Wrapping up Shor's and QFT; Quantum Approximate Optimization Algorithm

Yipeng Huang

Rutgers University

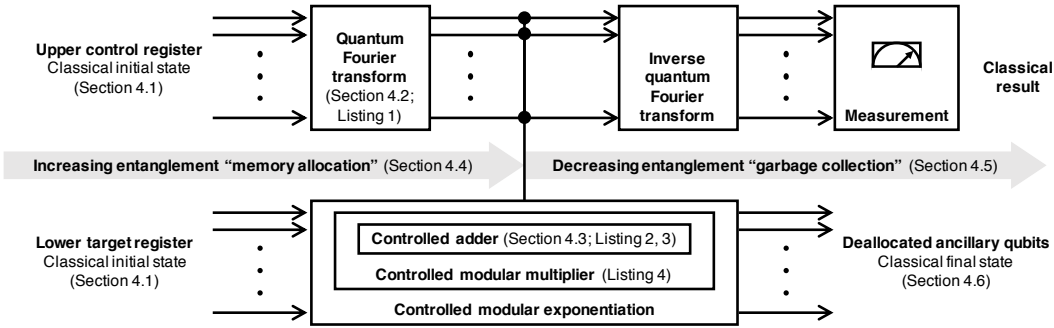
October 18, 2021

Table of contents

The quantum part: period finding using quantum Fourier transform

- After picking a value for a, use quantum parallelism to calculate modular exponentiation: $a^x \mod N$ for all $0 \leq x \leq 2^n - 1$ simultaneously.
- Use interference to find a global property, such as the period r.

Calculate modular exponentiation



- Image source: Huang and Martonosi, Statistical assertions for validating patterns and finding bugs in quantum programs, 2019.
- A good source on how to build the controlled adder, controlled multiplier, and controlled exponentiation is in Beauregard, Circuit for Shor's algorithm using 2n+3 qubits, 2002.

Calculate modular exponentiation

- State after applying modular exponentiation circuit is

$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \, |f(x)\rangle$$

- Concretely, using our running example of $N = 15$, need $n = 4$ qubits to encode, and suppose we picked $a = 2$, the state would be

$$\frac{1}{4} \sum_{x=0}^{15} |x\rangle \, |2^x \mod 15\rangle$$

Measurement of target (bottom, ancillary) qubit register

- We then measure the target qubit register, collapsing it to a definite value. The state of the upper register would then be limited to:

$$\frac{1}{\sqrt{A}} \sum_{a=0}^{A-1} |x_0 + ar\rangle$$

- Concretely, using our running example of $N = 15$, and suppose we picked $a = 2$, and suppose measurement results in 2, the upper register would be a uniform superposition of all $|x\rangle$ such that $2^x \equiv 2 \mod 15$:

$$\frac{|1\rangle}{2} + \frac{|5\rangle}{2} + \frac{|9\rangle}{2} + \frac{|13\rangle}{2}$$

- The key trick now is can we extract the period $r = 4$ from such a quantum state. We do this using the quantum Fourier transform.

Quantum Fourier transform to obtain period

The task now is to use Fourier transform to obtain the period.

$$QFT\Big(\,|x\rangle\,\Big) = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{\frac{2\pi i}{2^n} xy}\,|y\rangle$$

$$QFT = \frac{1}{\sqrt{2^n}} \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \cdots & \omega^{2^n-1} \\ 1 & \omega^2 & \omega^4 & \cdots & \omega^{2(2^n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{2^n-1} & \omega^{2(2^n-1)} & \cdots & \omega^{(2^n-1)(2^n-1)} \end{bmatrix}$$

Where

$$\omega = e^{\frac{2\pi i}{2^n}}$$

And recall that

$$e^{ix} = \cos x + i \sin x$$

Quantum Fourier transform to obtain period

The task now is to use Fourier transform to obtain the period.

$$QFT\Big(\,|x\rangle\,\Big) = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{\frac{2\pi i}{2^n} xy}\,|y\rangle$$

$$QFT\left(\frac{1}{\sqrt{A}} \sum_{a=0}^{A-1} |x_0 + ar\rangle\right)$$

$$= \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} \left(\frac{1}{\sqrt{A}} \sum_{a=0}^{A-1} e^{\frac{2\pi i}{2^n}(x_0+ar)y}\right) |y\rangle$$

$$= \sum_{y=0}^{2^n-1} \left(\frac{1}{\sqrt{2^n A}} e^{\frac{2\pi i}{2^n} x_0 y} \sum_{a=0}^{A-1} e^{\frac{2\pi i}{2^n} ary}\right) |y\rangle$$

Quantum Fourier transform to obtain period

$$\begin{aligned}\text{Prob}(y) &= \frac{A}{2^n}\left|\frac{1}{A}e^{\frac{2\pi i}{2^n}x_0 y}\sum_{a=0}^{A-1}e^{\frac{2\pi i}{2^n}ary}\right|^2 \\ &= \frac{A}{2^n}\left|\frac{1}{A}\sum_{a=0}^{A-1}e^{\frac{2\pi i}{2^n}ary}\right|^2\end{aligned}$$

- Here, values of y such that $\frac{ry}{2^n}$ is close to an integer will have maximal measurement probability.
- In our case, only $\frac{ry}{2^n} = \frac{4\cdot 4}{16}$, $|y\rangle = |4\rangle$ will have high measurement probability.
- To get a beautiful explanation of principle of least action, read Feynman, QED.

