On quantum factoring using noisy intermediate scale quantum computers

V. Kornienko, V. Phan, A. Pönni, M. Raasakka, I. Tittonen
Micro and Quantum Systems Group,
Department of Electronics and Nanoengineering,
Aalto University

Aalto University
School of Electrical
Engineering

BUSINESS
FINLAND

1 Introduction

Factoring large composite integers is a textbook example of a computational problem that is hard to solve on a classical computer, the best known algorithms run in super-polynomial time. It is an immensely important problem since the RSA cryptosystem and therefore much of the information security of the modern world relies on its hardness.

Variational quantum factoring (VQF) is a proposed variational approach to integer factoring [1]. It works by encoding the factoring problem to the ground state of an Ising Hamiltonian, which is then solved with a variational quantum optimizer. Here, we study the quantum resource requirements of VQF with different assumptions and compare factoring performance for entangled and non-entangled variational circuits.

2 Variational quantum algorithms

Variational quantum algorithms (VQAs) are the most promising approach to achieving practical quantum advantage using near-term NISQ computers. They circumvent gate count limitations of near-term devices by using short parametrized quantum circuits (PQCs). These PQCs are executed on the quantum processor but their parameters are optimized using a classical computer. VQAs can be seen as a quantum analogue of classical machine learning methods, such as neural networks.

There have been many proposed applications for VQAs, such as finding ground/excited states, simulation of quantum dynamics, combinatorial optimization, solving systems of equations, and machine learning algorithms.

3 Variational quantum factoring

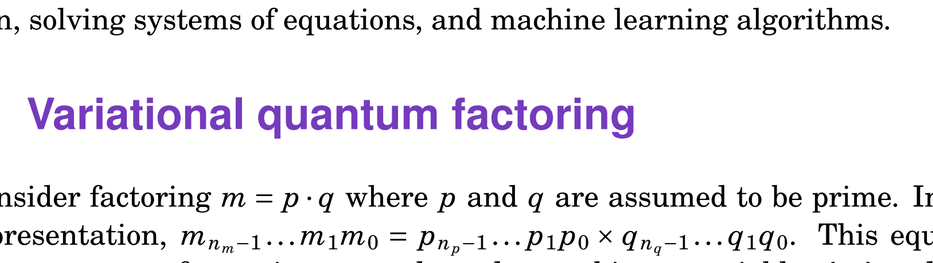
Consider factoring $m = p \cdot q$ where p and q are assumed to be prime. In a binary representation, $m_{n_m-1}\ldots m_1 m_0 = p_{n_p-1}\ldots p_1 p_0 \times q_{n_q-1}\ldots q_1 q_0$. This equation implies a system of equations over the unknown binary variables $\{p_i\}$ and $\{q_i\}$. The equations are

$$C_i = \sum_{j=0}^{i} q_j p_{i-j} + \sum_{j=0}^{i} z_{j,i} - m_i - \sum_{j=1}^{n_c} 2^j z_{i,i+j}\,, \quad i = 0,\ldots,n_c\,, \tag{1}$$

where $z_{i,j}$ are the carry bits originating from the binary multiplication. These equations are quantized to a Hamiltonian by the replacement

$$b_k \mapsto \frac{1}{2}(1 - Z_{b,k})\,, \tag{2}$$

where Z is the Pauli-Z operator, $b = \{p, q, z\}$, and k is the bit index. This produces a Hamiltonian $\hat{H} = \sum_i \hat{C}_i^2$ over qubits whose ground state (with zero energy) is in one-to-one correspondence with bit assignments which satisfy $m = p \times q$. Therefore, factoring is reduced to the problem of finding the ground state of $\hat{H}$. We will test two variational quantum circuits:



The first circuit is conventional entangled circuit with parametrized Pauli-Y rotations. The second one is a circuit where the entangling operations are replaced with T-gates. The purpose is to study whether entanglement in the ansatz exhibits better performance than the non-entangled one, which could be simulated efficiently on a classical computer. The circuits have a repeating layered structure and the performance of VQF is controlled by changing the number of these layers. More layers means a more flexible state $|\psi(\theta)\rangle$, so finding the ground state is easier, but it also takes more time because there are more parameters to optimize.

