Benchmarking tensor network simulations of Shor's algorithm under coherent noise

Asmita Datta
(*with Flavio Baccari, Ilaria Siloi and Simone Montangero)*

University of Padova and University of Cyprus

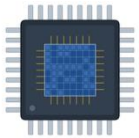
29th September 2026, Larnaca

Funded by the European Union

AQTIVATE

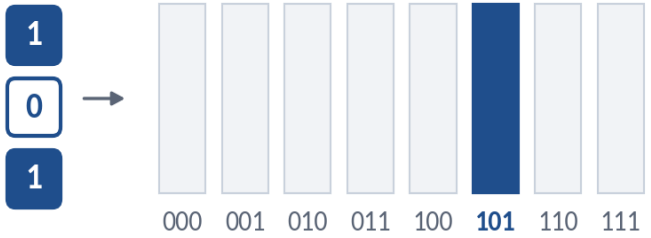
The AQTIVATE project receives funding from the European Union's HORIZON MSCA Doctoral Networks programme, under Grant Agreement No. 101072344.

Introduction to quantum computing

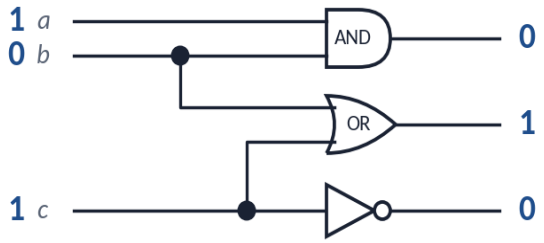


Classical

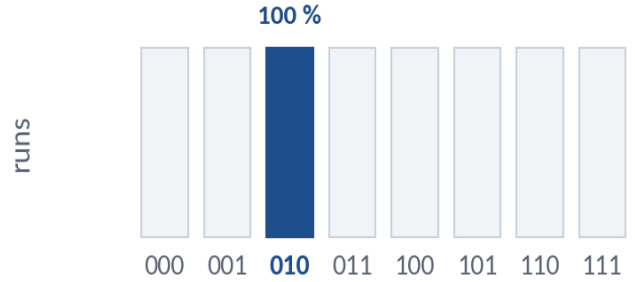
Transistors
'n' bits



A point in $\{0,1\}^n$: n numbers, freely copied



Logic gates: deterministic; irreversible

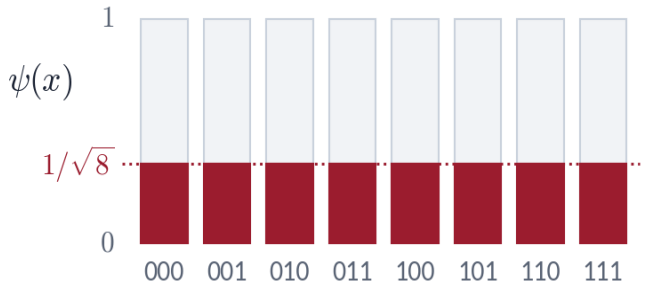


Read any time: the same answer every run

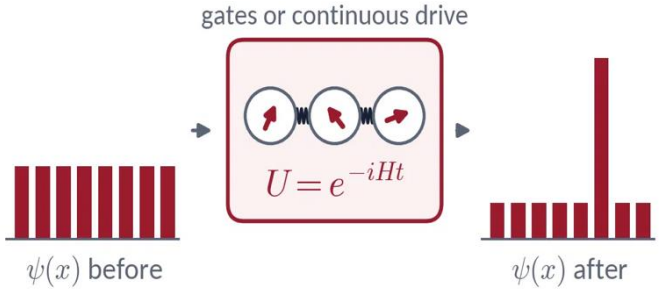


Quantum

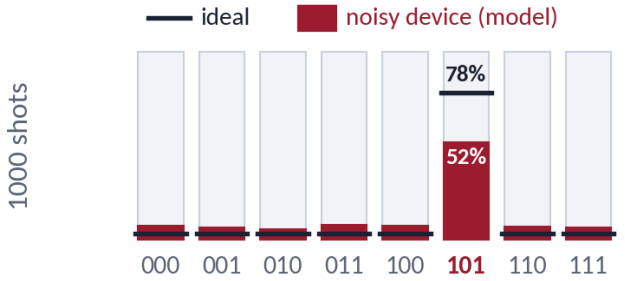
Atoms, ions, photons
'n' qubits



Complex vector in 2^n dimensions: the many-body wall



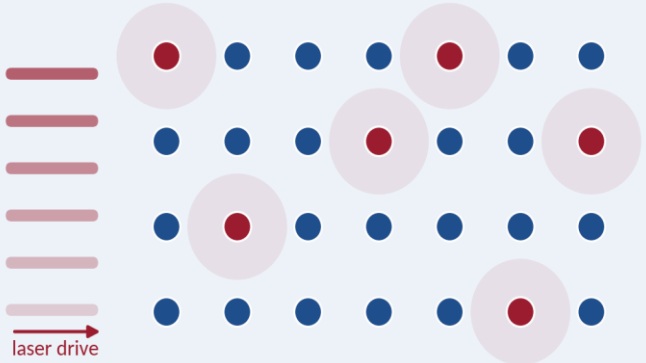
Unitary evolution (ideal): amplitudes interfere



Born rule: 1 random outcome/run, $p(x) = |\psi(x)|^2$; the state collapses

Digital and analog quantum processing

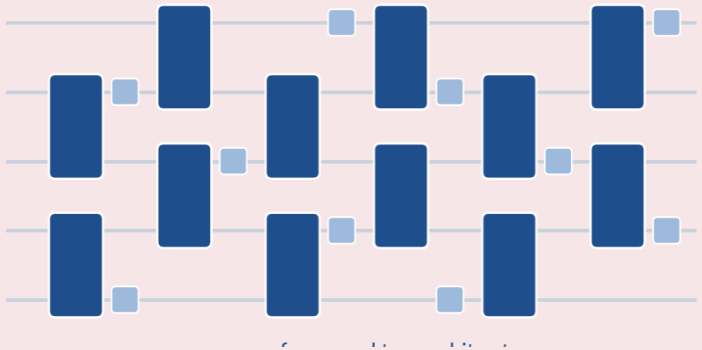
Analog: Hamiltonian-based



$$|\psi(t)\rangle = e^{-iHt}\,|\psi(0)\rangle$$

- Engineer and evolve *H* directly: cold atoms, ions, Rydberg arrays
- Not suitable for all algorithms

Digital: gate-based



$$e^{-iHt} \approx \left(\prod_k e^{-iH_k \delta t}\right)^{t/\delta t}$$

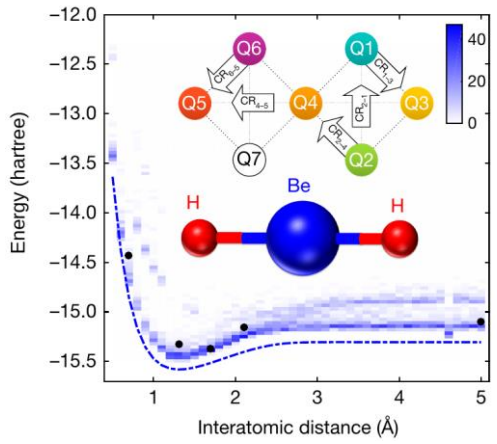
- Universal: any Hamiltonian as gates
- Limited by gate errors, state preparation and measurement errors

This work uses the gate-model of quantum computation

Cirac & Zoller, Nat. Phys. 8, 264 (2012)
Aharonov et al., SIAM J. Comput. 37, 166 (2007)
Daley et al., Nature 607, 667 (2022)

Quantum computers and simulators as a tool

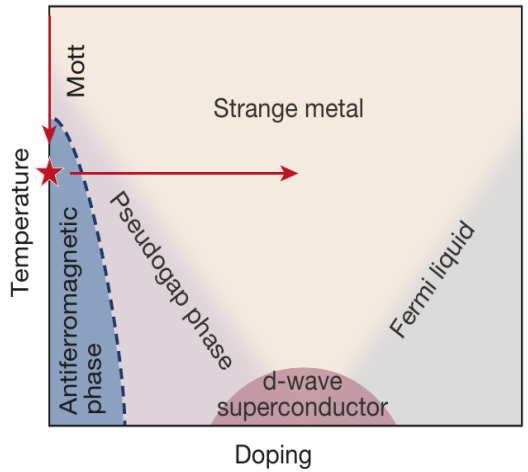
Quantum Chemistry



A six-qubit quantum processor estimated molecular ground-state energies up to BeH_2

Fig.: Kandala et al., Nature 549, 242 (2017)
FeMoco: Reiher et al., PNAS 114, 7555 (2017)

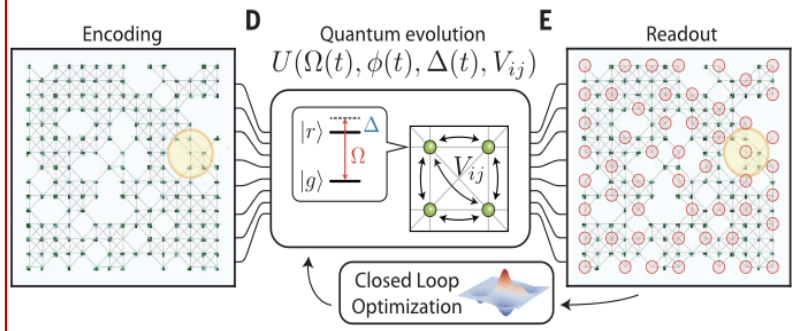
Material Science



Ultracold atoms simulated magnetic ordering in a doped Hubbard model

Fig.: Mazurenko et al., Nature 545, 462 (2017)
Greiner et al., Nature 415, 39 (2002)

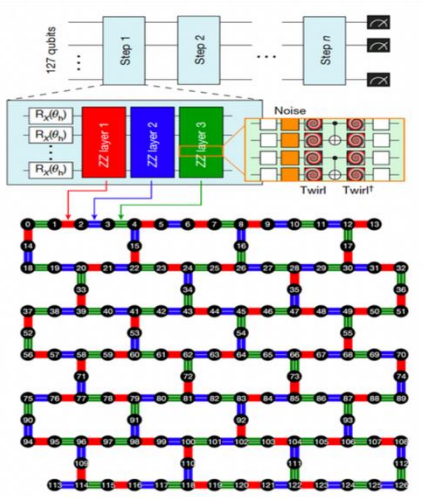
Optimization



Hard instances of MIS graph problem solved on a 289-atom Rydberg processor with super-linear speedup

Fig.: Ebadi et al., Science 376, 1209 (2022)
Farhi et al., arXiv:1411.4028 (2014)

Many-body dynamics

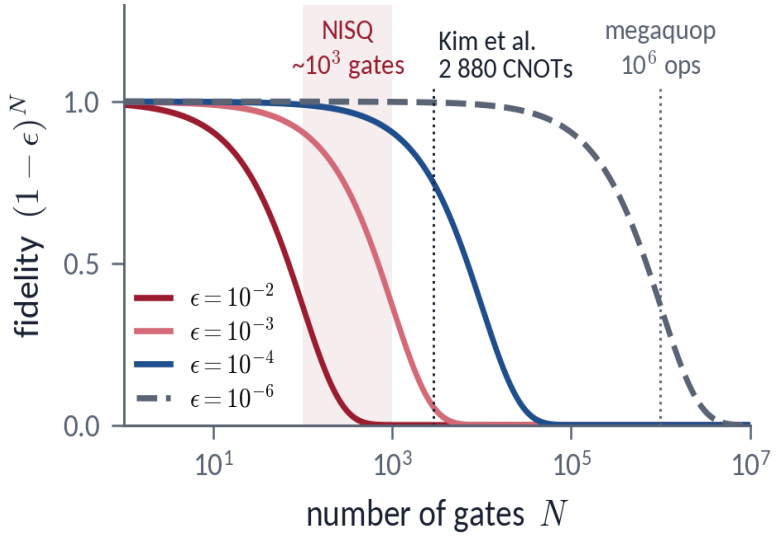


Error mitigation recovered accurate observables from 127-qubit Ising-model circuits.

Fig.: Kim et al., Nature 618, 500 (2023)
Kinoshita et al., Nature 440, 900 (2006)

The NISQ era: noise limits the size of a computation

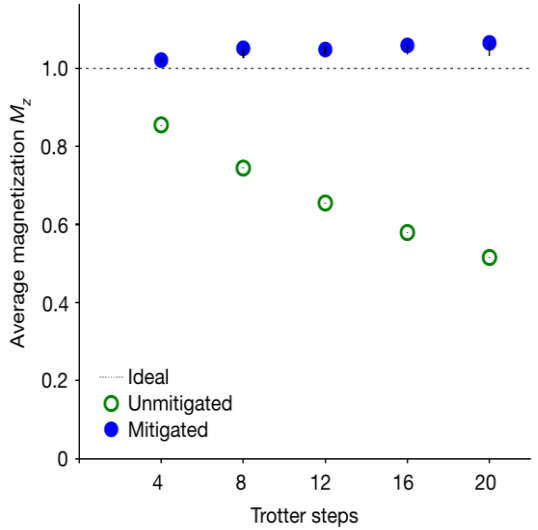
Noise sets a gate budget



Error ε per gate: fidelity ≈ e^(−εN). At ε ≈ 10^{-3} a circuit survives ~10^3 gates; useful algorithms need 10^6, i.e. error correction.

