Quantum Annealing for Prime Factorization

Shuxian Jiang, Sabre Kais
Department of Chemistry and Computer Science, Purdue University

Keith A. Britt, Alexander J. McCaskey, Travis S. Humble
Quantum Computing Institute, Oak Ridge National Laboratory

Qubits 2018

Integer Factorization Problem

Classical Factorization

- Methods:
  1. Trial Division($n^{\frac{1}{2}}$): try 2,3,5,...,$n^{\frac{1}{2}}$ to divide n
  2. Shanks, Pollard, Strassen (1970s)($n^{\frac{1}{4}}$): complicated math
  3. CFRAC(1970), QS(1980), NFS(1990) $O(\exp^{\sqrt{(ln(n))(ln(ln(n)))}})$: nonrigorous
  4. Elliptic Curve Method(1985)$O(\exp^{\sqrt{(ln(n))(ln(ln(n)))}})$: probabilistic, nonrigorous
- Limitations:

  EXP time if no randomness, no unproved hypotheses
  Quadratic Sieve Method(subexponential, not polynomial)

Integer Factorization Problem

Quantum Factorization

- Gate Model
  Shor's algo: order-finding
    Exponential speedup: polynomial time
    Hard to physically implement
    Largest Number: 21
- Adiabatic Computation Model
  Convert to optimization problem
  1. NMR
     $f = (N - pq)^2$
  2. Ising Machine: D-wave, ...
     Multiplication Table
  3. Nitrogen-Vacancy (NV) center in diamond
     Multiplication Table

Integer Factorization Problem

Quantum Factorization

- Gate Model
  Shor's algo: order-finding
    - Exponential speedup: polynomial time
    - Hard to physically implement
    - Largest Number: 21
- Adiabatic Computation Model
  Convert to optimization problem
  1. NMR
     $f = (N - pq)^2$
  2. Ising Machine: D-wave, ...
     Multiplication Table
  3. Nitrogen-Vacancy (NV) center in diamond
     Multiplication Table

Quantum Adiabatic Computation

Method

1 Define Hamiltonian:

$$\mathcal{H}(t) = (1 - t/T)\mathcal{H}_0 + (t/T)\mathcal{H}_P$$

2 Set system to ground state of initial $\mathcal{H}_0$ (easy)

3* Define final $\mathcal{H}_P$ s.t. its ground state encodes problem's solution

4 System slowly evolves to final state(eigenvector w.r.t. smallest eigenvalue),measure it to get soln

How to encode H_p

$$f_p(s_1, s_2, ..., s_n) = \sum_{k=1}^{K} \sum_{j_1,...,j_k=1}^{n} J_{j_1...j_k} s_{j_1} ... s_{j_k}, s_i = \pm 1$$

is the energy func.(eigenvalue func.) of Hamiltonian

$$\mathcal{H}_p(\sigma_z^{(1)}, \sigma_z^{(2)}, ..., \sigma_z^{(n)}) = \sum_{k=1}^{K} \sum_{j_1,...,j_k=1}^{n} J_{j_1...j_k} \sigma_z^{(j_1)} ... \sigma_z^{(j_k)}$$

Here $\sigma_z^{(i)} = \overbrace{I \otimes I \otimes ... \otimes I}^{i-1} \otimes \sigma_z \otimes \overbrace{I \otimes ... \otimes I}^{n-i}$ with eigenvector $|x_1 x_2 ... x_n\rangle, x_i = \{0, 1\}, s_i = (-1)^{x_i}$

Ising model

Definition

$$\mathcal{H}_p(\sigma_z^{(1)}, \sigma_z^{(2)}, ..., \sigma_z^{(n)}) = \sum_{i=1}^{n} h_i \sigma_z^{(i)} + \sum_{i,j=1}^{n} J_{ij} \sigma_z^{(i)} \sigma_z^{(j)}$$

h_i: external magnetic

J_{ij}: interaction between two adjacent sites i, j

Ising Model $\leftrightarrow$ Quadratic Function

Our Method for Factorization[1]

- Define Cost Function
  - Direct Method: $f = (N - pq)^2$
  - Modified Multiplication Table Method
- Order Reducing Method
  - $x, y, z \in \{0, 1\}$
    $xy = z$ iff $xy - 2xz - 2yz + 3z = 0$,
    $xy \neq z$ iff $xy - 2xz - 2yz + 3z > 0$
    $\Rightarrow x_1, x_2, x_3 \in \{0, 1\}$
    $\min(x_1x_2x_3) = \min_{x_4=x_1x_2}(x_4x_3 + 2(x_1x_2 - 2x_1x_4 - 2x_2x_4 + 3x_4))$
    $\min(-x_1x_2x_3) = \min_{x_4=x_1x_2}(-x_4x_3 + 2(x_1x_2 - 2x_1x_4 - 2x_2x_4 + 3x_4))$

[1] Shuxian Jiang et al. "Quantum Annealing for Prime Factorization". In: *arXiv preprint arXiv:1804.02733* (2018).

