The impact of hardware specifications on reaching quantum advantage in the fault tolerant regime

Cite as: AVS Quantum Sci. 4, 013801 (2022); https://doi.org/10.1116/5.0073075
Submitted: 27 September 2021 • Accepted: 07 December 2021 • Published Online: 25 January 2022

COLLECTIONS

The impact of hardware specifications on reaching quantum advantage in the fault tolerant regime

C a : AVS Q a S . **4**, 013801 (2022); : 10.1116/5.0073075
S b : 27 S b 2021 · A : 7 D b 2021 ·
P b O : 25 Ja a 2022

Ma W bb , [1,2,a)] V E , [3] S ba a W , [1,2] a W K. H [1,2]

logical qubits and operations is known. The quantum threshold theorem states that a quantum computer using error correction schemes, classical methods but with run times comparable to the approximate techniques, such as density functional theory.

The quantum phase estimation (QPE) algorithm generates eigenvalues for a general unitary operator, and it can be applied to quantum chemistry to find the eigenenergies of chemistry Hamiltonians to FCI (full configuration interaction, i.e., exact) precision. Unlike the variational quantum eigensolver (VQE)[34] that involves many iterations [$1/\epsilon^2$ with accuracy ϵ] of low depth circuits, the QPE algorithm requires 1 iterations of a circuit with a depth scaling as $1/\epsilon$. The large depth required in the QPE algorithm means that it will only be possible with error corrected devices because NISQ devices would lose their coherence long before the end of the circuit.

Hamiltonian simulation is used as a subroutine in the quantum phase estimation (QPE) algorithm, and it involves constructing a quantum circuit that approximates the evolution of the input state according to the Hamiltonian. Two of the main paradigms for Hamiltonian simulation are trotterization and qubitization. Qubitization[35,36] can be used to simulate the Hamiltonian evolution by using quantum signal processing,[37] but more commonly, it is used to generate a quantum walk[38] upon which one can directly perform phase estimation. Qubitization is perhaps the most favored method for simulating chemistry Hamiltonian dynamics because it achieves sufficiently high-quality magic state, a distillation protocol[54,55] can be used, which essentially involves converting multiple low fidelity states into fewer higher fidelity states. Due to the high time cost associated with magic state distillation (the production and consumption), we can make a simplifying assumption that the time required to perform the T-gates effectively determines the final run time of an algorithm, as the relative cost of performing the Clifford gates fault-tolerantly is negligible. Some algorithms more naturally lend themselves to being expressed in terms of Toffoli gates, and there exist distinct specialized distillation by the data block, tick limited, the rate of magic state production by

While very long-range shuttling operations may be protected from error by periodic cooling operations and mid-circuit syndrome extraction and correction, the total time cost must be considered. With entanglement swapping, long-range interactions can be enabled between logical qubits in the surface code in a single beat, provided there are sufficient available ancilla qubits between the locations. To contrast this capability, we estimate the range at which physical shuttling may remain competitive with entanglement swapping. Assuming a code distance of 30, and logical qubits distributed across a 2D square grid, we estimate that a logical qubit could interact via physical shuttling with another logical qubit in the range of 3–30 grid spaces away within a single beat (d code cycles), depending on physical ion density and shuttling speed. While this is, indeed, unlikely to be sufficient for mediating all long-range interactions between logical qubits, the capa-

III. RESULTS

To calculate the results presented in this section, we use various surface code strategies, including the Game of Surface Codes scheme, which uses units to parallelize layers of T gates[18] and AutoCCZ factories,[31,32] which are both highlighted in Sec. II.

A. Simulating FeMoco as a function of the code cycle time

There has been extensive research into both algrithmic development and resource estimation in the field of fault tolerant overhead may appear daunting and implies that hardware with slower code cycle times will have to be more scalable to compete, assuming equal error rates and physical connectivity. We plot for a range of possible measurement depths, labeled as a fraction of the total Toffoli count, as this was not provided along with the other logical requirements.[42] In the AutoCCZ scheme, the measurement depth does not directly impact the efficiency of the approach, instead it only determines in combination with the reaction time, what the time optimal (reaction) limit is. The labels then indicate the reaction limit, the point at which the trend would end, given that measurement depth.

The assumption of a base physical error rate of 10

they are processed with higher priority and, therefore, would require considerably more physical qubits to break the encryption in time. The Bitcoin network could nullify this threat by performing a soft fork onto an encryption method that is quantum secure, where Lamport signatures[75] are the front-running candidate, but such a scheme would require much more memory per key. The bandwidth of Bitcoin is one of the main limiting factors in scaling the network, and so, changing the encryption method in this way could have serious drawbacks.