Preskill, J. Quantum 2, 79 (2018);
Preskill, J. ACM Transactions on Quantum Computing, 6(3), 1-7 (2025).

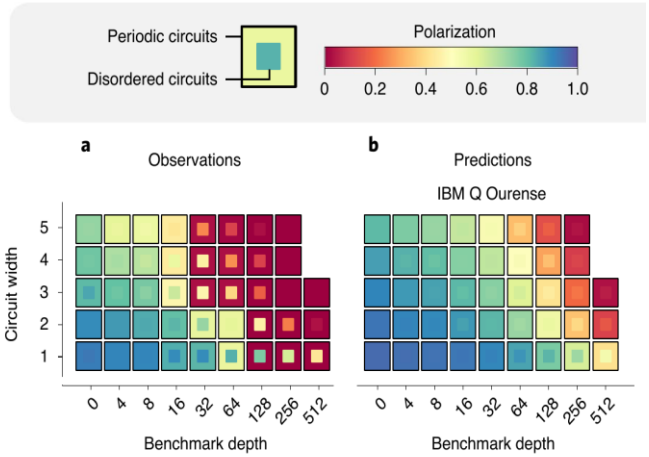
Measured observable decays



127 qubits: the ideal value is 1; the raw data decay with depth, and only error mitigation recovers them.

Kim et al., Nature 618, 500 (2023)

One error rate is not enough



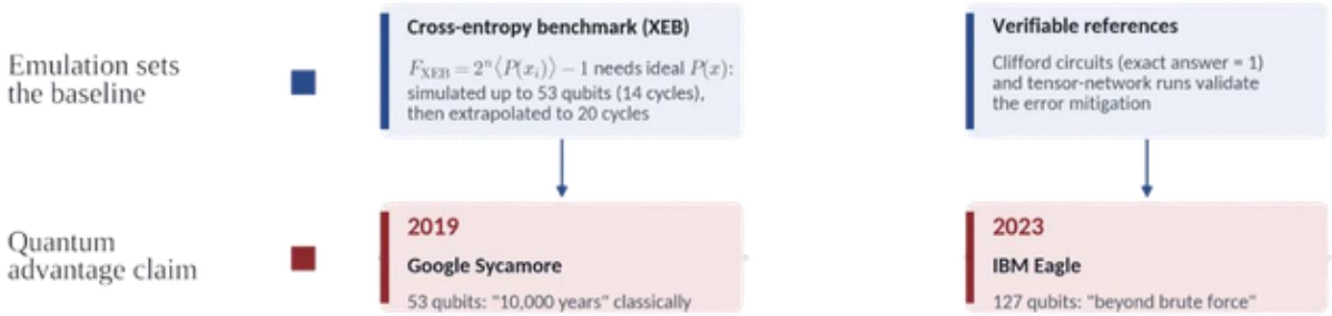
Structured (periodic) circuits fail far earlier than their error rates predict: up to 10× across 12 processors.

Proctor et al., Nat. Phys. 18, 75 (2022)

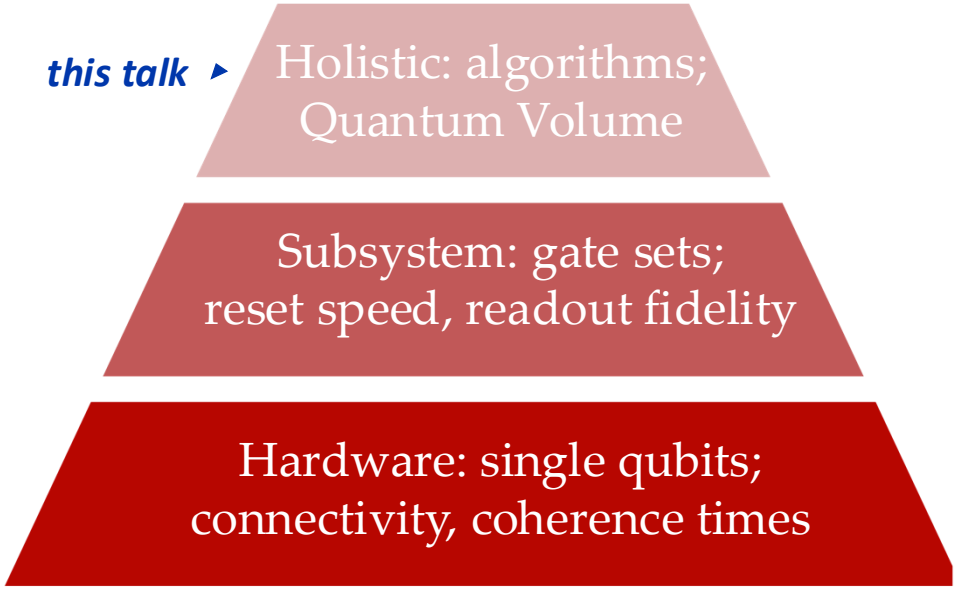
→ Our work: use a structured algorithm like Shor's under the effect of controlled noise

Importance of benchmarking

→ **Benchmarking: How faithful is a quantum device or a classical emulation?**



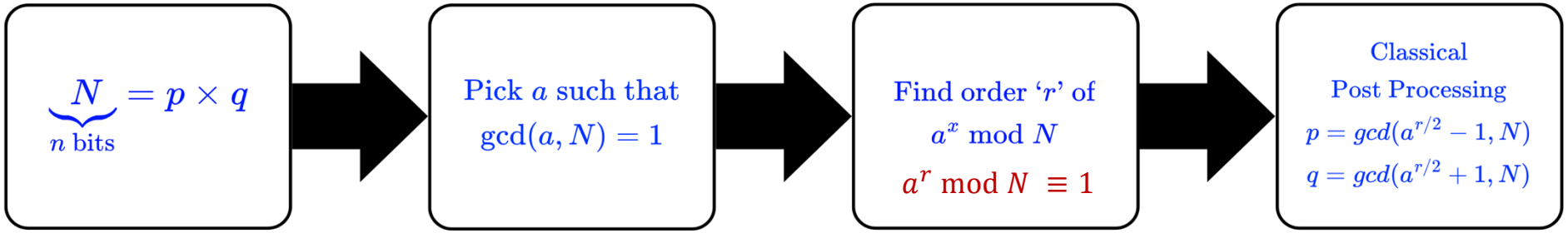
this talk ▸

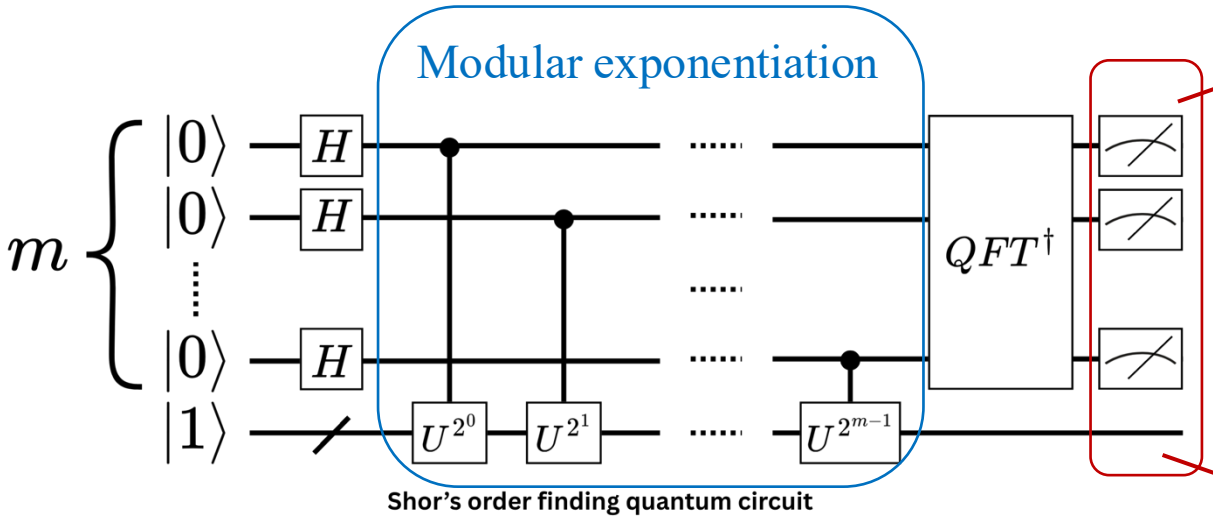


Our benchmark: Shor's algorithm

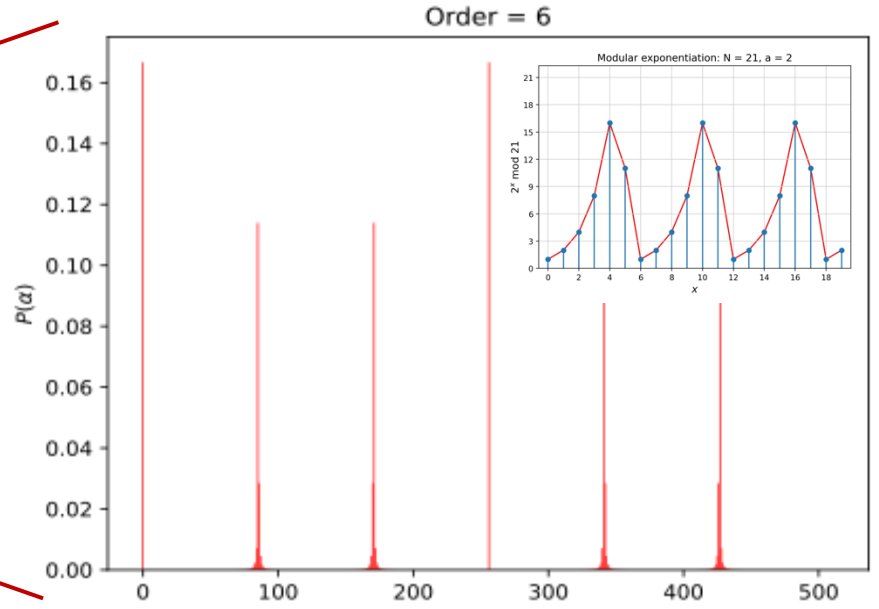
- A fully compiled, deep circuit
- Verifiable output
- Entanglement study

