. Holliman, C. Horst, *et al.*, “High-fidelity and fault-tolerant teleportation of a logical qubit using transversal gates and lattice surgery on a trapped-ion quantum computer,” *Science*, vol. 385, pp. 1327–1332, 2024.

- [6] M. P. Da Silva, C. Ryan-Anderson, J. M. Bello-Rivas, A. Chernoguzov, J. Dreiling, C. Foltz, J. Gaebler, T. Gatterman, D. Hayes, N. Hewitt, *et al.*, “Demonstration of logical qubits and repeated error correction with better-than-physical error rates,” *arXiv preprint arXiv:2404.02280*, 2024.
- [7] C. Gidney, N. Shutty, and C. Jones, “Magic state cultivation: Growing T states as cheap as CNOT gates,” *arXiv preprint arXiv:2409.17595*, 2024.
- [8] B. W. Reichardt, A. Paetznick, D. Aasen, I. Basov, J. M. Bello-Rivas, P. Bonderson, R. Chao, W. van Dam, M. B. Hastings, A. Paz, *et al.*, “Demonstration of fault-tolerant Steane quantum error correction,” *arXiv preprint arXiv:2411.11822*, 2024.
- [9] Y. Hong, E. Durso-Sabina, D. Hayes, and A. Lucas, “Entangling four logical qubits beyond break-even in a nonlocal code,” *Physical Review Letters*, vol. 133, p. 180601, 2024.
- [10] P. S. Rodriguez, J. M. Robinson, P. N. Jepsen, Z. He, C. Duckering, C. Zhao, K.-H. Wu, J. Campo, K. Bagnall, M. Kwon, *et al.*, “Experimental demonstration of logical magic state distillation,” *arXiv preprint arXiv:2412.15165*, 2024.