How to construct the Quantum Fourier transform

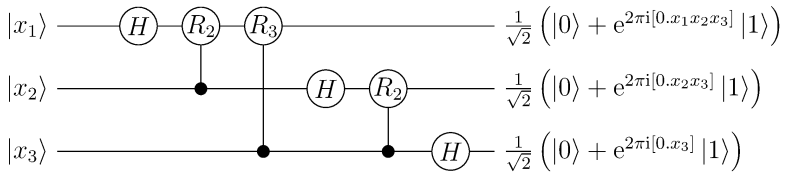


Figure: Credit: Wikimedia

How to construct the Quantum Fourier transform

$$R_k = \begin{bmatrix} 1 & 0 \\ 0 & \exp\frac{2\pi i}{2^k} \end{bmatrix}$$

- Cost of computing the FFT for functions encoded in n bits: $O(2^n n)$
- Cost of quantum Fourier transform for functions encoded in n qubits: $O(n^2)$ gates.

1. $$R_0 = \begin{bmatrix} 1 & 0 \\ 0 & \exp\frac{2\pi i}{2^0} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$$
2. $$R_1 = \begin{bmatrix} 1 & 0 \\ 0 & \exp\frac{2\pi i}{2^1} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = Z$$
3. $$R_2 = \begin{bmatrix} 1 & 0 \\ 0 & \exp\frac{2\pi i}{2^2} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} = S$$
4. $$R_3 = \begin{bmatrix} 1 & 0 \\ 0 & \exp\frac{2\pi i}{2^3} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & \frac{\sqrt{2}}{2} + \frac{\sqrt{2}i}{2} \end{bmatrix} = T$$

Time cost and implementation

Factoring underpins cryptosystems.

For number represented as b bits:

- Classical algorithm: needs $O(2^{\sqrt[3]{b}})$ operations. Factoring 512-bit integer: 8400 years. 1024-bit integer: 13×10^12 years.
- Quantum algorithm: needs $O(b^2 log(b))$ operations. Factoring 512-bit integer: 3.5 hours. 1024-bit integer: 31 hours.

Source: Oskin et al. A Practical Architecture for Reliable Quantum Computers.

Time cost and implementation

Figure 1. Scaling the classical number field sieve (NFS) vs. Shor's quantum algorithm for factoring.[37]

The horizontal axis is the length of the number to be factored. The steep curve is NFS, with the marked point at $L = 768$ requiring 3,300 CPU-years. The vertical line at $L = 2048$ is NIST's 2007 recommendation for RSA key length for data intended to remain secure until 2030. The other lines are various combinations of quantum computer logical clock speed for a three-qubit operation known as a Toffoli gate (1Hz and 1MHz), method of implementing the arithmetic portion of Shor's algorithm (BCDP, D, and F), and quantum computer architecture (NTC and AC, with the primary difference being whether or not long-distance operations are supported). The assumed capacity of a machine in this graph is $2L^2$ logical qubits. This figure illustrates the difficulty of making pronouncements about the speed of quantum computers.

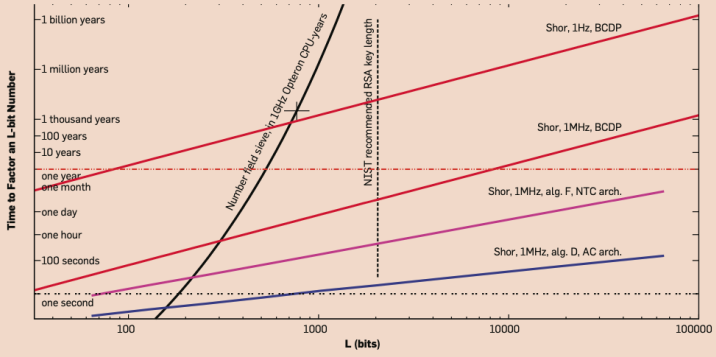


Figure: Credit: Van Meter and Horsman. A Blueprint for Building a Quantum Computer. Communications of the ACM. 2013.

Near-term and far-future quantum computing

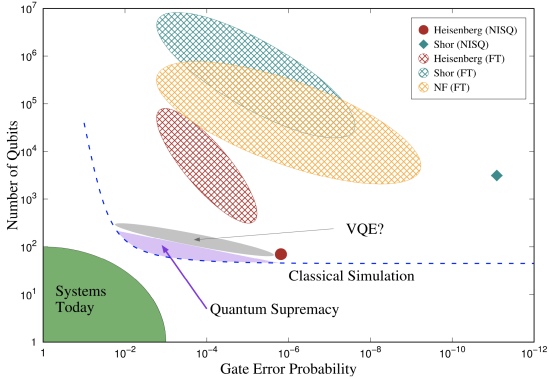
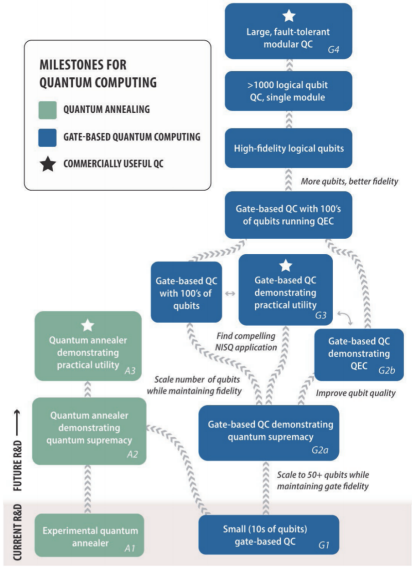


Figure: Credit: Maslov, Nam, and Kim. An Outlook for Quantum Computing. Proceedings of the IEEE. 2019.