Shor's Algorithm





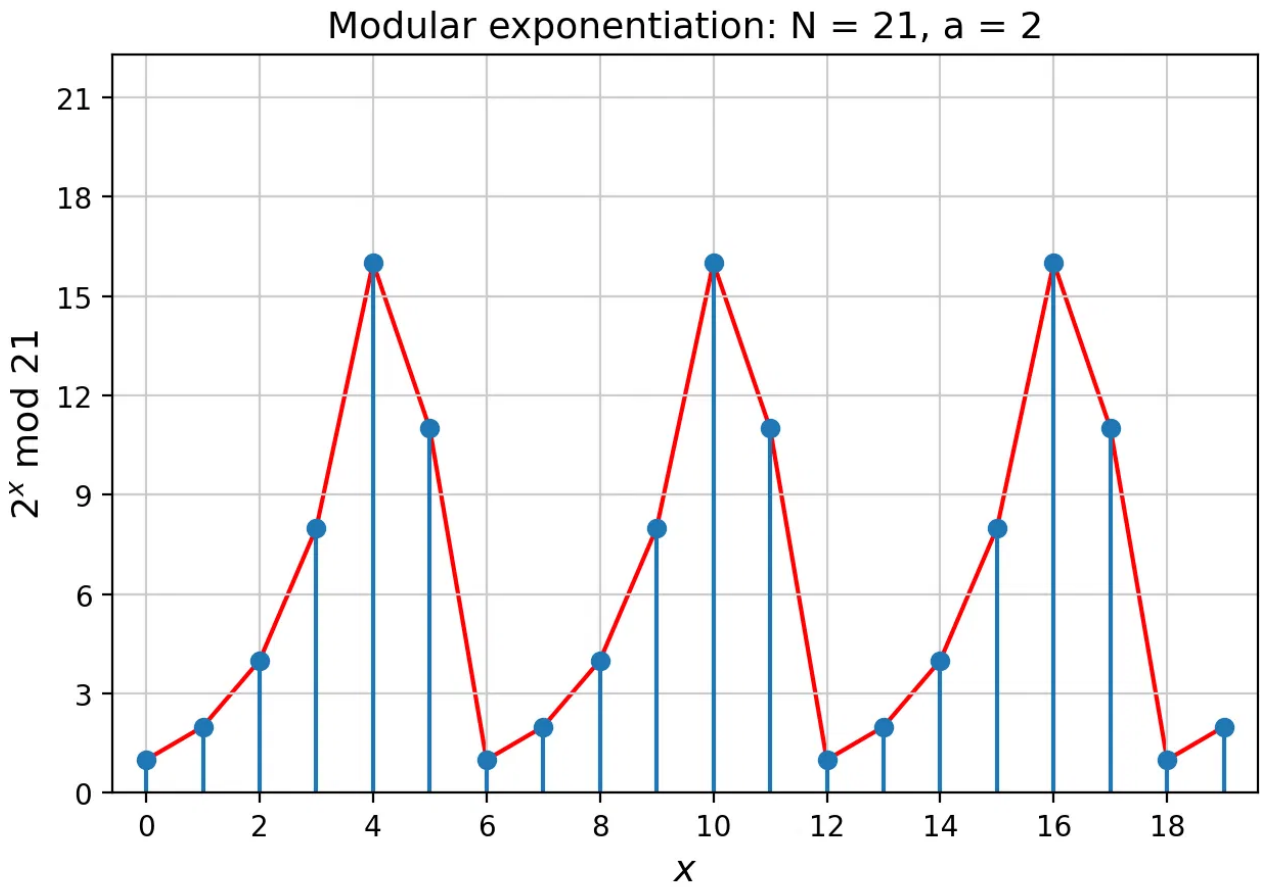
Shor's order finding quantum circuit

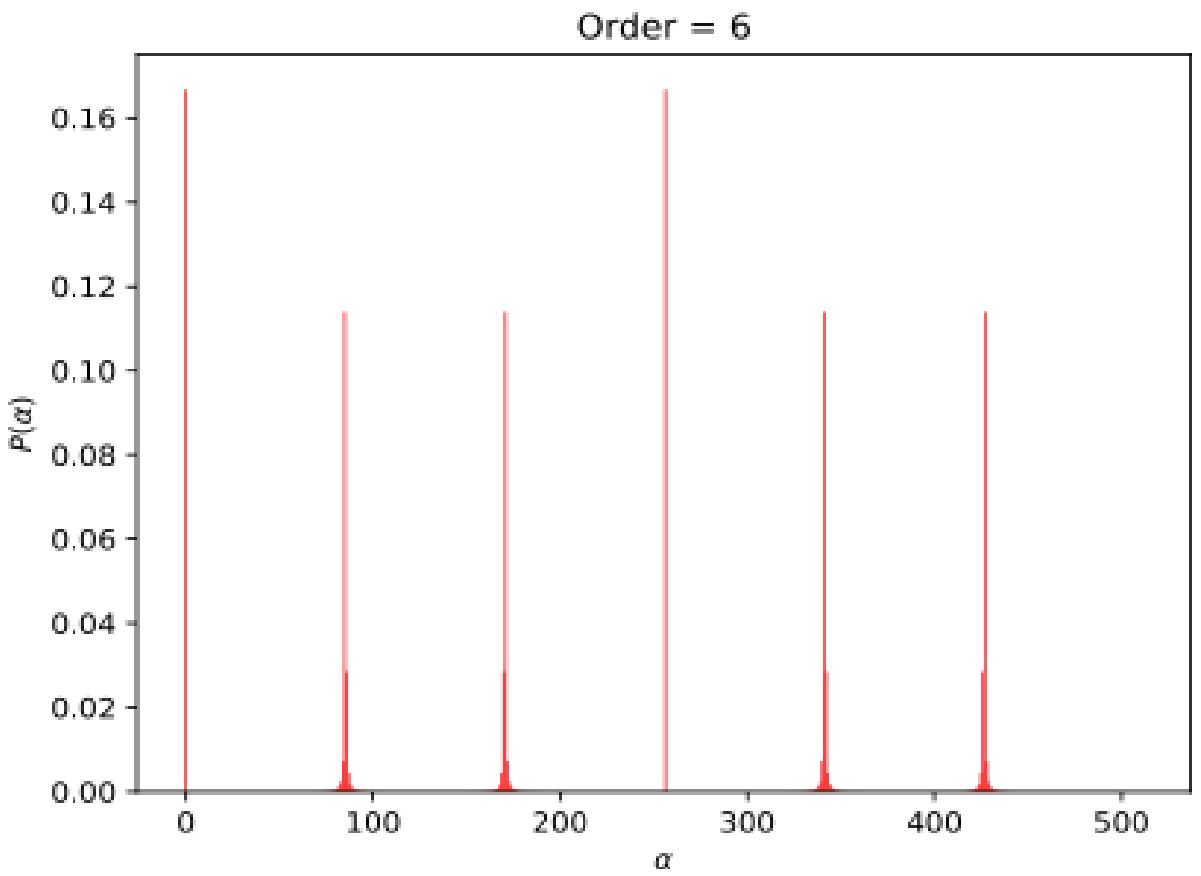


Order found using the phase estimation circuit: modular exponentiation + QFT inverse

Exact output distribution: peaked around $2^{2n}/r$
Continued fractions recover r

Shor's Algorithm

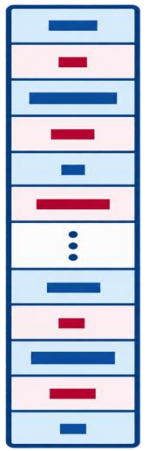




N = 21, a = 2 gives order (r) = 6 i.e.
$2^r \bmod 21 \equiv 1$

Exact output distribution: peaked around $2^{2n}/r$
Continued fractions recover r

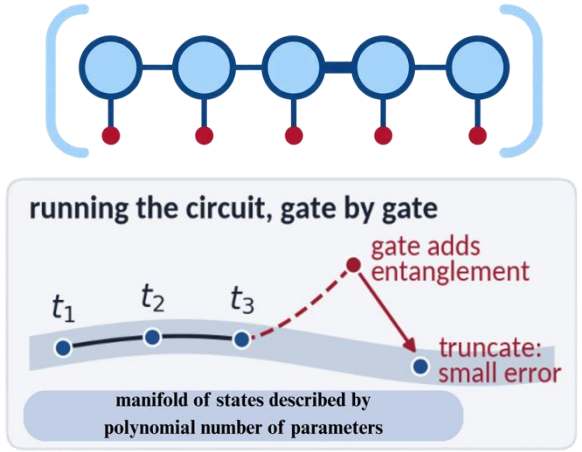
Classical simulations of quantum circuits



State vector

Store all amplitudes

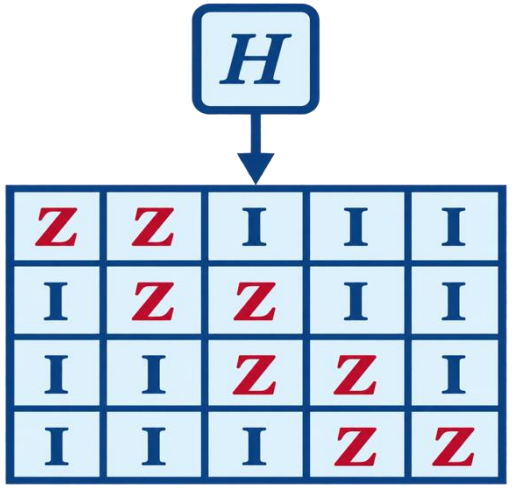
Cost: exponential memory



Tensor networks

Exploit network structure

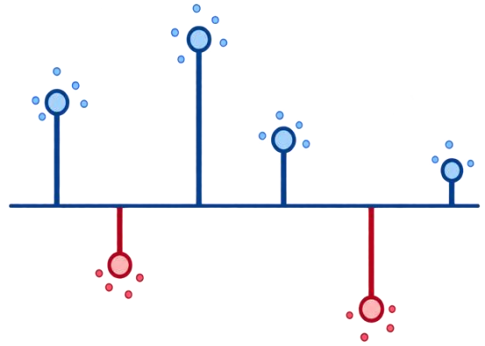
Cost: bond size or network width



Stabilizer methods

Track Clifford structure

Cost: non-Clifford gates



Quasiprobability

Estimate by sampling

Cost: negativity and variance

Exact simulation: exponential

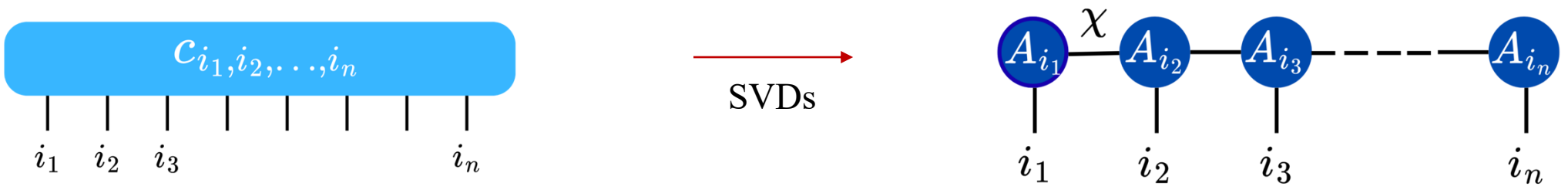
- beyond 40-50 qubits not possible

Classical simulation: approximate and polynomial

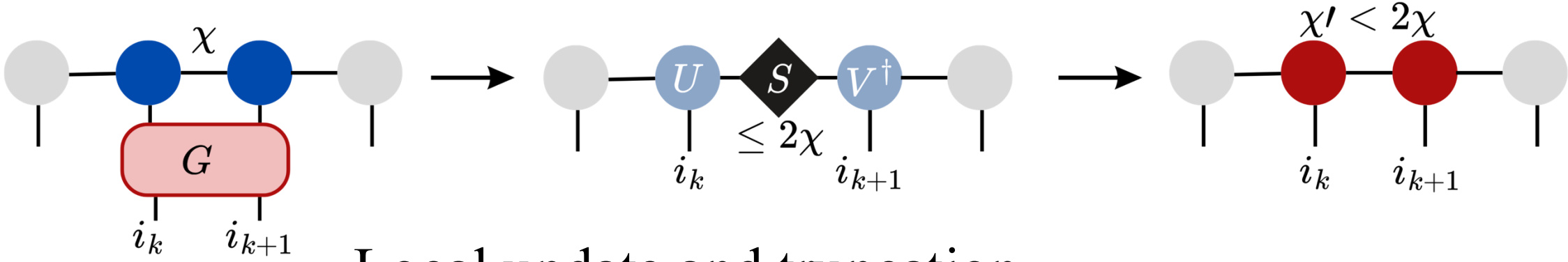
- Not perfect but errors can be controlled to mimic quantum hardware fidelities

Matrix Product States (MPS) simulations

$$|\Psi\rangle = \sum_{i_1,i_2,\ldots,i_n \in (0,1)} c_{i_1,i_2,\ldots,i_n} |i_1, i_2, \ldots, i_n\rangle \qquad |\Psi\rangle = \sum_{i_1,i_2,\ldots,i_n \in (0,1)} A_{i_1} A_{i_2} \ldots A_{i_n} |i_1, i_2, \ldots, i_n\rangle$$

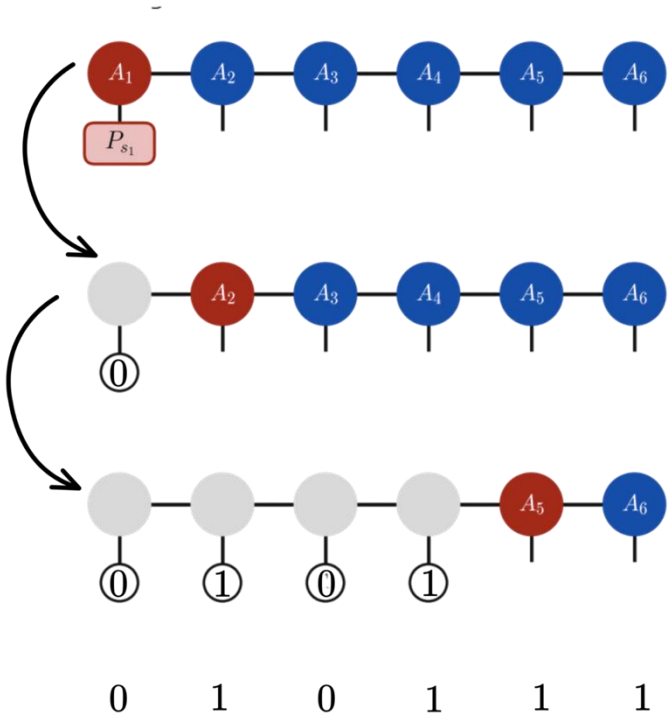


$O(2^n)$ $O(2n\chi^2)$ χ : bond dim



Local update and truncation

Matrix Product States (MPS) simulations

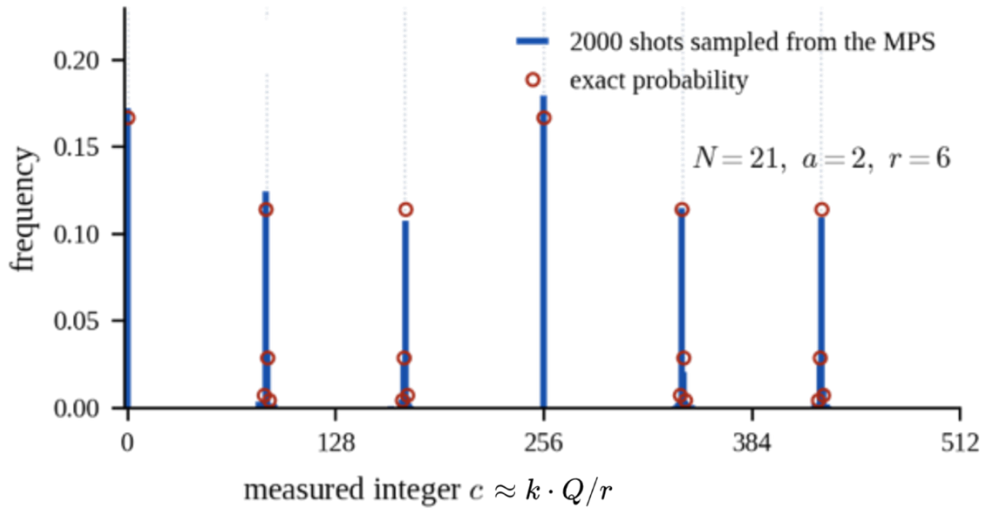


$$p(s_1) = \langle \Psi | P_{s_1} | \Psi \rangle$$

$$u \sim U(0,1):$$
$$s_1 = 0 \text{ if } u < p(0)$$

$$p(\mathbf{s}) = p(s_1)p(s_2|s_1)\cdots$$
$$\mathcal{O}(2mn\chi^2): \ m \text{ shots}$$