4 Qubit requirements

The number of available qubits is an important bottleneck for NISQ devices. Factoring larger numbers often require more qubits in the VQF algorithm so the qubit number places a practical bound on the size of numbers to be factored. Typically however, an additional simplification step is performed on (1), where "obvious" equations are immediately solved. For example, one could deduce that $xy = 1$ is equivalent to $x = y = 1$, which can eliminate some of the binary variables. In addition, in the original paper [1] the prior knowledge of n_p and n_q was assumed, which obviously is not possible in real factoring challenges.

We compared qubit requirements with and without prior knowledge of n_p and n_q. The qubit requirement scales in both cases linearly in $\log m$. Prior knowledge resulted in a 40% reduction in qubit requirements, on average. However, with prior knowledge some instances are drastically simplified, sometimes even completely solved.

5 Energy optimization

We will now consider a simple gradient based variational quantum eigensolver (VQE) method for finding the ground state of H. We simply use the quantum computer to evaluate the energy $E(\theta) = \langle\psi(\theta)|H|\psi(\theta)\rangle$ and its gradients. The classical part of the algorithm then adjusts the parameters θ so that $E(\theta)$ reaches a local minimum. The optimization problem is non-convex, so we study the probability of converging to the global minimum over uniformly random parameter initializations. Convergence to a suboptimal minimum can mean a failure to factor m.

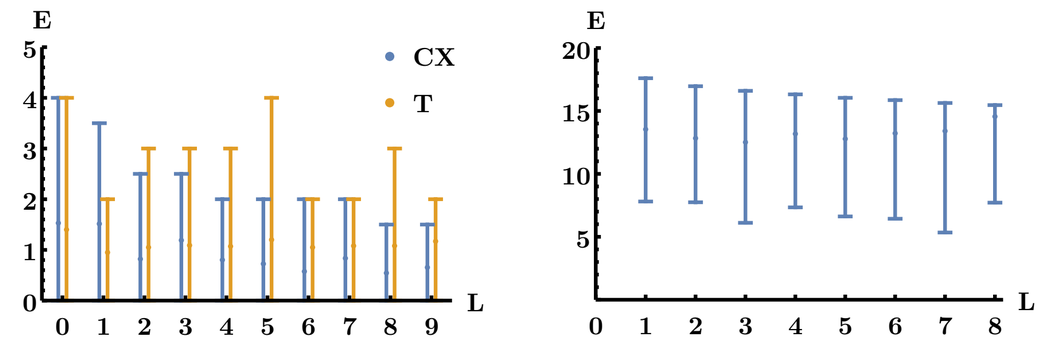


Figure 1: **Left:** The average final optimization energy of $m = 91$ for different numbers of layers L and entangled/non-entangled ansatz circuits with statistics over 100 random parameter initializations. This instance requires in total 10 qubits. Error bars indicate the 5% and 95% quantiles over all runs. **Right:** Energy achieved by QAOA on the same factorization instance for a few different numbers of layers.

We notice that VQE has better performance compared to QAOA, which is an algorithm designed for combinatorial optimization used in previous VQF papers. Also we note that entanglement in the VQE circuit seems to have little effect on performance.

6 Conclusion

- Prior knowledge significantly reduces qubit requirements for VQF.
- VQE achieves better energies than QAOA while also using shorter circuits.
- There is no significant difference in optimization performance between entangled and non-entangled variational circuits.

References

[1] E. R. Anschütz, J. Olson, A. Aspuru-Guzik, and Y. Cao *QTOP@NetSys* (2018)

Contact information for comments & improvement ideas: Arttu Pönni
Email: arttu.ponni@aalto.fi