Cost Function: Direct Method

For $N = pq$

$p = (p_{l-1}p_{l-2}...p_1 1)_2, q = (q_{l'-1}q_{l'-2}...q_1 1)_2$

$$
\begin{aligned}
\text{Define} \quad f &= (N - pq)^2 \\
&= [N - (\sum_{i=1}^{l-1} 2^i p_i + 1)(\sum_{j=1}^{l'-1} 2^j q_j + 1)]^2 \\
&= N^2 + (\sum_{i=1}^{l-1} 2^i p_i + 1)^2 (\sum_{j=1}^{l'-1} 2^j q_j + 1)^2 \\
&\quad -2N(\sum_{i=1}^{l-1} 2^i p_i + 1)(\sum_{j=1}^{l'-1} 2^j q_j + 1)
\end{aligned}
$$

Reduce Order:

$$\min(x_1x_2x_3) = \min_{x_4 = x_1x_2}(x_4x_3 + 2(x_1x_2 - 2x_1x_4 - 2x_2x_4 + 3x_4))$$

Cost Function: Direct Method

For $N = 15 = 5 \times 3$

$p = (x_1 1)_2 = x_1 * 2 + 1, q = (x_2 x_3 1)_2 = x_2 * 2^2 + x_3 * 2 + 1$

$$
\begin{aligned}
& f(x_1, x_2, x_3) \\
= \; & (N - pq)^2 \\
= \; & [15 - (x_1 * 2 + 1)(x_3 * 2^2 + x_2 * 2 + 1)]^2 \\
= \; & 15^2 + (2x_1 + 1)^2(4x_3 + 2x_2 + 1)^2 - 30(2x_1 + 1)(4x_3 + 2x_2 + 1) \\
= \; & 128x_1x_2x_3 - 56x_1x_2 - 48x_1x_3 + 16x_2x_3 - 52x_1 - 52x_2 - 96x_3 \\
& +196
\end{aligned}
$$

Reduce Order:

$$
\begin{aligned}
& f'(x_1, x_2, x_3, x_4) \\
= \; & 128(x_4x_3 + 2(x_1x_2 - 2x_1x_4 - 2x_2x_4 + 3x_4)) - 56x_1x_2 \\
& -48x_1x_3 + 16x_2x_3 - 52x_1 - 52x_2 - 96x_3 + 196
\end{aligned}
$$

Cost Function: Modified Multiplication Table Method

Table: Multiplication table for $11 \times 13 = 143$ in binary.

	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
p					1	p_2	p_1	1
q					1	q_2	q_1	1
					1	p_2	p_1	1
				q_1	$p_2 q_1$	$p_1 q_1$	q_1	
			q_2	$p_2 q_2$	$p_1 q_2$	q_2		
		1	p_2	p_1	1			
carries		c_4	c_3	c_2	c_1			
$p \times q = 143$	1	0	0	0	1	1	1	1

$$2(p_2 + p_1 q_1 + q_2) + (p_1 + q_1) \quad = \quad 8c_2 + 4c_1 + 3$$

...

Cost Function: Modified Multiplication Table Methods

From

$$2(p_2 + p_1 q_1 + q_2) + (p_1 + q_1) \;\; = \;\; 8c_2 + 4c_1 + 3$$

We got

$$f_1 = (2p_2 + 2p_1 q_1 + 2q_2 - 8c_2 - 4c_1 + p_1 + q_1 - 3)^2$$

Reduce order

$$\min(\pm x_1 x_2 x_3) \;\; = \;\; \min_{x_4 = x_1 x_2}(\pm x_4 x_3 + 2(x_1 x_2 - 2x_1 x_4 - 2x_2 x_4 + 3x_4))$$

Embed to D-wave

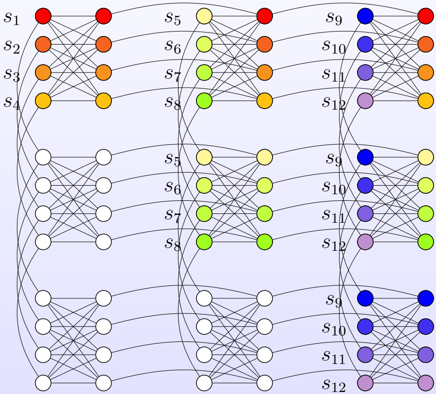
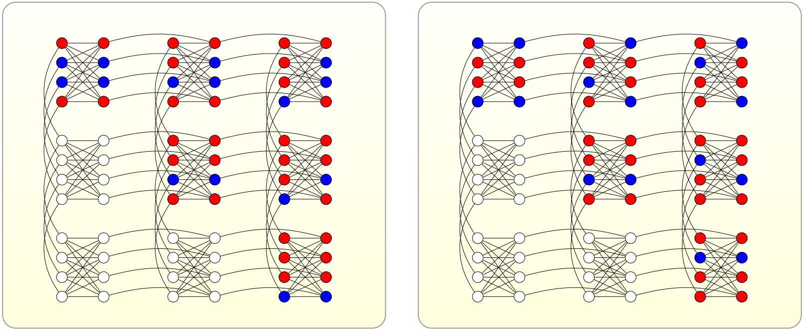