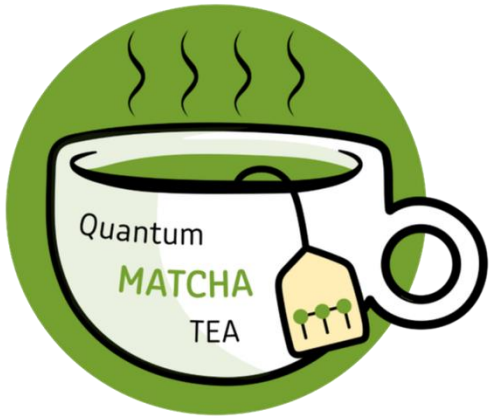
bit string sampled in one shot



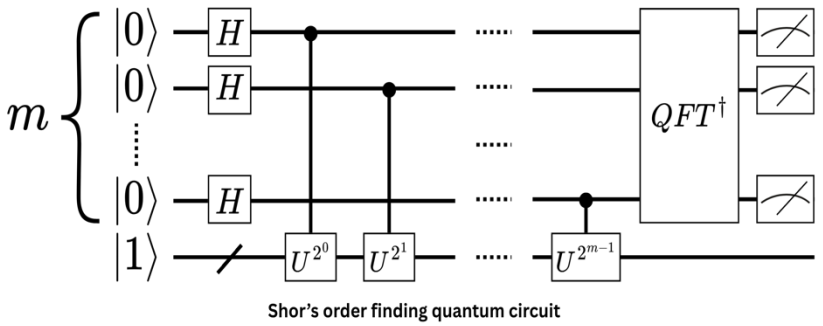
Q : top register with 9 qubits

r : order

- Each shot drawn independently from the MPS
- Similar to the measurements from an experiment



Shor's Algorithm – simulating the ME circuit



Shor's order finding quantum circuit

7n + 2 qubits

O(n³) gates

5 types of gates: **H, X, CX, SWAP, CCX**

PHYSICAL REVIEW A VOLUME 54, NUMBER 1 JULY 1996

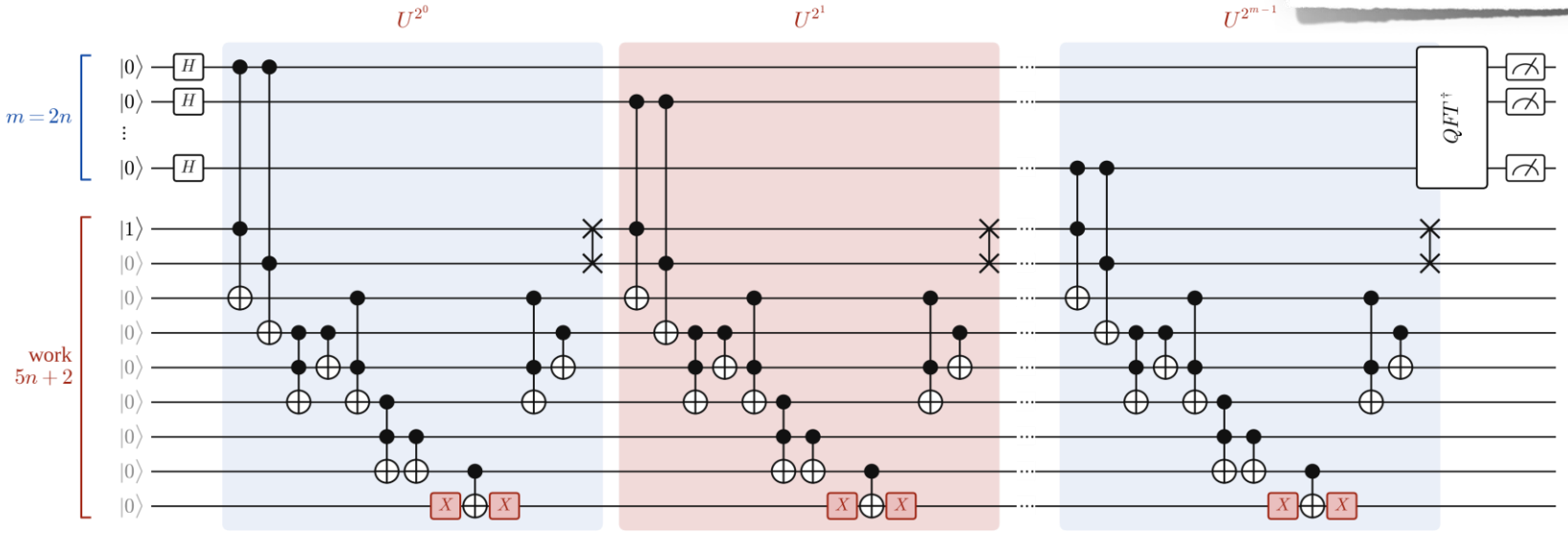
Quantum networks for elementary arithmetic operations

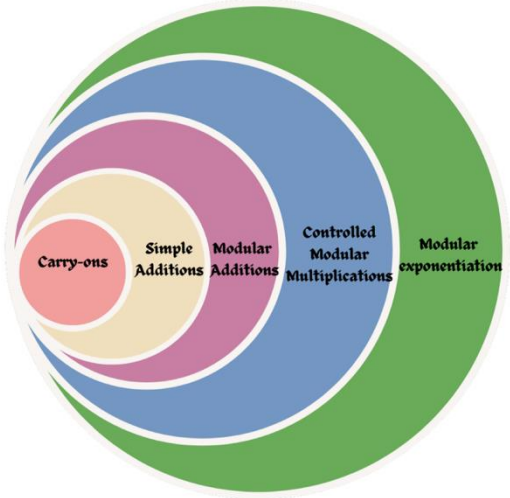
Vlatko Vedral,* Adriano Barenco, and Artur Ekert
Clarendon Laboratory, Department of Physics, University of Oxford, Oxford OX1 3PU, United Kingdom

(Received 3 November 1995)

Quantum computers require quantum arithmetic. We provide an explicit construction of quantum networks effecting basic arithmetic operations: from addition to modular exponentiation. Quantum modular exponentiation seems to be the most difficult (time and space consuming) part of Shor's quantum factorizing algorithm. We show that the auxiliary memory required to perform this operation in a reversible way grows linearly with the size of the number to be factorized. [S1050-2947(96)05707-1]

PACS number(s): 03.65.Ca, 07.05.Bx, 89.80.+h

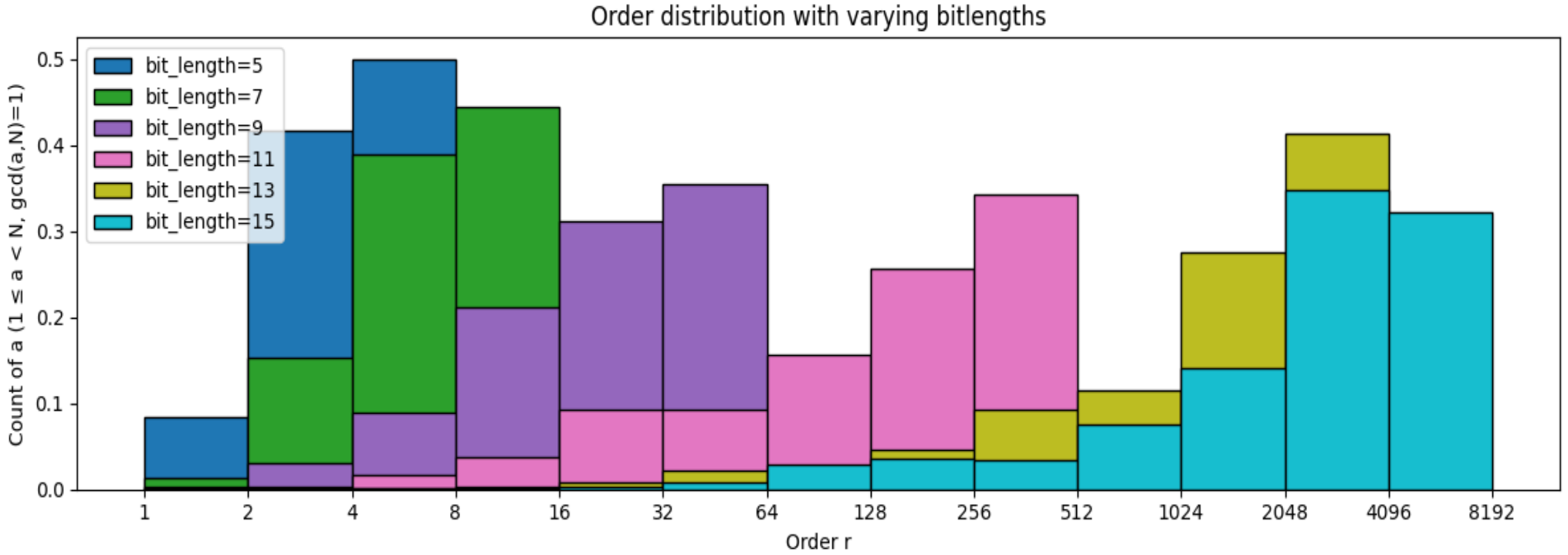




Most simulations ~ 100k gates

Largest simulation ~ 4M gates (bit-length = 26, nqubits = 184)

Factors affecting simulation cost



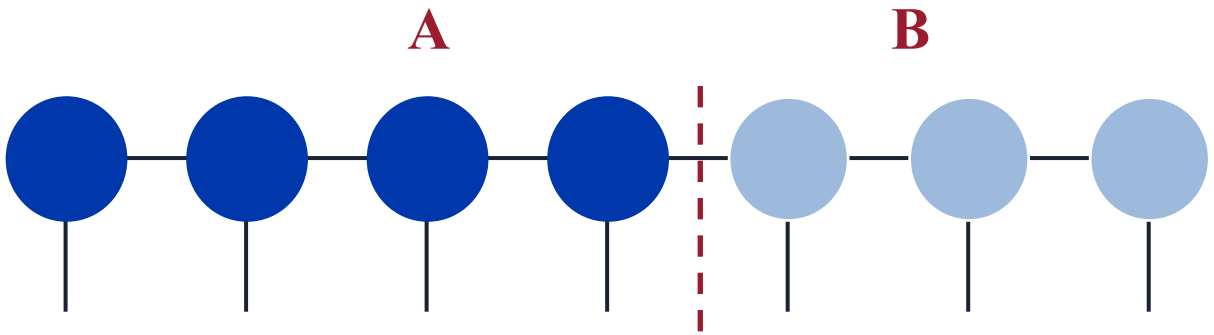
Complexity depends on the number of bits (n)?

Naïve guess would be yes

The choice of co-prime (a) we randomly pick?

Less obvious

Factors affecting simulation cost



$$\sum_{k=1}^{\chi} \sqrt{\lambda_k}\, |\phi_k\rangle_A |\nu_k\rangle_B$$

Maximal accessible Schmidt rank limited by the bond dimension

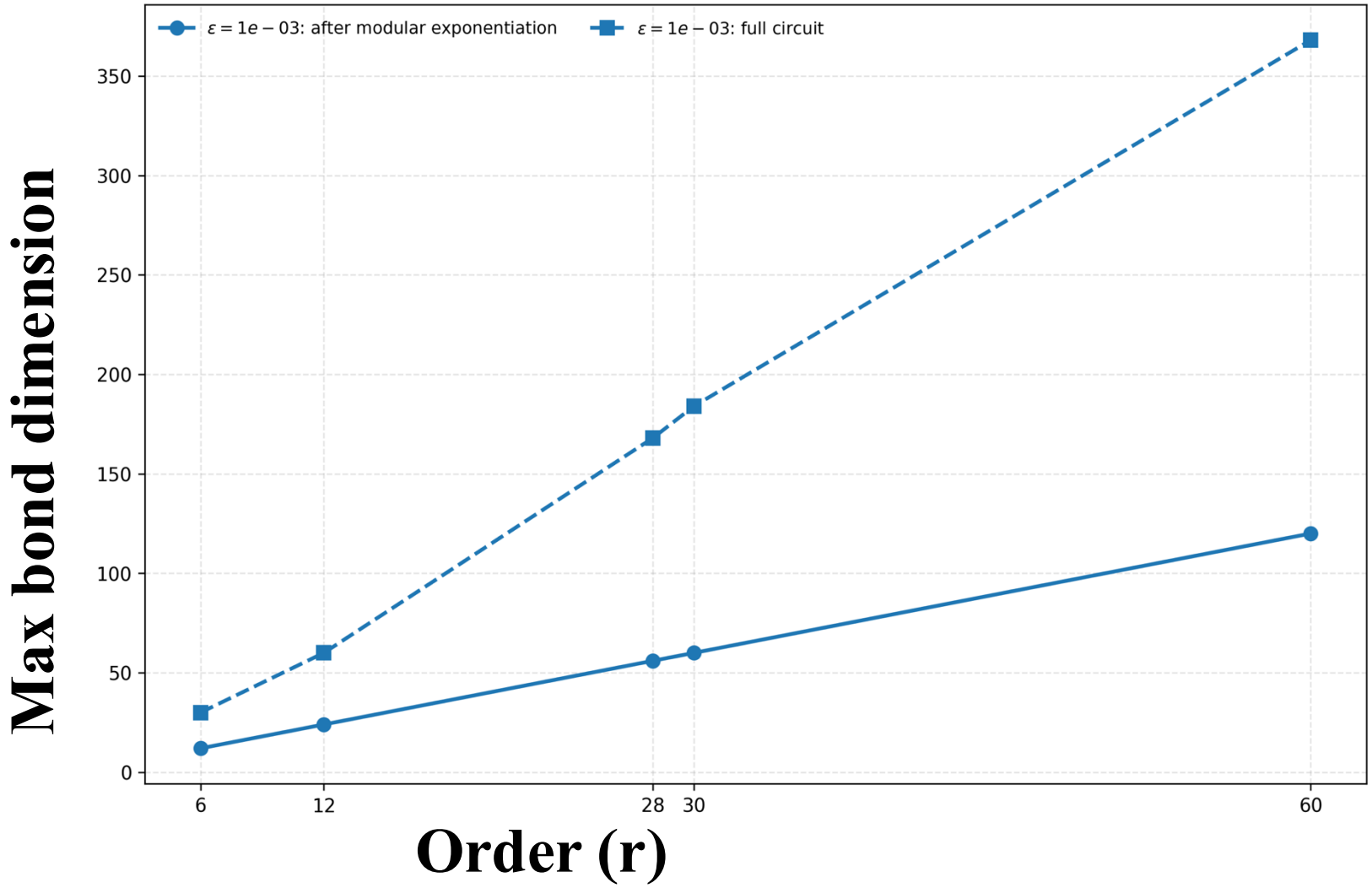
A: *m* qubit 'register'