Fig. 2. ***Performance space of quantum computers, measured by the error probability of each entangling gate in the horizontal axis (roughly inversely proportional to the total number of gates that can be executed on a NISQ machine), and the number of qubits in the system in the vertical axis. Blue dotted line approximately demarcates quantum systems that can be simulated using best classical computers, while the green colored region shows where the existing quantum computing systems with verified performance numbers lie (as of September 2018). Purple shaded region indicates computational tasks that accomplish the so-called "quantum supremacy," where the computation carried out by the quantum computer defies classical simulation regardless of its usefulness. The different shapes illustrate resource counts for solving various problems, with solid symbols corresponding to the exact entangling gate counts and number of qubits in NISQ machines, and shaded regions showing approximate gate error requirements and number of qubits for an FT implementation (not pictured are the regions where the error gets too close to the known fault-tolerance thresholds): cyan diamond and shaded region correspond to factoring a 1024-bit number using Shor's algorithm [14], magenta circle and shaded region represent simulation of a 72-spin Heisenberg model [20], and orange shaded region illustrates NF simulation [21].***

Steps toward useful quantum computing



An illustration of potential milestones of progress in quan-

Figure: Credit: National Academies of Sciences, Engineering, and Medicine. Quantum Computing: Progress and Prospects. 2019.

Near-term intermediate-scale quantum (NISQ) computers

The limitations of near term quantum computers

- NISQ systems have limited number of qubits:
  No error correction.
  (In contrast, error corrected Shor's would need a million qubits.)
- NISQ systems have limited coherence time:
  Relative shallow depth of circuits.
  (In contrast, error corrected Shor's would need hundreds of millions of gates.)
- NISQ systems have limited operation accuracy

NISQ variational algorithms

Use a classical algorithm to train a "quantum neural network".

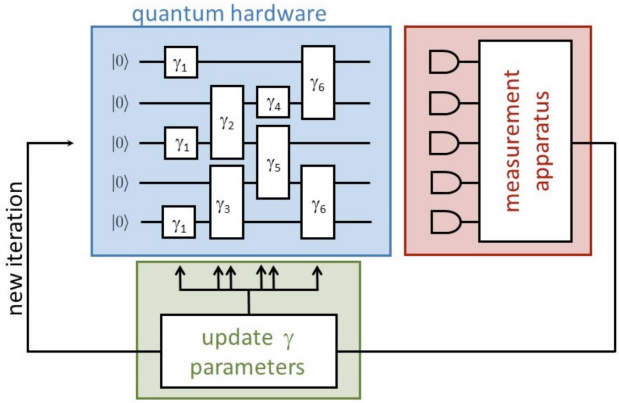


Figure:
Credit: [Guerreschi and Smel

FIG. 1. Illustration of the three common steps of hybrid quantum-classical algorithms. These steps have to be repeated until convergence or when a sufficiently good quality of the solution is reached. 1) State preparation involving the quantum hardware capable of tunable gates characterized by parameters γ_n (blue), 2) measurement of the quantum state and evaluation of the objective function (red), 3) iteration of the

NISQ variational algorithms

Use a classical algorithm to train a "quantum neural network".

1. Quantum computer prepares a quantum state that is a function of classical parameters.
2. Quantum computer measures quantum state to provide classical observations.
3. Classical computer uses observations to calculate an objective function.
4. Classical computer uses optimization routine to propose new classical parameters to maximize objective function.
5. Repeating steps 1 through 4, the algorithm leads to better approximations to underlying problem.

NISQ variational algorithms

Benefits of quantum-classical scheme:

1. Provides meaningful results even without error correction
2. Shallow circuits (not many operations on each qubit)
3. Draws on strengths of quantum and classical:
4. Prepare and measure a quantum state
5. Optimize for a set of optimal parameters based on classical measurements

NISQ variational algorithms

Great! Can NISQ variational algorithms solve useful problems?

1. Variational quantum eigensolver (VQE):
   Simulate quantum mechanics
2. Quantum approximate optimization algorithm (QAOA):
   Approximate solutions to constraint satisfaction problems (CSPs) [Farhi et al., 2014]

Constraint satisfaction problems $\in$ Combinatorial optimization problems

- 3SAT
- Traveling salesman
- Knapsack
- Graph coloring

Boolean satisfiability problem

- 3-SAT: NP-Complete
- n bits; m constraints/clauses
- A Boolean formula consisting of m clauses
  $C_1 \wedge C_2 \wedge ... \wedge C_m$
  For example:
  $(\neg z_0 \vee z_1 \vee z_2) \wedge (\neg z_1 \vee z_2 \vee z_3) \wedge ... \wedge C_m$
- C_α depends only on $l = 3$ coordinates of $\vec{z}$.
- Each clause C_α is either True or False.
  for each constraint $\alpha \in [m]$ and each n-bit string $\vec{z} \in \{0,1\}^n$, define

$$C_\alpha(\vec{z}) = \begin{cases} 1 & \text{if } \vec{z} \text{ satisfies the constraint } \alpha \\ 0 & \text{if } \vec{z} \text{ does not} \end{cases}$$

3-SAT and connections

Figure 8.7 Reductions between search problems.

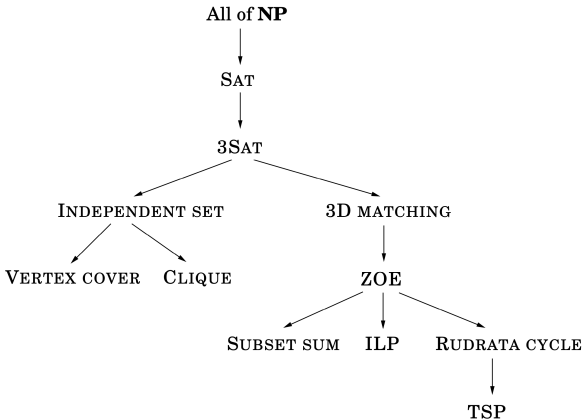


Figure: Credit: Dasgupta, Papadimitriou, and Vazirani. Algorithms.