The logical resources provided by Häner *et al.*[47] for breaking elliptic curve encryption improve on the prior state of the art of Roetteler *et al.*[48] by over an order of magnitude. In the quantum threat to Bitcoin work of Aggarawal *et al.*,[43] the older and less favorable logical resource requirements were considered.[48] Aggarawal *et al.* estimate that it would require 6.5 days and 1.7×10^6 physical qubits to break the encryption with a base physical error rate of 5×10^{-4}. The code cycle time is not explicitly defined, and instead, a physical gate rate of 66.6 MHz is assumed, which we estimate would correspond to a code cycle time of approximately 0.1 μs. Next, we calculate the physical resources using the assumptions and logical requirements of Aggarawal *et al.*, and we find that a device with three AutoCCZ factories would complete in seven days and require 5×10^6 physical qubits. There is rough agreement between the final physical resources between our methods; the remaining discrepancy originates from the differing estimates of the number of physical qubits that are required per logical (abstract) qubit. The conversion factor between logical to physical qubits of Aggarawal *et al.* is stated to be 735.5 for this problem, which should include the overhead associated with the degree of encoding (code distance), distillation factories, and routing space. We find that a code distance, d, of 25 is required to maintain a final failure rate below 6%, implying at least $2 \times d^2$, or 1250, physical qubits per logical qubit. When we include the distillation and routing overhead, our final physical to logical qubit conversion factor is 2140. Whileme6(.)]6.s 6(.)]6aq.3(g)-10.TD-.01

distance), and so, the depth optimized approaches are the most suitable when room for parallelization is desired. The ratio of the measurement depth to total gate count is the inverse of the number of T gates per layer, [illegible] (when considering T gates as opposed to some other non-Clifford operation). In the GoSC method of parallelization with units, all aspects of the cost depend on the number of T gates per layer, including the footprint of the unit, the time it takes to prepare a unit, and the number T gates that are effectuated within the preparation time.

In Fig. 3, we plot the efficiency of the GoSC meCe4.9(m)2.2]TJ03.8(nn3.9(g)-293.3(22.093)-253.2(TDr)-15(i)15(t)-.3(e)-27(TDrS03249(o.5(oac)2]TJ03.8nm3)-1

the AutoCCZ method of parallelization produces more favorable final resource estimates. As mentioned, the AutoCCZ method does not display this rich behavior with the efficiency dependence on the measurement depth, and we believe that further research is warranted to compare the underlying assumptions of these two methods of parallelization.

IV. CONCLUSION

Within a particular time frame, the code cycle time and the number of achievable physical qubits may vary by orders of magnitude between hardware types. When envisaging a fault tolerant implementation, there are numerous decisions to be made based on a preference for either space or time. In this work, we compare surface code strategies of parallelization that allow one to speed up the computation until the reaction limit is reached. Most of the fault tolerant resource estimation work has focused on code cycle times corresponding to superconducting architectures. A space optimized quantum advantage case study translated for hardware with slower code cycle times may lead to run times in excess of 1000 days, and so parallelization would have to be performed to reach desirable run times. In this work, we have calculated the required number of physical qubits to reach a given desirable run time for two representative quantum advantage cases (chemistry and encryption) across a range of code cycle times. The feasibility of using these time optimization strategies will depend upon the number of physical qubits achievable within a device; therefore, the scalability of an architecture will play an important role in determining whether a quantum advantage is achievable. We contrast two methods of parallelizateanydot(si)13.5(at)9(s)-e3Mfo-Cs(s)h-2u26.6(v)10inuime3(i)14.343(i)200IoateeiC7vtou42 teseto td6.31494ntf todn4.13.d6.9(i),6.314ntd6.31494 tTc[(l)15

ia285515(l)-235(4406.6(ql)16.9(i)1a12.8(t)18.5(ei)14.3(o)15(9)-347.2(to)-331.9(s)17.5(i)14.3(mu)28(l)16.9(a)1524(t)16.1(e)12.8(n)1r)]5(q)16355(a)9(s)0eo 44

[9] A. W. Cross, L. S. Bishop, S. Sheldon, P. D. Nation, and J. M. Gambetta, Phys. Rev. A 100, 032328 (2019).
[10] M. Webber, S. Herbert, S. Weidt, and W. Hensinger, Adv. Quantum Technol. 3, 2000027 (2020).
[11] J. Roffe, D. R. White, S. Burton, and E. Campbell, arXiv:2005.07016 (2020).
[12] N. de Beaudrap and S. Herbert, Quantum 4, 356 (2020).
[13] E. T. Campbell, B. M. Terhal, and C. Vuillot, Nature 549, 172 (2017).
[14] M. Vasmer and D. E. Browne, Phys. Rev. A 100, 012312 (2019).
[15] C. Monroe, R18Raussendorf, A. Ruthven, Rrowne BP aMaunz,-332.27L.