B: *5n+2* qubit 'ancilla'

$$|\psi\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r} |k\rangle_A |a^k \bmod N\rangle_B$$

Schmidt rank after modular exponentiation is determined by *r*

Factors affecting simulation cost



Reported for oracle-level simulations

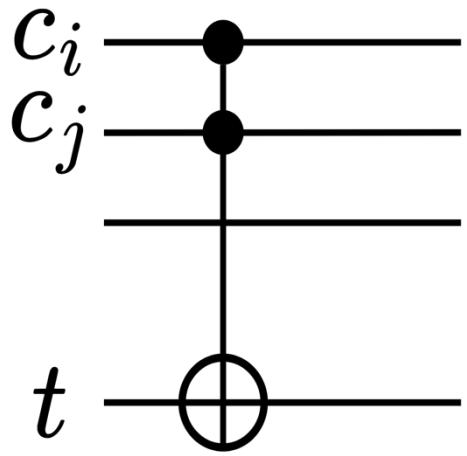
Dang, Hill, Hollenberg, Quantum 3, 116 (2019)

Dumitrescu, Physical Review A, 96(6), 062322 (2017)

Confirmed here for the full gate-level circuit simulation

Circuit optimizations

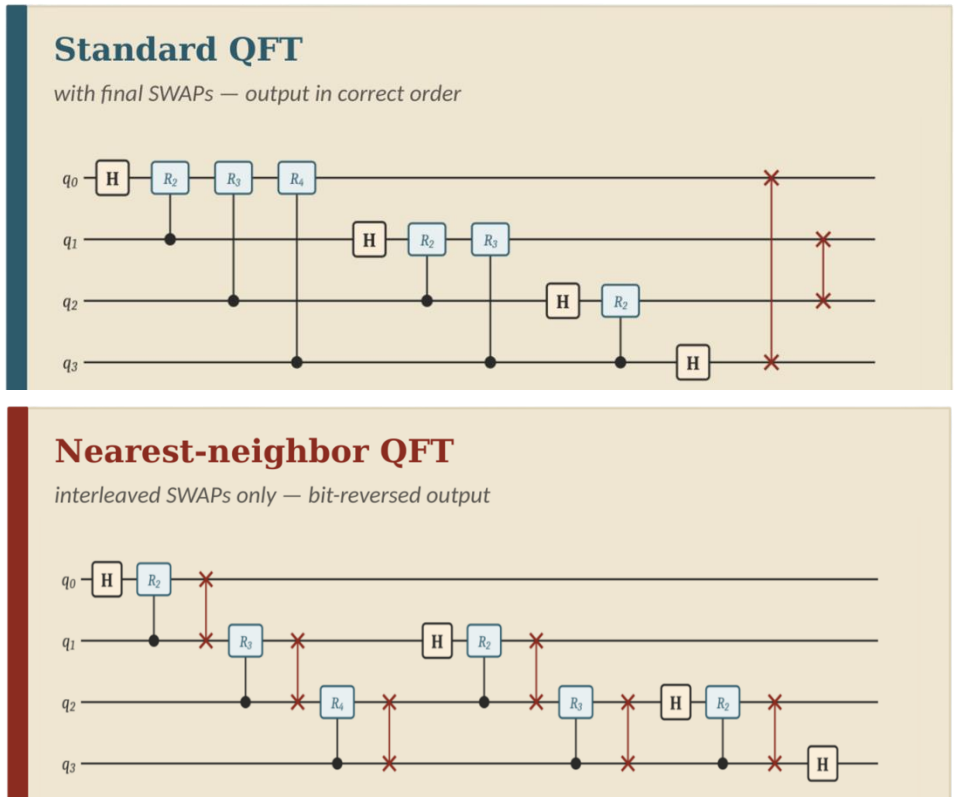
Toffoli gate → one MPO with $\chi = 2$



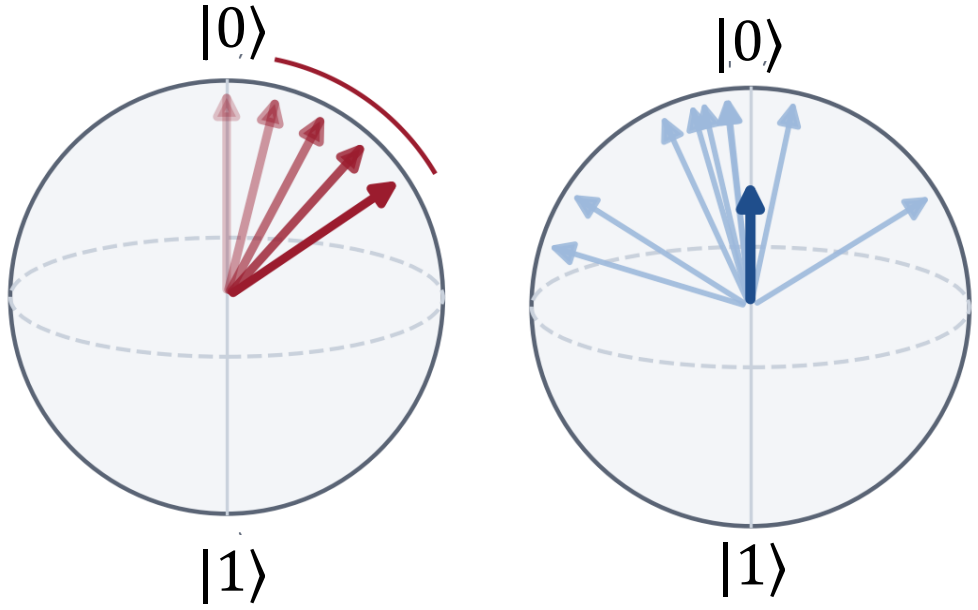
Applied exactly: no decomposition into 1 and 2 qubit gates, shallower circuit, no extra truncation.

MPO bond dim doesn't increase with the number of controls

Nearest-neighbor QFT†



Modelling noise in Shor's algorithm

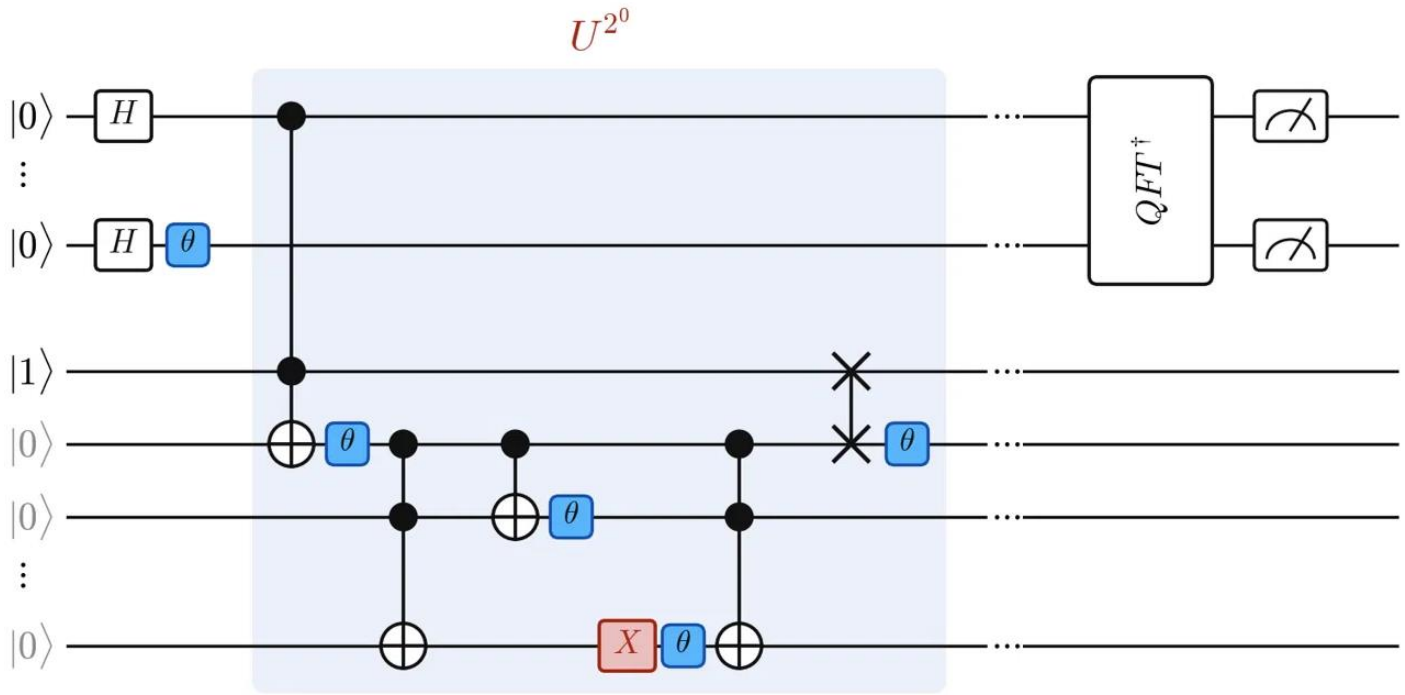


coherent noise

miscalibrated rotations: errors add in amplitude

incoherent noise

dephasing, random kicks: errors add in probability



θ = $e^{i\theta\sigma_z}$

Random unitary overrotations occurring with probability p at each qubit-gate instance

Figures of merit

Fidelity estimate: approximation to the fidelity of the final state (n qubits) solely in terms of truncated singular values

$$\mathcal{F}(n) \approx \prod_{i=1}^{n} f_i, \qquad f_i = \frac{\sum_{\mu=1}^{\chi} S_\mu^2}{\sum_{\mu=1}^{2\chi} S_\mu^2}$$

f_i : effective fidelity of a two-qubit gate

S_μ : non-zero singular values remaining

Zhou, Stoudenmire, Waintal, Physical Review X, 10(4), 041038 (2020)

Success probability: most straightforward metric

$$P_{succ} = \frac{\text{No. of instances factors are obtained correctly}}{\text{Total no. of shots}}$$

Figures of merit

Jensen-Shannon (JS) divergence: distance from the ideal distribution, finite, bounded

$$D_{JS}(p(x)||q(x)) = \frac{1}{2}D_{KL}(p(x)||m(x)) + \frac{1}{2}D_{KL}(q(x)||m(x))$$

$$D_{KL}(p(x)||q(x)) = \sum_{x\in X} p(x)\ln\frac{p(x)}{q(x)}$$

$p(x)$: true distribution

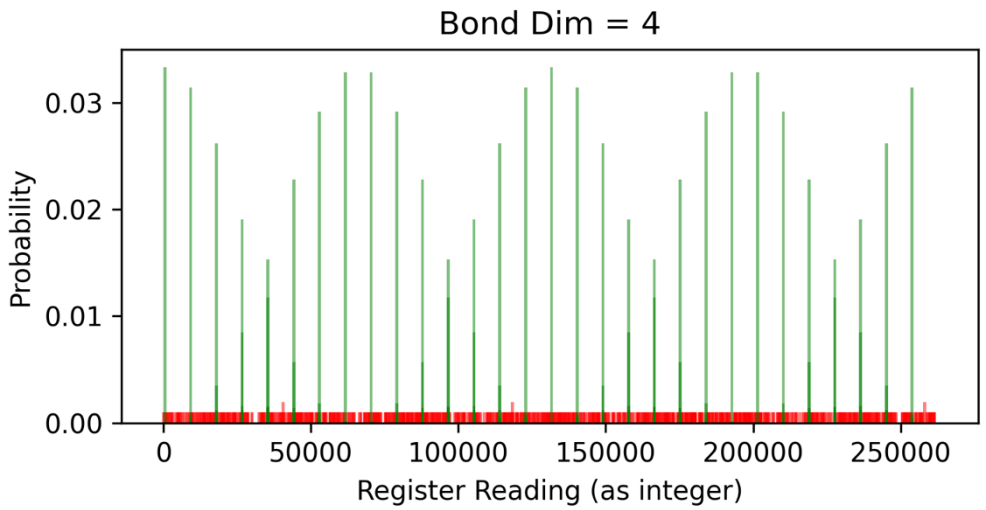
$$P(\alpha) = \frac{1}{2^{2m}}\sum_{k=0}^{r-1}\frac{\sin^2\left[\pi(M+1)\frac{r\alpha}{2^m}\right]}{\sin^2\left(\pi\frac{r\alpha}{2^m}\right)} \qquad M = \left\lfloor\frac{2^m - k - 1}{r}\right\rfloor$$