Constraint satisfaction problem (CSP): MAX-SAT

- MAX-SAT: NP-Hard
- A Boolean formula consisting of m clauses
  $C_1 \wedge C_2 \wedge ... \wedge C_m$
- Each clause C_α is either True or False.
  for each constraint $\alpha \in [m]$ and each n-bit string $\vec{z} \in \{0,1\}^n$, define
  $$C_\alpha(\vec{z}) = \begin{cases} 1 & \text{if } \vec{z} \text{ satisfies the constraint } \alpha \\ 0 & \text{if } \vec{z} \text{ does not} \end{cases}$$
- Satisfy as many clauses as possible to maximize objective function $C(z)$:
  $$\max_{\vec{z}} C(\vec{z}) = \max_{\vec{z}} \sum_{\alpha=1}^{m} C_\alpha(\vec{z})$$

Approximate MAX-SAT

Approximate the maximum:

$$\max_{\vec{z}} C(\vec{z}) = \max_{\vec{z}} \sum_{\alpha=1}^{m} C_\alpha(\vec{z})$$

Constraint satisfaction problem (CSP): MAX-CUT

- Given an arbitrary undirected graph $G = (V(G), E(G))$
- goal of MAX-CUT is to assign one of two partitions to each node so as to maximize the number of cuts

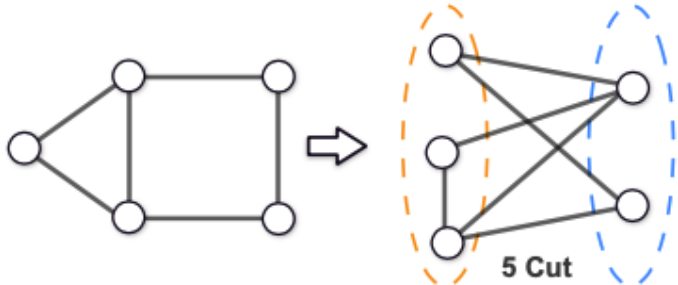


FIG. 39: An illustration of the MaxCut problem.

Figure: Credit: Quantum Algorithm Implementations for Beginners Coles.

Constraint satisfaction problem (CSP): MAX-CUT

- Given an arbitrary undirected graph $G = (V(G), E(G))$
- goal of MAX-CUT is to assign one of two partitions $\sigma_i \in \{-1, +1\}$ to each node $i \in V(G)$ so as to maximize the number of cuts
- Identical form to the MAX-SAT problem with objective function $C(\vec{\sigma})$:
$$\max_{\vec{\sigma}} C(\vec{\sigma}) = \max_{\vec{\sigma}} \sum_{<jk> \in E(G)} C_{<jk>}(\vec{\sigma})$$
- But the constraints are now:
$$C_{<jk>}(\vec{\sigma}) = \frac{1}{2}(1 - \sigma_j \sigma_k) = \begin{cases} 1 & \text{if } \sigma_j \text{ and } \sigma_k \text{ are different} \\ 0 & \text{if } \sigma_j \text{ and } \sigma_k \text{ are the same} \end{cases}$$

QAOA for MAX-CUT: general strategy

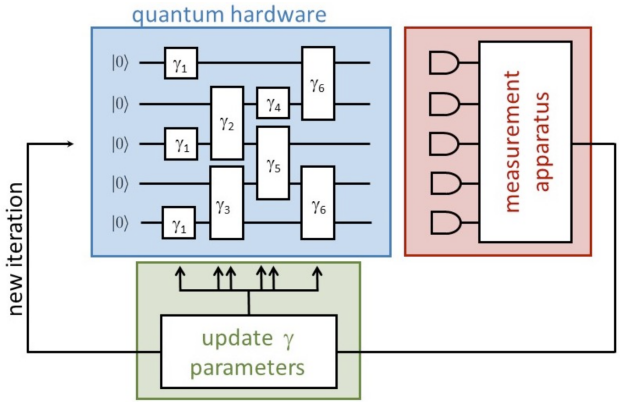


Figure:
Credit: [Guerreschi and Smel

FIG. 1. Illustration of the three common steps of hybrid quantum-classical algorithms. These steps have to be repeated until convergence or when a sufficiently good quality of the solution is reached. 1) State preparation involving the quantum hardware capable of tunable gates characterized by parameters γ_n (blue), 2) measurement of the quantum state and evaluation of the objective function (red), 3) iteration of the optimization method to determine promising changes in the state preparation (green). Notice that a single parameter γ_n may characterize more than one gate, for example see γ_1 and γ_6 in the blue box. In practice,

QAOA for MAX-CUT: general strategy

1. Each node in n nodes of the MAX-CUT graph corresponds to one of n qubits in the quantum circuit.
2. The state vector across the qubits $|\psi\rangle$ encodes a node partitioning $\vec{\sigma} \in \{-1, +1\}^n$
3. Put the initial state vector $|\psi_s\rangle$ in a superposition of all possible node partitionings
4. Need an operator (quantum gate) that encodes an edge $< jk > \in E(G)$
5. Provide classical parameters such that the classical computer can control quantum partitioning
6. Perform a series of operations parameterized by classical parameters $\vec{\gamma}$ and $\vec{\beta}$ such that the final state vector $|\psi(\vec{\gamma}, \vec{\beta})\rangle$ is a superposition of good partitionings
7. Optimize for a good set of $\vec{\gamma}$ and $\vec{\beta}$