Figure: Embed problem graph of factoring 143 using method one to Chimera graph

Embed to D-wave



(a) Result 13×11 (b) Result 11×13

Figure: Final ground state of factoring 143. Red nodes:+1, Blue nodes:-1. (a) $s_1 = 1, s_2 = -1, s_3 = -1, s_4 = 1$ ($p = 1101, q = 1011$). (b) $s_1 = -1, s_2 = 1, s_3 = 1, s_4 = -1$ ($p = 1011, q = 1101$).

Cost Function: Modified Multiplication Table Method

Table: Multiplication table for $659 \times 571 = 376289$ in binary.

2^{18}	2^{17}	2^{16}	2^{15}	2^{14}	2^{13}	2^{12}	2^{11}	2^{10}	2^{9}	2^{8}	2^{7}	2^{6}	2^{5}	2^{4}	2^{3}	2^{2}	2^{1}	2^{0}
									1	p_8	p_7	p_6	p_5	p_4	p_3	p_2	p_1	1
									1	q_8	q_7	q_6	q_5	q_4	q_3	q_2	q_1	1
									1	p_8	p_7	p_6	p_5	p_4	p_3	p_2	p_1	1
								q_1	p_8q_1	p_7q_1	p_6q_1	p_5q_1	p_4q_1	p_3q_1	p_2q_1	p_1q_1	q_1	
							q_2	p_8q_2	p_7q_2	p_6q_2	p_5q_2	p_4q_2	p_3q_2	p_2q_2	p_1q_2	q_2		
						q_3	p_8q_3	p_7q_3	p_6q_3	p_5q_3	p_4q_3	p_3q_3	p_2q_3	p_1q_3	q_3			
					q_4	p_8q_4	p_7q_4	p_6q_4	p_5q_4	p_4q_4	p_3q_4	p_2q_4	p_1q_4	q_4				
				q_5	p_8q_5	p_7q_5	p_6q_5	p_5q_5	p_4q_5	p_3q_5	p_2q_5	p_1q_5	q_5					
			q_6	p_8q_6	p_7q_6	p_6q_6	p_5q_6	p_4q_6	p_3q_6	p_2q_6	p_1q_6	q_6						
		q_7	p_8q_7	p_7q_7	p_6q_7	p_5q_7	p_4q_7	p_3q_7	p_2q_7	p_1q_7	q_7							
	q_8	p_8q_8	p_7q_8	p_6q_8	p_5q_8	p_4q_8	p_3q_8	p_2q_8	p_1q_8	q_8								
1	p_8	p_7	p_6	p_5	p_4	p_3	p_2	p_1	1									
c_{14}	c_{13}			c_9	c_8	c_7	c_6	c_5	c_4	c_3		c_2	c_1					
		c_{12}	c_{11}	c_{10}														
1	0	1	1	0	1	1	1	1	0	1	1	1	1	0	0	0	0	1

Experimental Results

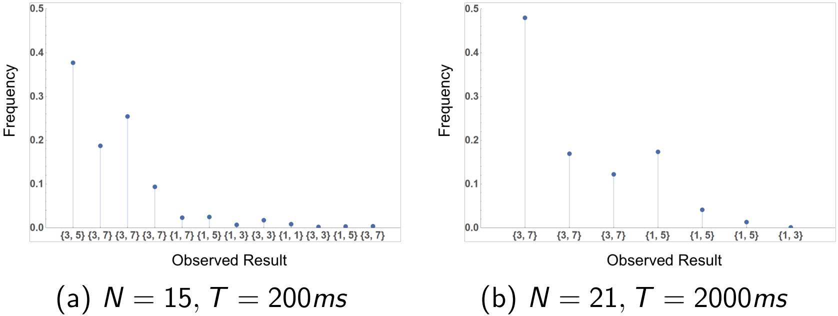


Figure: D-wave Results for Method One: rates of getting different solutions.

Experimental Results

Table: D-wave Results for Method Two

N	factors	logic#qb	phy#qb	embed	sol
35	7× 5	5	8	✓	✓
143	13× 11	12	48	✓	✓
391	23× 17	20	113	✓	✓
1517	41× 37	30	270	✓	✓
8137	103 × 79	43	535	✓	✓
56153	241× 233	58	1085	✓	–
249919	509×491	77	1803	✓	–
376289	659×571	94	–	–	–