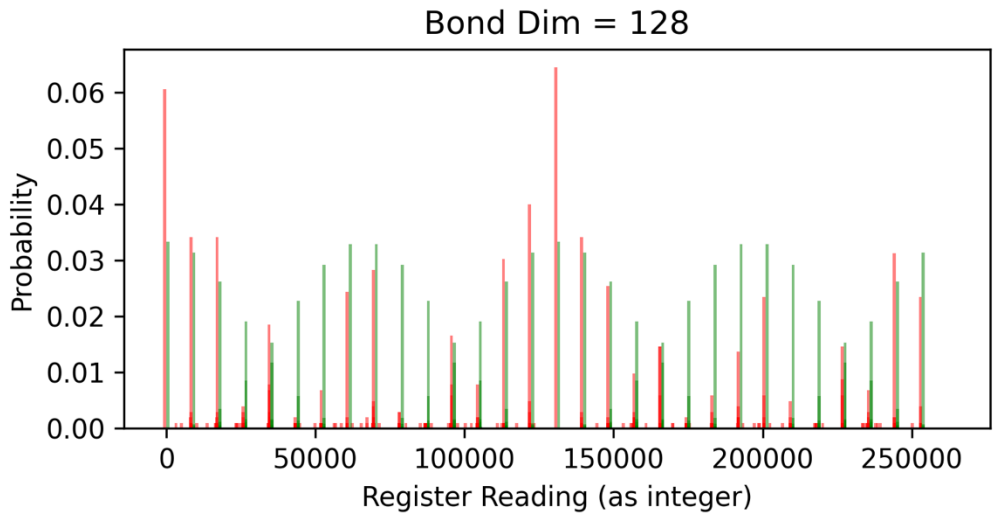
Einarsson(2003)