QAOA for MAX-CUT: general strategy

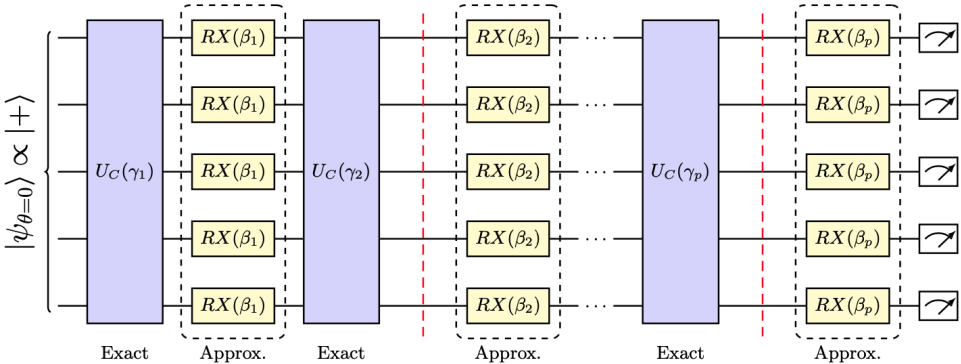


FIG. 1. A schematic representation of the QAOA circuit and our approach to simulating it. The input state is trivially initialized to $|+\rangle$. Next, at each p, the exchange of exactly (U_C, Sec. II B 1) and approximately ($RX(\beta) = e^{-i\beta X}$, Sec. II B 2) applicable gates is labeled. As noted in the main text, each (exact) application of the U_C gate leads to an increase in the number of hidden units by $|E|$ (the number of edges in the graph). In order to keep that number constant, we compress the number of hidden units (Sec. II C), indicated by red dashed lines after each U_C gate. The compression is repeated at each layer after the first, halving the number of hidden units each time.

Figure: Credit: Classical variational simulation of the Quantum Approximate Optimization Algorithm. Medvidovic and Carleo.

1. Each node in n nodes of the MAX-CUT graph corresponds to one of n qubits in the quantum circuit.

Let's use an $n = 3$ example in the figure.

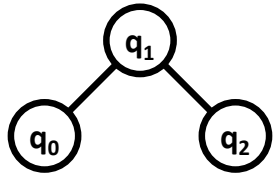


Figure: $G = (V(G), E(G)) = (\{q0, q1, q2\}, \{< q0q1 >, < q1q2 >\})$

$$|\psi\rangle = \alpha_0 |000\rangle + \alpha_1 |001\rangle \ldots + \alpha_7 |111\rangle = \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \ldots \\ \alpha_7 \end{bmatrix}$$

So now we have quantum amplitudes for each of the basis states.

Probability of measuring outcome z is $|\alpha_z|^2$. $\sum^{n-1} |\alpha_z|^2 = 1$

2. The state vector across the qubits $|\psi\rangle$ encodes a node partitioning

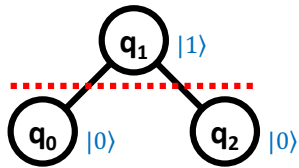


Figure: A max-cut corresponding to $|\psi\rangle = |010\rangle$.

- In our $n = 3$ running example, $|\psi\rangle = |010\rangle$, $\alpha_2 = 1$, $\alpha_0 = \alpha_1 = \alpha_3 = \alpha_4 = \alpha_5 = \alpha_6 = \alpha_7 = 0$, is a max-cut.
- The other max-cut is $|\psi\rangle = |101\rangle$.
- A superposition $|\psi\rangle = \frac{1}{\sqrt{2}}|010\rangle + \frac{1}{\sqrt{2}}|101\rangle$ would be an equal superposition of the two max cuts.

3. Put the initial state vector $|\psi_s\rangle$ in a superposition of all possible node partitionings

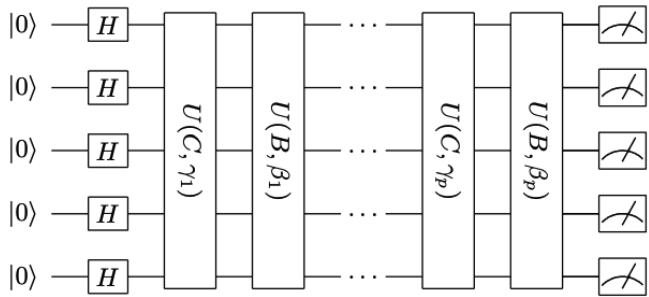


FIG. 2: Framework for a QAOA circuit. Each qubit begins with a Hadamard gate, and then $2p$ gates are performed alternating between applying Hamiltonian C and applying Hamiltonian B.

Figure: Credit: How many qubits are needed for quantum computational supremacy. Dalzell et al.

3. Put the initial state vector $|\psi_s\rangle$ in a superposition of all possible node partitionings

A superposition across all the bitstrings representing partitionings.

$$|\psi_s\rangle = |+\rangle^{\otimes n} = H^{\otimes n} |0\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{z=0}^{2^n-1} |z\rangle$$

3. Put the initial state vector $|\psi_s\rangle$ in a superposition of all possible node partitionings

In our $n = 3$ running example:

$$|+\rangle^{\otimes n} = H^{\otimes 3}|0\rangle^{\otimes 3} = \begin{bmatrix} \frac{+1}{\sqrt{2}} & \frac{+1}{\sqrt{2}} \\ \frac{+1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{bmatrix}^{\otimes 3} \begin{bmatrix} 1 \\ 0 \end{bmatrix}^{\otimes 3} = \begin{bmatrix} \frac{+1}{\sqrt{2}} \begin{bmatrix} \frac{+1}{\sqrt{2}} & \frac{+1}{\sqrt{2}} \\ \frac{+1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{bmatrix} & \frac{+1}{\sqrt{2}} \begin{bmatrix} \frac{+1}{\sqrt{2}} & \frac{+1}{\sqrt{2}} \\ \frac{+1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{bmatrix} \\ \frac{+1}{\sqrt{2}} \begin{bmatrix} \frac{+1}{\sqrt{2}} & \frac{+1}{\sqrt{2}} \\ \frac{+1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{bmatrix} & \frac{-1}{\sqrt{2}} \begin{bmatrix} \frac{+1}{\sqrt{2}} & \frac{+1}{\sqrt{2}} \\ \frac{+1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{bmatrix} \end{bmatrix} \otimes$$

$$\begin{bmatrix} \frac{+1}{\sqrt{2}} & \frac{+1}{\sqrt{2}} \\ \frac{+1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix}^{\otimes 3} = \frac{1}{\sqrt{8}} \sum_{z=0}^{7} |z\rangle = [\frac{1}{\sqrt{8}}, \frac{1}{\sqrt{8}}, \frac{1}{\sqrt{8}}, \frac{1}{\sqrt{8}}, \frac{1}{\sqrt{8}}, \frac{1}{\sqrt{8}}, \frac{1}{\sqrt{8}}, \frac{1}{\sqrt{8}}]^{\dagger}$$

4. Need an operator (quantum gate) that encodes an edge $< jk > \in E(G)$

- In the Max-Cut type of CSP, constraints correspond to edges
- $C = \sum_{<jk> \in E(G)} C_{<jk>} = \sum_{<jk> \in E(G)} \frac{1}{2}(1 - \sigma_j^z \otimes \sigma_k^z)$
- σ_i^z is the Pauli-Z operator on qubit i
- $\sigma^z = \begin{bmatrix} +1 & 0 \\ 0 & -1 \end{bmatrix}$
- Claim: ψ that maximizes $\langle \psi | C | \psi \rangle$ is the graph partition with the maximum cut.

4. Need an operator (quantum gate) that encodes an edge $< jk > \in E(G)$

In our $n = 3$ running example:

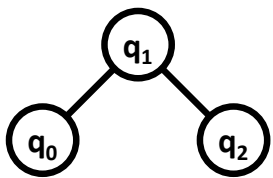


Figure: $G = (V(G), E(G)) = (\{q0, q1, q2\}, \{< q0q1 >, < q1q2 >\})$

$$C = \sum_{<jk> \in E(G)} \frac{1}{2}(1 - \sigma_j^z \otimes \sigma_k^z) =$$

$$\frac{1}{2}(1 - \sigma_0^z \otimes \sigma_1^z) + \frac{1}{2}(1 - \sigma_1^z \otimes \sigma_2^z) =$$

$$\frac{1}{2}(I - \sigma^z \otimes \sigma^z \otimes I) + \frac{1}{2}(I - I \otimes \sigma^z \otimes \sigma^z) =$$

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

4. Need an operator (quantum gate) that encodes an edge $< jk > \in E(G)$

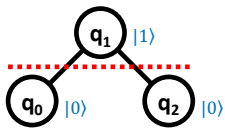


Figure: A max-cut corresponding to $|\psi\rangle = |010\rangle$.

- Claim: ψ that maximizes $\langle\psi| C |\psi\rangle$ is the graph partition with the maximum cut.
- $\langle 010| C |010\rangle =$

$$\begin{bmatrix}0\\0\\1\\0\\0\\0\\0\\0\end{bmatrix}^{\dagger} \begin{bmatrix}0&0&0&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&2&0&0&0&0&0\\0&0&0&1&0&0&0&0\\0&0&0&0&1&0&0&0\\0&0&0&0&0&2&0&0\\0&0&0&0&0&0&1&0\\0&0&0&0&0&0&0&0\end{bmatrix} \begin{bmatrix}0\\0\\1\\0\\0\\0\\0\\0\end{bmatrix} =$$

2

4. Need an operator (quantum gate) that encodes an edge $< jk > \in E(G)$

- $\langle 010| C |010\rangle = \begin{bmatrix}0\\0\\1\\0\\0\\0\\0\\0\end{bmatrix}^{\dagger} \begin{bmatrix}0&0&0&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&2&0&0&0&0&0\\0&0&0&1&0&0&0&0\\0&0&0&0&1&0&0&0\\0&0&0&0&0&2&0&0\\0&0&0&0&0&0&1&0\\0&0&0&0&0&0&0&0\end{bmatrix} \begin{bmatrix}0\\0\\1\\0\\0\\0\\0\\0\end{bmatrix} = 2$
- Note the size of state vector $|\psi\rangle$ is 2^n.
- Size of constraint matrix C is $2^n \times 2^n$.
- We wouldn't want to construct C explicitly, but it can be created effciently using gates and tensor products.
- We will enlist a quantum computer to create $|\psi\rangle$ and C.

5. Provide classical parameters such that the classical computer can control quantum partitioning

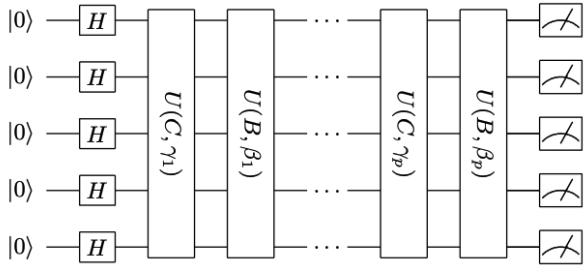


FIG. 2: Framework for a QAOA circuit. Each qubit begins with a Hadamard gate, and then $2p$ gates are performed alternating between applying Hamiltonian C and applying Hamiltonian B.

Figure: Credit: How many qubits are needed for quantum computational supremacy. Dalzell et al.