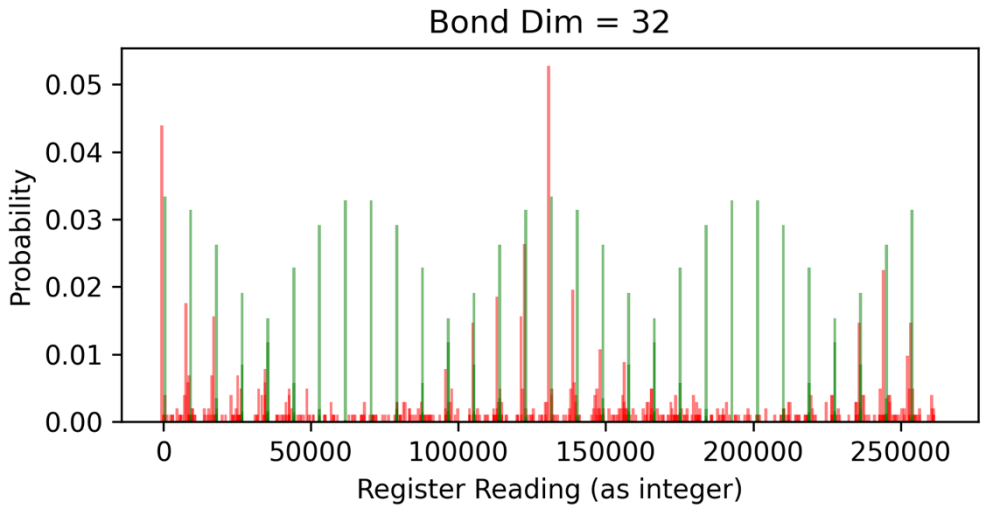
$q(x)$: sampled distribution from MPS

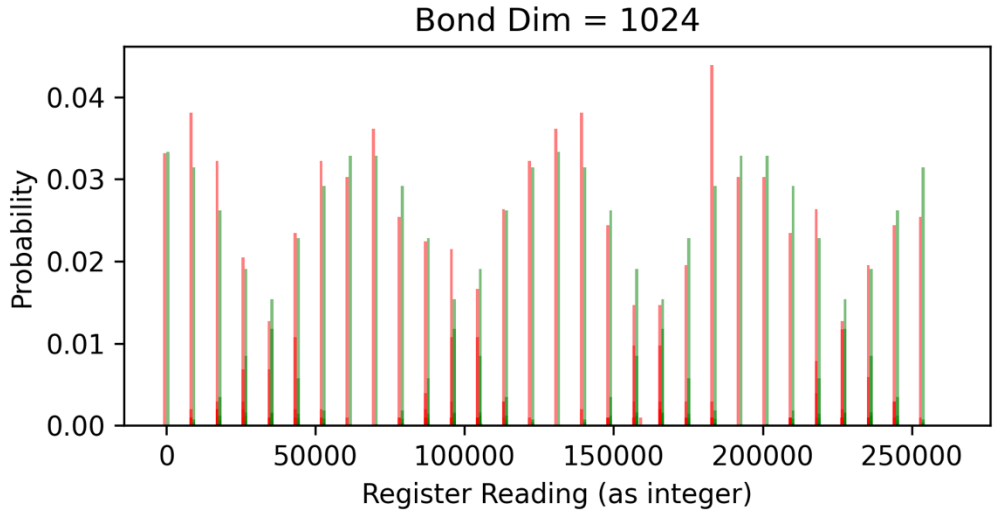
Performance of Shor without noise

Sampling with 1024 shots
Analytic solution

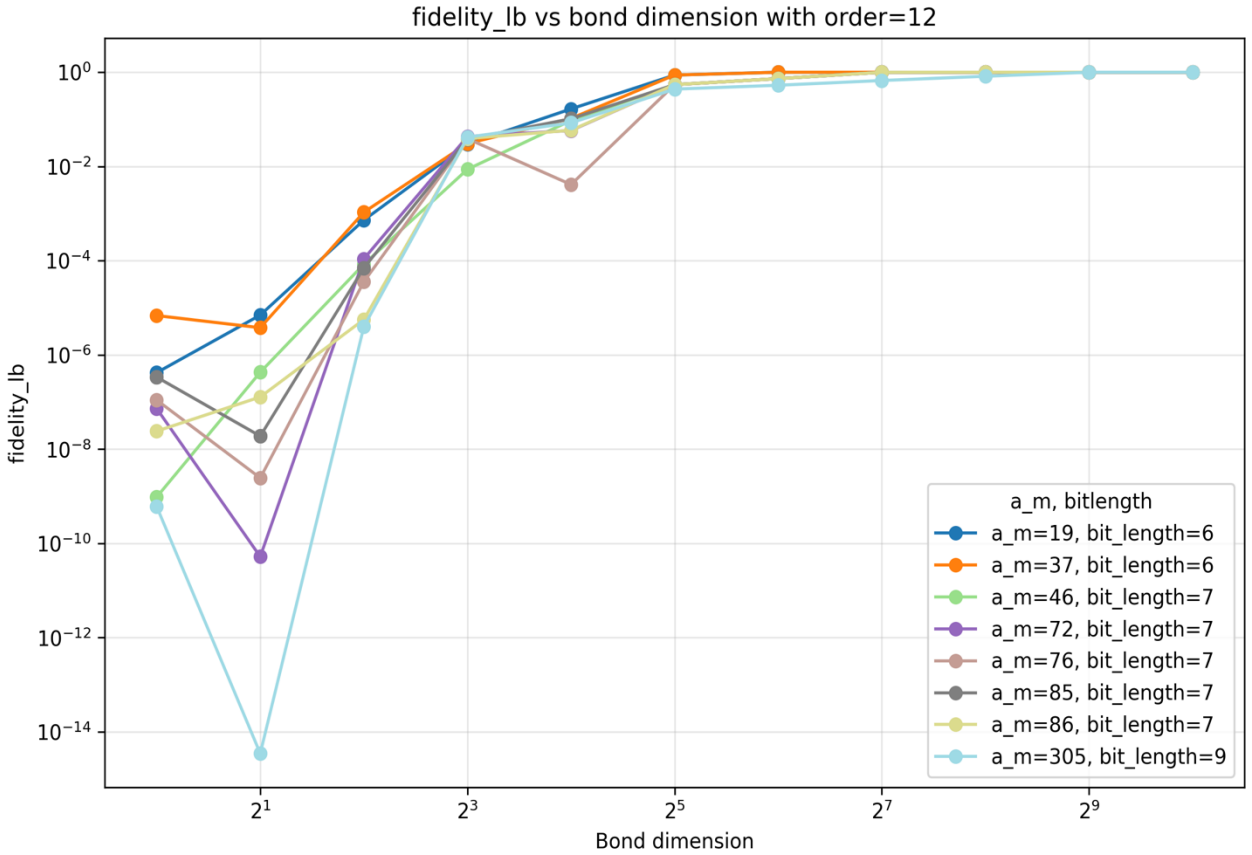


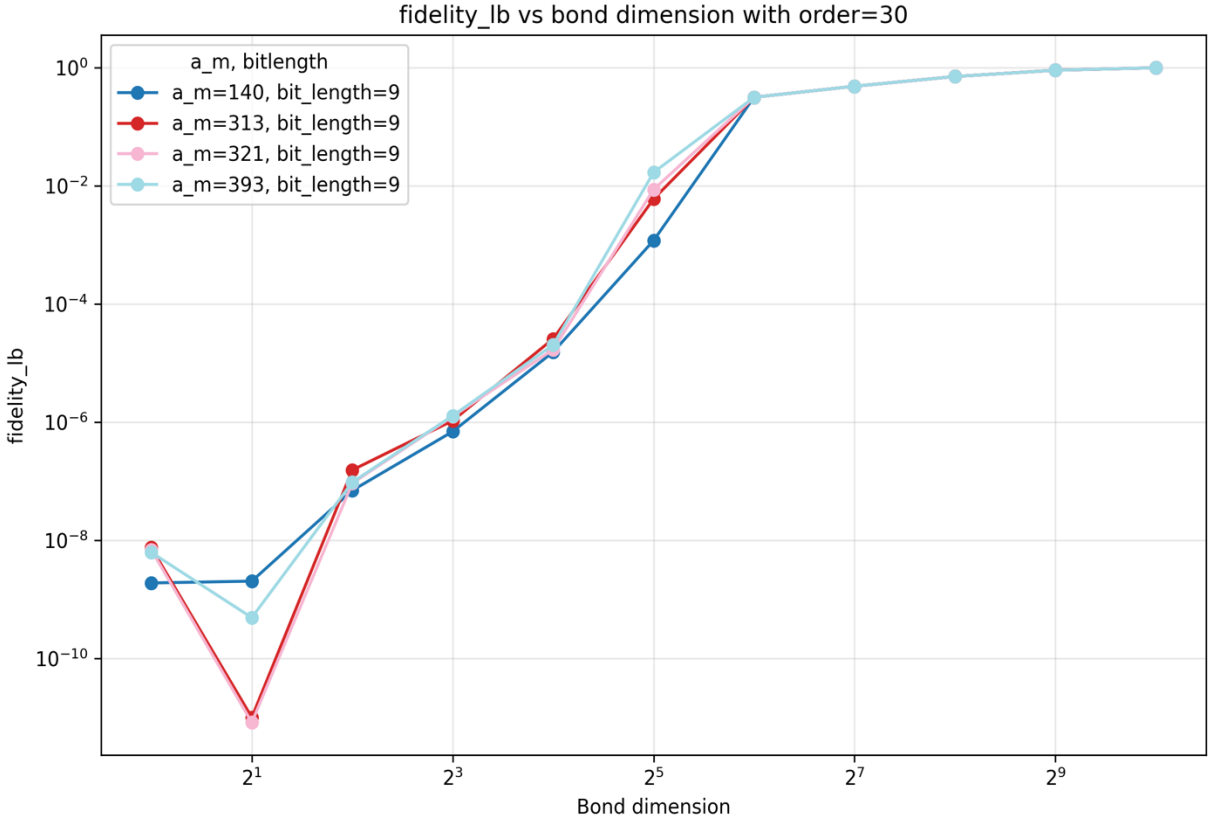




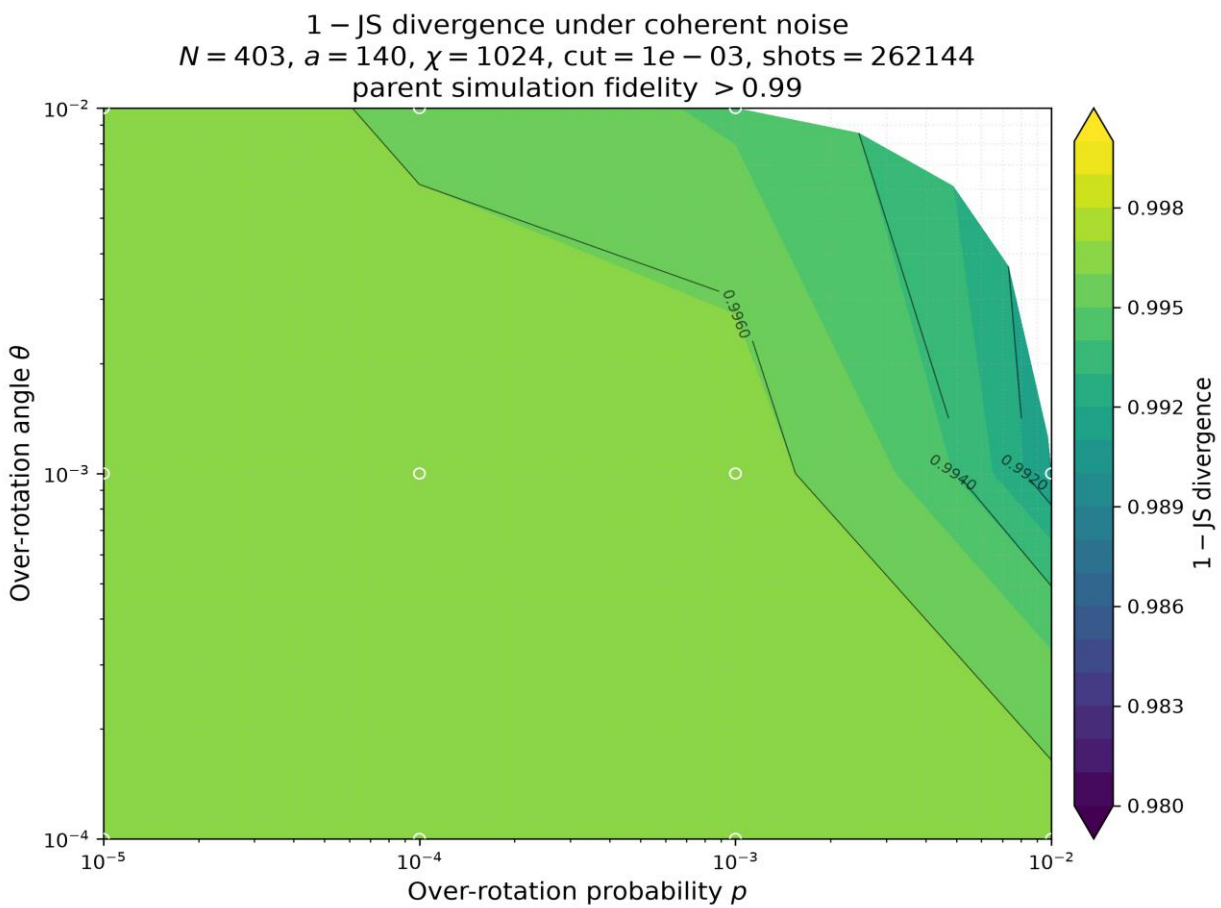


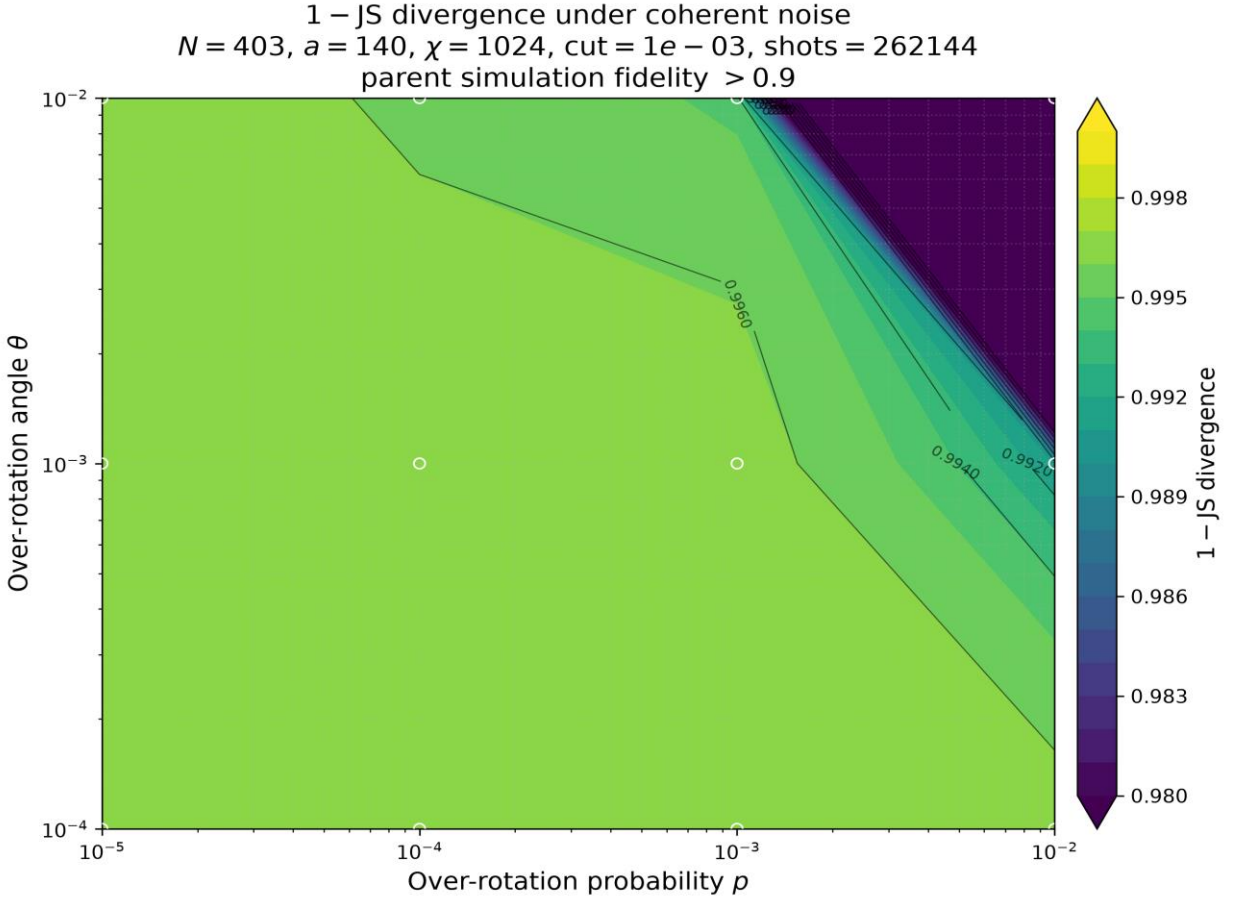
Performance of Shor without noise





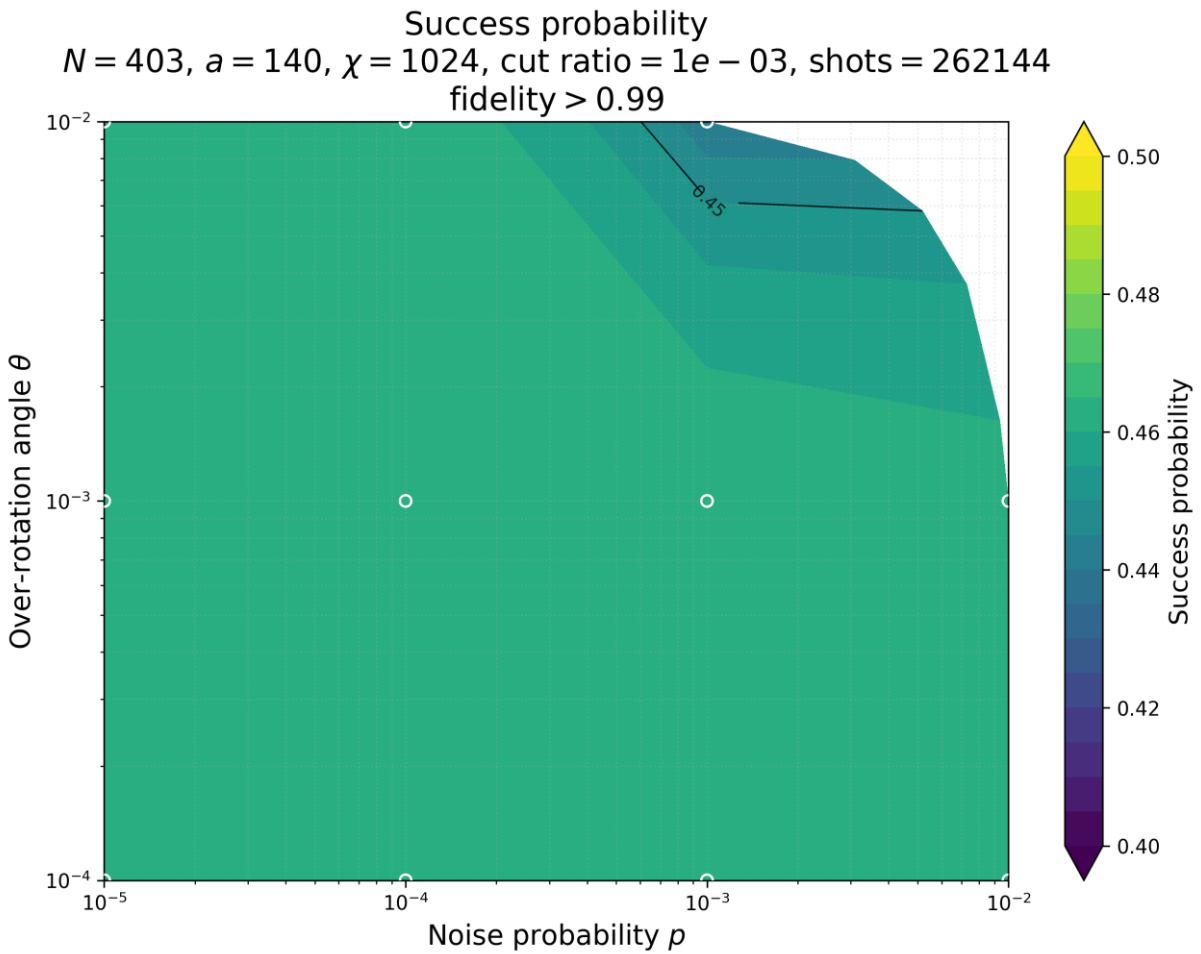
Performance of Shor with circuit noise (JS divergence)