5. Provide classical parameters such that the classical computer can control quantum partitioning

- A parameter p that controls how many iterations of algorithm and how complete of a graph to see.
- Do optimization across $2p$-dimensional vector of $\vec{\gamma}$ and $\vec{\beta}$ parameters
- $(\vec{\gamma}, \vec{\beta}) = (\gamma_1, \beta_1, ...\gamma_p, \beta_p)$
- $\gamma_i \in [0, 2\pi]$
- $\beta_i \in [0, \pi]$

6. Perform a series of operations parameterized by classical parameters $\vec{\gamma}$ and $\vec{\beta}$ such that the final state vector $|\psi(\vec{\gamma}, \vec{\beta})\rangle$ is a superposition of good partitionings

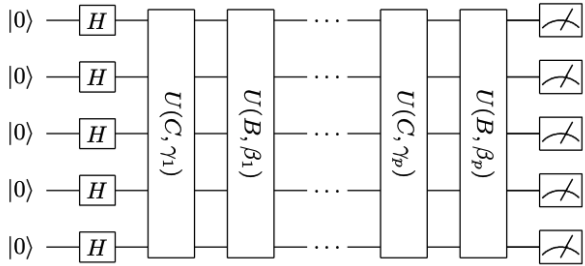


FIG. 2: Framework for a QAOA circuit. Each qubit begins with a Hadamard gate, and then $2p$ gates are performed alternating between applying Hamiltonian C and applying Hamiltonian B.

Figure: Credit: How many qubits are needed for quantum computational supremacy. Dalzell et al.

6. Perform a series of operations parameterized by classical parameters $\vec{\gamma}$ and $\vec{\beta}$ such that the final state vector $|\psi(\vec{\gamma}, \vec{\beta})\rangle$ is a superposition of good partitionings

$U(C, \gamma)$, $U(B, \beta)$ are $2^n \times 2^n$ linear operators (Unitary matrices)

1. Problem Hamiltonian enforces constraints.
   A product across all the graph edges.
   $U(C, \gamma) = e^{-i\gamma C} = \prod_{<jk> \in E(G)} e^{-i\gamma C_{<jk>}}$

2. Admixing Hamiltonian perturbs the assignments.
   A product across all the qubits representing graph vertices.
   $U(B, \beta) = e^{-i\beta B} = \prod_{q \in V(G)} e^{-i\beta \sigma_q^x}$

6. Perform a series of operations parameterized by classical parameters $\vec{\gamma}$ and $\vec{\beta}$ such that the final state vector $|\psi(\vec{\gamma}, \vec{\beta})\rangle$ is a superposition of good partitionings

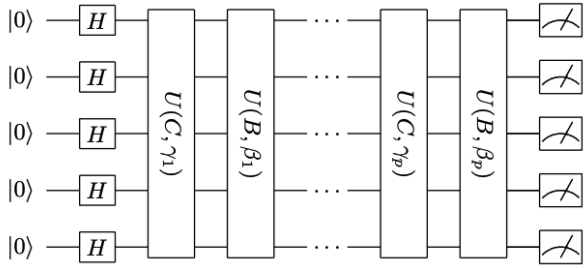


FIG. 2: Framework for a QAOA circuit. Each qubit begins with a Hadamard gate, and then $2p$ gates are performed alternating between applying Hamiltonian C and applying Hamiltonian B.

Figure: Credit: How many qubits are needed for quantum computational supremacy. Dalzell et al.

6. Perform a series of operations parameterized by classical parameters $\vec{\gamma}$ and $\vec{\beta}$ such that the final state vector $|\psi(\vec{\gamma},\vec{\beta})\rangle$ is a superposition of good partitionings

- Create ansatz states $|\psi(\vec{\gamma},\vec{\beta})\rangle$
- $|\psi(\vec{\gamma},\vec{\beta})\rangle = U(B,\beta_p)U(C,\gamma_p)...U(B,\beta_1)U(C,\gamma_1)\,|\psi_s\rangle =$
$$\prod_{i=1}^{p}\left(\prod_{q\in V(G)} e^{-i\beta_i\sigma_q^x}\prod_{<jk>\in E(G)} e^{-i\gamma_i C_{<jk>}}\right)|+\rangle^{\otimes n}$$

7. Optimize for a good set of $\vec{\gamma}$ and $\vec{\beta}$

- Measure this state to compute the objective function. That is, given the current set of parameters $\vec{\gamma}$ and $\vec{\beta}$, how much of the CSP is satisified
- Use a classical optimization algorithm such as Nelder-Mead to maximize $F_p(\vec{\gamma}, \vec{\beta}) = \langle \psi(\vec{\gamma}, \vec{\beta}) | \, C \, | \psi(\vec{\gamma}, \vec{\beta}) \rangle$

Evaluation of QAOA for NISQ: Number of iterations?

- Let M_p be the maximum of F_p over the angles: $M_p = \max_{\vec{\gamma},\vec{\beta}} F_p(\vec{\gamma},\vec{\beta})$
- QAOA needs a big parameter p to see the whole graph
- As $p \to \infty$, $\lim_{p\to\infty} M_p = \max_z C(z)$

Evaluation of QAOA for NISQ: Number of iterations?

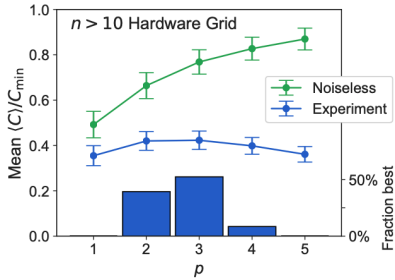


FIG. 5. QAOA performance as a function of depth, p. In ideal simulation, increasing p increases the quality of the solution. For experimental Hardware Grid results, we observe increased performance for $p > 1$ both as measured by the mean over all 10 instances studied for each value of $n \in [11, 23]$ (lines) and statistics of which p value maximizes performance on a per-instance basis (histogram). At larger p, errors overwhelm the theoretical performance increase.

Figure: Credit: [Arute et al., 2020]

Evaluation of QAOA for NISQ: Number of qubits?