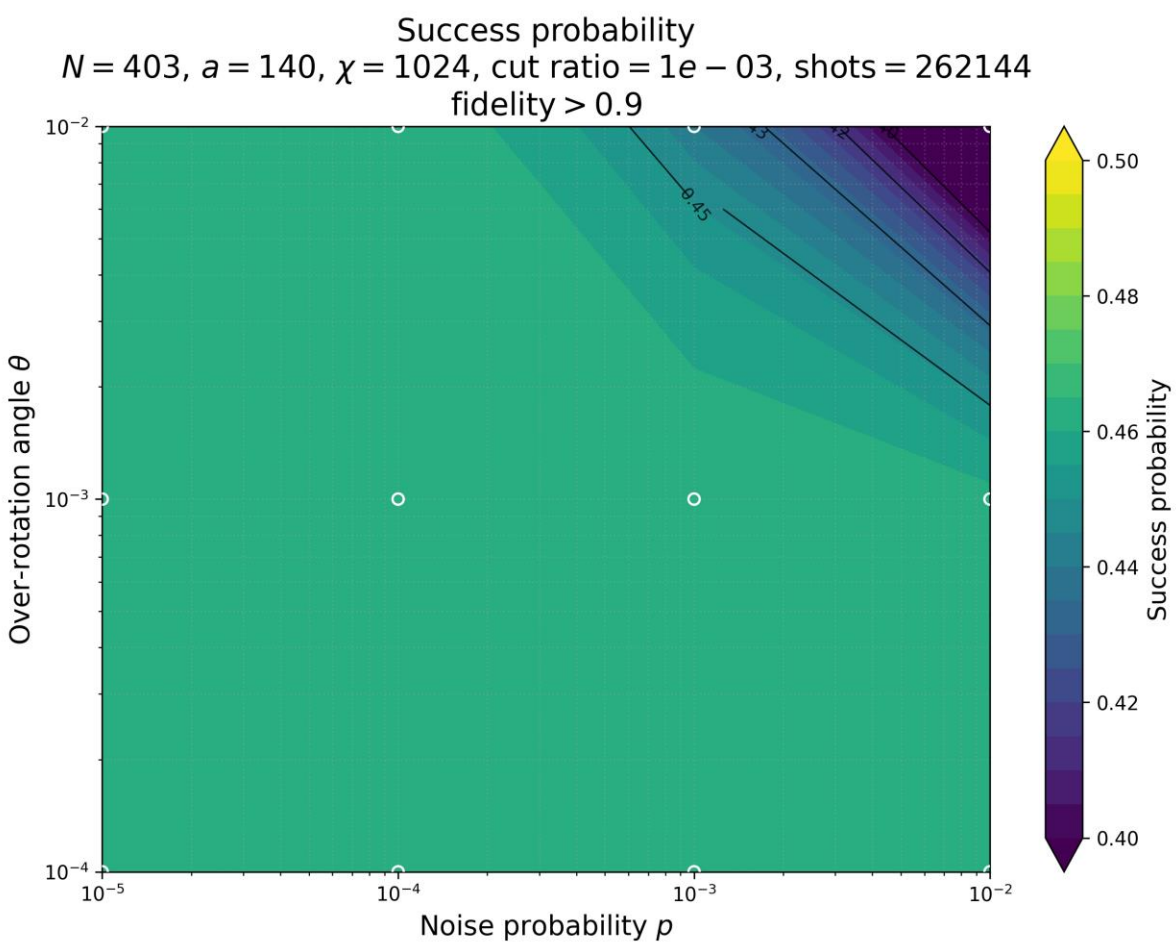




Order (r) = 30, $\chi_{max} = 1024$, cut-ratio (ϵ) = 10^{-3}

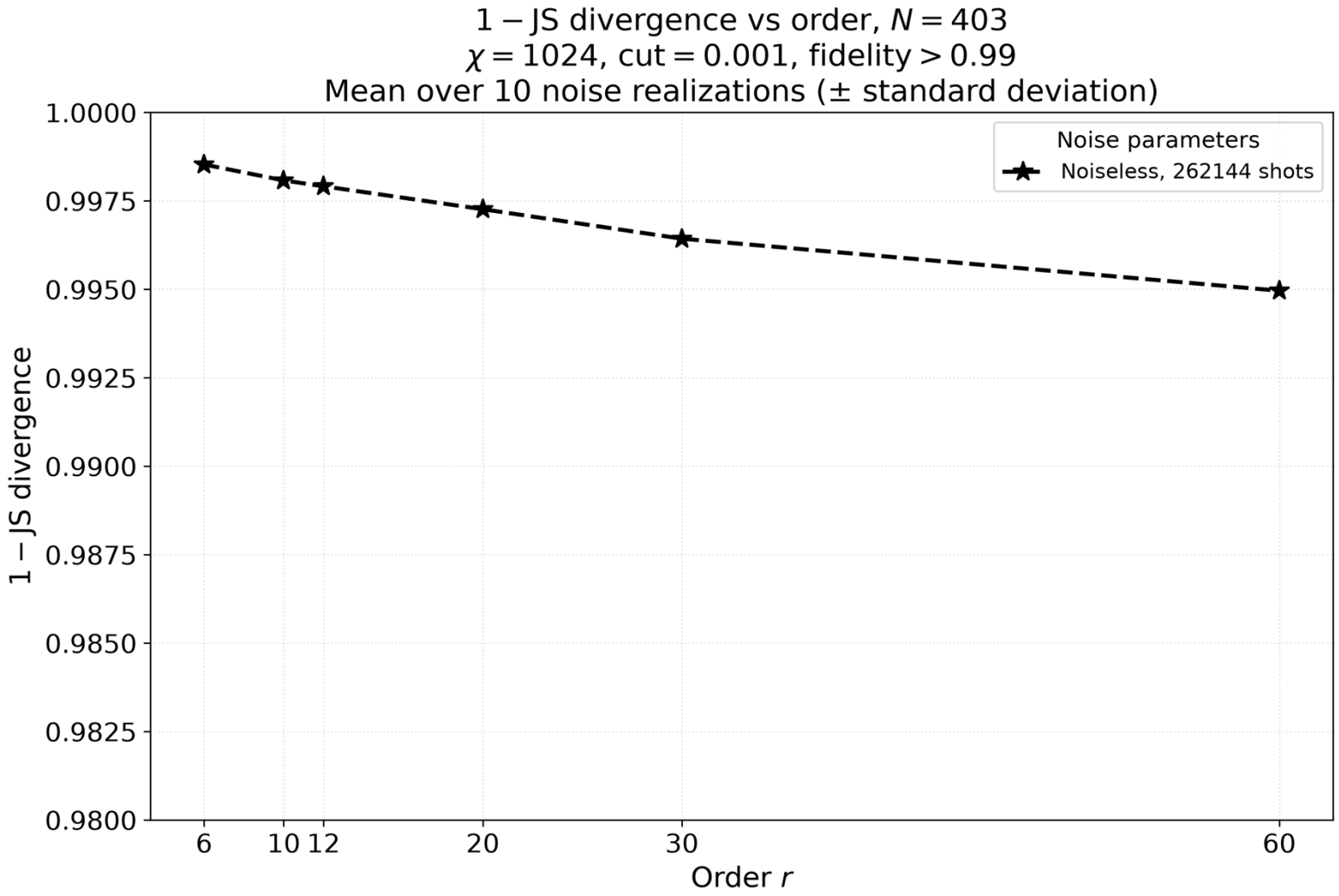
Performance of Shor with circuit noise (success probability)



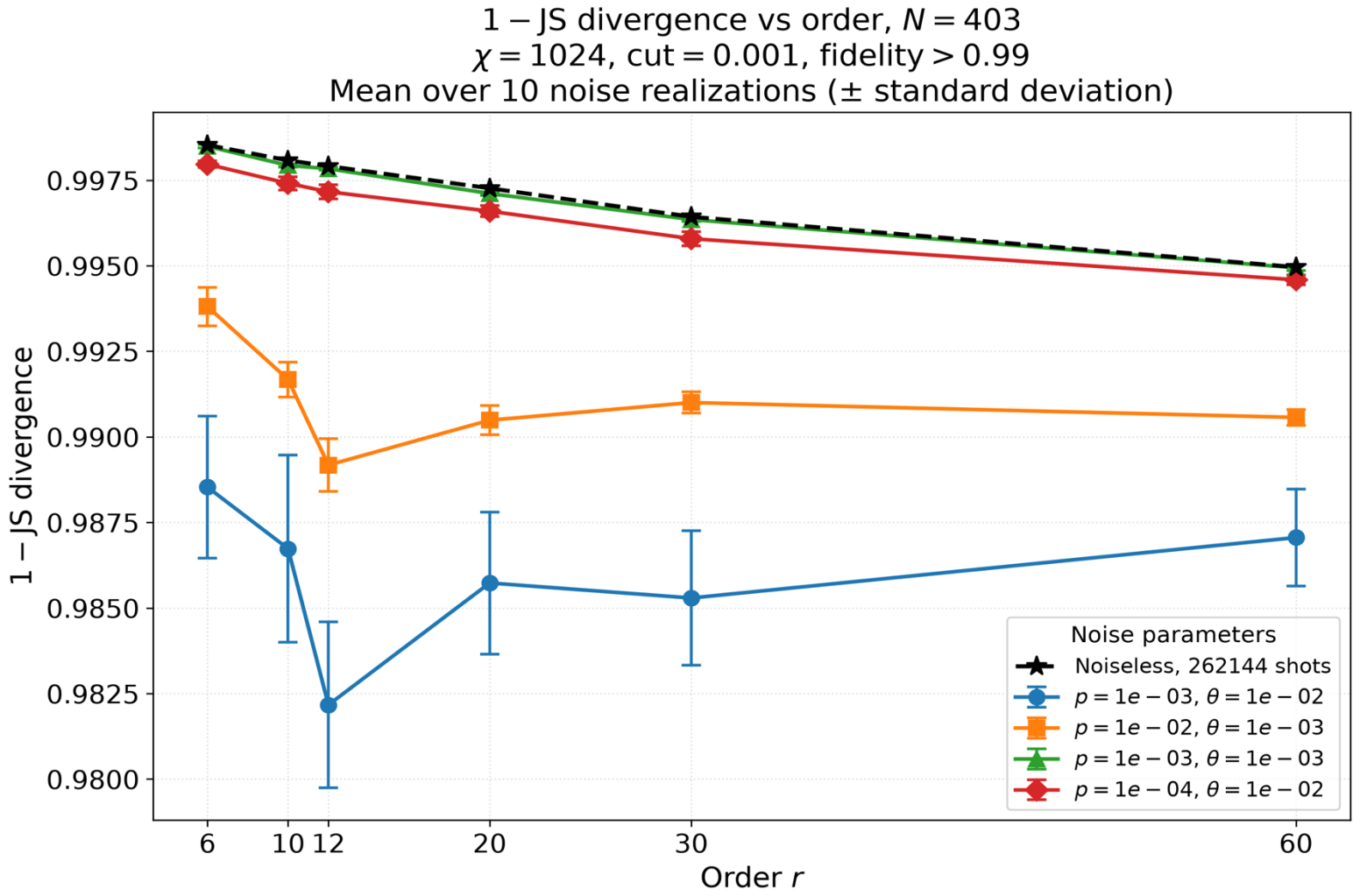


Order (r) = 30, $\chi_{max} = 1024$, cut-ratio (ϵ) = 10^{-3}

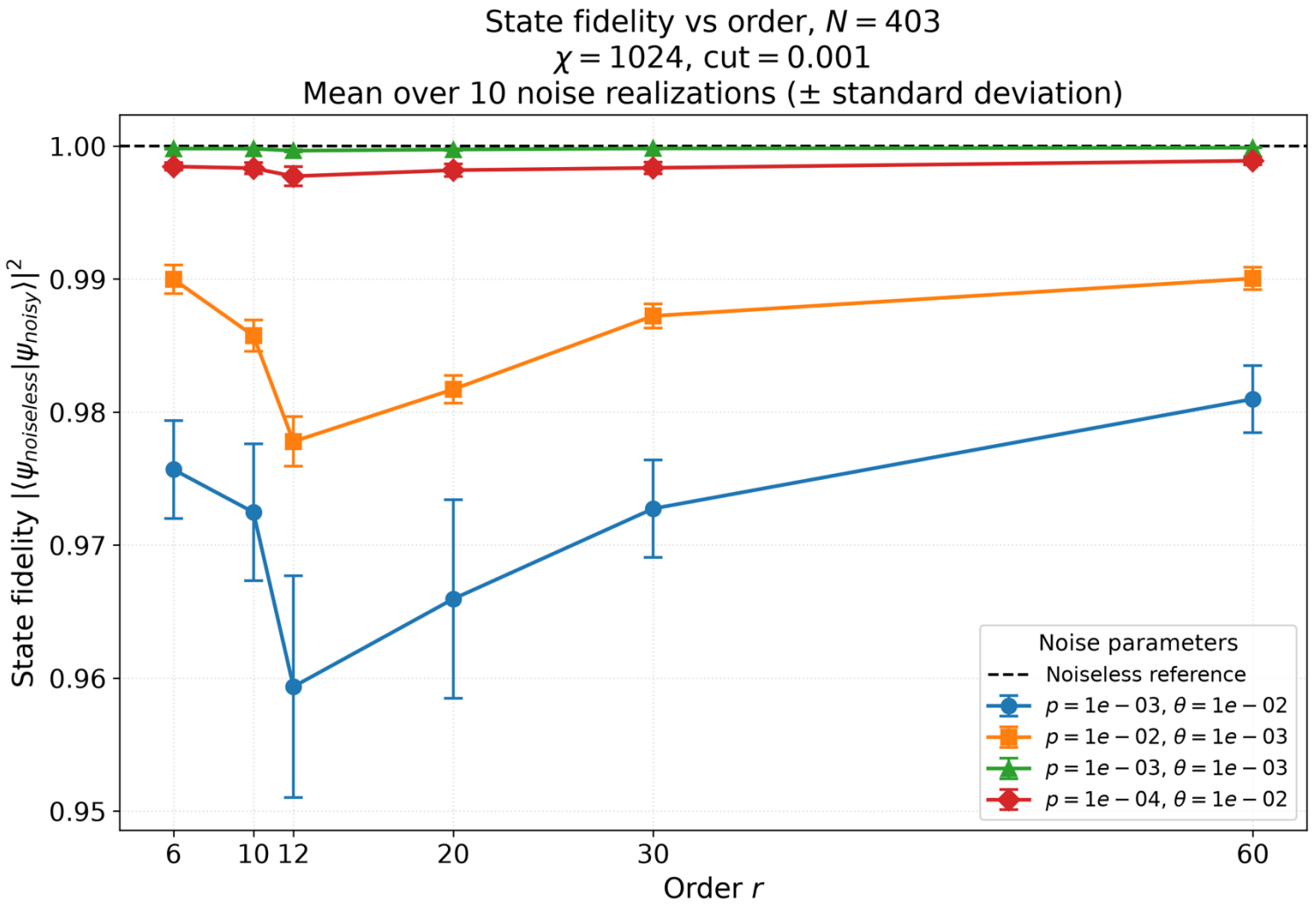
Performance of Shor with circuit noise



Performance of Shor with circuit noise



Performance of Shor with circuit noise



State fidelity : overlap between the simulated MPS with no noise and the final MPS with different noise parameters

Effects due to finite shot sampling are resolved!

Summary

- Typical (not all) Shor's circuit will require a bond dimension increasing exponentially with bit-length
- Entanglement in the noiseless circuit is governed by the order r
- Introducing noise leads to an almost loss of dependence on r

- Currently studying whether the small fluctuations obtained with r depend on the structure of the circuit
- Also analyzing how the lucky runs respond to different levels of noise

Thank you

Additional benchmarks of Quantum Matcha Tea were done as part of Quantinuum's benchmarking challenge. Details are available here:



The AQTIVATE project receives funding from the European Union's HORIZON MSCA Doctoral Networks programme, under Grant Agreement No. 101072344.