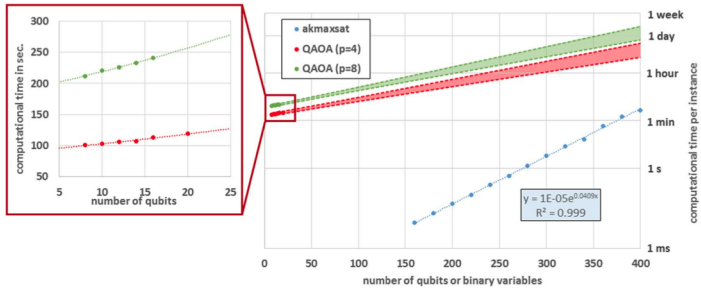


Figure 2. Main panel: Computational cost of solving a single Max-Cut instance on random 3-regular graphs. Blue markers correspond to the classical baseline (AKMAXSAT solver) while red and green marks correspond to the experimental time required by the quantum algorithm QAOA, with $p = 4$ and $p = 8$ respectively. The error bars for the single data points are smaller than the markers (see Supplementary Information). Notice that in the time needed by QAOA to partition graphs with 20 vertices, AKMAXSAT partitions graphs about 20 times larger. The blue dashed line is the result of a fitting procedure with an exponential function. The red and green areas are associated with a 95% confidence interval for the prediction of the QAOA cost based on a linear regression of $\log_{10}(T)$ as a function of the number of qubits (here T is the computational time per instance). This extrapolation should be seen as suggesting a qualitative behavior due to the uncertainty in the extrapolation from relatively small system sizes. Insert panel: Magnification of QAOA datapoints. Notice that exponential curves, and smooth curves in general, locally resemble straight lines and this makes it difficult to exclude other functional forms for the extrapolation. It is, however, believed that even quantum computers will not be able to solve NP-hard problems in polynomial time.

Figure: Credit: [Guerreschi and Matsuura, 2019]

Evaluation of QAOA for NISQ: Number of constraints?

- Findings for MAX-CUT on connected 3-regular graphs [Farhi et al., 2014]
  1. For p = 1, QAOA will always produce a cut whose size is at least 0.6924 times the size of the optimal cut.
  2. This was the best known possible approximation for a few months until classical algorithm found.
  3. For p = 2, the approximation ratio becomes 0.7559 and grows depending on the type of graph.
- Difficulty of solving problems with higher constraint ratios [Akshay et al., 2020]

Evaluation of QAOA for NISQ: Optimization method?

Optimization using gradients [Guerreschi and Smelyanskiy, 2017].

Evaluation of QAOA for NISQ: Generalizations?

- Can be generalized to solve related problems [Hadfield et al., 2019].
- Factoring [Anschuetz et al., 2019].

Read also

- Primary sources: [Farhi et al., 2014]
- Additional source: [Wang and Abdullah, 2018]

Akshay, V., Philathong, H., Morales, M. E. S., and Biamonte, J. D. (2020).
Reachability deficits in quantum approximate optimization.
Phys. Rev. Lett., 124:090504.

Anschuetz, E., Olson, J., Aspuru-Guzik, A., and Cao, Y. (2019).
Variational quantum factoring.
In Feld, S. and Linnhoff-Popien, C., editors, *Quantum Technology and Optimization Problems*, pages 74–85, Cham. Springer International Publishing.

Arute, F. C., Arya, K., Babbush, R., Bacon, D., Bardin, J., Barends, R., Boixo, S., Broughton, M. B., Buckley, B. B., Buell, D. A., Burkett, B., Bushnell, N., Chen, J., Chen, Y., Chiaro, B., Collins, R., Courtney, W., Demura, S., Dunsworth, A., Farhi, E., Fowler, A., Foxen, B. R., Gidney, C. M., Giustina, M., Graff, R., Habegger, S., Harrigan, M., Hong, S., Ioffe, L., Isakov, S., Jeffrey, E., Jiang, Z., Jones, C., Kafri, D., Kechedzhi, K., Kelly, J., Kim, S., Klimov, P., Korotkov, A., Kostritsa, F., Landhuis, D., Laptev, P., Leib, M., Lindmark, M., Lucero, E., Martin, O., Martinis, J., McClean, J. R., McEwen, M., Megrant, A., Mi, X., Mohseni, M., Mruczkiewicz, W., Mutus, J., Naaman, O., Neeley, M., Neill, C., Neukart, F., Neven, H., Niu, M. Y., O'Brien, T. E., O'Gorman, B., Petukhov, A., Putterman, H., Quintana, C., Roushan, P., Rubin, N., Sank, D., Satzinger, K., Skolik, A., Smelyanskiy, V., Strain, D., Streif, M., Sung, K. J., Szalay, M., Vainsencher, A., White, T., Yao, J., Zalcman, A., and Zhou, L. (2020).
Quantum approximate optimization of non-planar graph problems on a planar superconducting processor.
arXiv:2004.04197.

Farhi, E., Goldstone, J., and Gutmann, S. (2014).
A quantum approximate optimization algorithm.
arXiv preprint arXiv:1411.4028.

Guerreschi, G. G. and Matsuura, A. Y. (2019).
Qaoa for max-cut requires hundreds of qubits for quantum speed-up.

Scientific Reports, 9(1):6903.


Guerreschi, G. G. and Smelyanskiy, M. (2017).
Practical optimization for hybrid quantum-classical algorithms.
arXiv preprint arXiv:1701.01450.


Hadfield, S., Wang, Z., O'Gorman, B., Rieffel, E. G., Venturelli, D., and Biswas, R. (2019).
From the quantum approximate optimization algorithm to a quantum alternating operator ansatz.
Algorithms, 12(2):34.


Wang, Q. and Abdullah, T. (2018).
An introduction to quantum optimization approximation algorithm.