WASEDA University
Graduate School of Information, Production and Systems

Poster C6

Prime Factorization with Fewer Qubits by Combining Quantum Annealing and Classical Algorithm

Geguang Miao, Shinji Kimura

(Waseda University)

Adiabatic Quantum Computing Conference 2021 (AQC 2021)

June 23, 2021

Background: Prime Factorization

- For an input number N, find primes p and q satisfying

$$N = p \times q$$

  - Belong to NP problem, but generally not considered to be NP-complete [1]
- Recently, Ising computers have been developed and applied to combinatorial optimization problems
  - Many combinatorial optimization problems can be mapped into Ising model [2]
    - Prime Factorization is also considered for application
  - Ising model or QUBO (Quadratic Unconstrained Binary Optimization) formulation is the input of Ising computers
- QUBO is to decide the variable values minimizing
  - $O(\boldsymbol{x}) = \sum_i Q_{i,i} x_i + \sum_{i<j} Q_{i,j} x_i x_j \, , x_i \in \{0,1\}$
  - Formula of quadratic terms of binary variables

[1] Goldreich, O., & Wigderson, A. (2008). IV. 20 Computational Complexity. In The Princeton Companion to Mathematics (pp. 575-604). Princeton University Press.

[2] Lucas, A. (2014). Ising formulations of many NP problems. Frontiers in Physics, 2, 5.

Related Work: Multiplication Table Method [3]

- Binary multiplication is represented as addition of partial products
  - Addition of each column i should equal to N_i plus carry-outs
  - Carry variables are introduced column-wise
    - c_{ij} is generated at column i and affects to j
- MSBs and LSBs of p and q are set to 1
- Each column corresponds one term of $O(\boldsymbol{x})$
  - The square of the addition of each column terms plus carry-ins minus carry-outs and N_i, then sum
- Weakness
  - Requiring a lot of carry variables
  - Lots of auxiliary variables also needed to convert higher order terms to quadratic terms

Prime factorization problem

$N = p \times q$

p					1	p_2	p_1	1
q					1	q_2	q_1	1
$p \cdot q$					1	p_2	p_1	1
				q_1	p_2q_1	p_1q_1	q_1	
			q_2	p_2q_2	p_1q_2	q_2		
		1	p_2	p_1	1			
Carries	c_{67}	c_{56}	c_{45}	c_{34}	c_{23}	c_{12}		
	c_{57}	c_{46}	c_{35}	c_{24}				
N	1	0	0	0	1	1	1	1

Expanding, simplifying by $x^2 = x$, erasing high-order terms

$$
\begin{aligned}
&(p_1 + q_1 - 2c_{12} - 1)^2 + \\
&(p_2 + p_1q_1 + q_2 + c_{12} - (2c_{23} + 4c_{24}) - 1)^2 + \\
&(1 + p_2q_1 + p_1q_2 + 1 + c_{23} - (2c_{34} + 4c_{35}) - 1)^2 + \\
&(q_1 + p_2q_2 + p_1 + c_{24} + c_{34} - (2c_{45} + 4c_{46}))^2 + \\
&(p_2 + q_2 + c_{45} + c_{35} - (2c_{56} + 4c_{57}))^2 + \\
&(1 + c_{56} + c_{46} - 2c_{67})^2 + \\
&(c_{57} + c_{67} - 1)^2
\end{aligned}
$$

QUBO

[3] Schaller, G., & Schützhold, R. (2007). The role of symmetries in adiabatic quantum algorithms. arXiv preprint arXiv:0708.1882.

Related Work: Modified Multiplication Table Method [4]

- Several consecutive columns are merged into one block
  - 2 to 4 consecutive columns are combined
- Carries are generated block by block and $O(x)$ is also constructed from block by block
  - Carry variables are decided based on the former block
  - The number of carry variables can be reduced
- Factoring up to 376289 (19-bit number) using 94 logical qubits

Prime factorization problem

$N = p \times q$

Blocks	Ⅲ			Ⅱ		Ⅰ		
p					1	p_2	p_1	1
q					1	q_2	q_1	1
$p \cdot q$					1	p_2	p_1	1
				q_1	p_2q_1	p_1q_1	q_1	
			q_2	p_2q_2	p_1q_2	q_2		
		1	p_2	p_1	1			
$Carries$		c_4	c_3	c_2	c_1			
N	1	0	0	0	1	1	1	1

$$\left((p_1 + q_1) + 2(p_2 + p_1q_1 + q_2) - (8c_2 + 4c_1) - 3\right)^2 + \left((1 + p_2q_1 + p_1q_2 + 1 + c_1) + 2(q_1 + p_2q_2 + p_1 + c_2) - (8c_4 + 4c_3) - 1\right)^2 + \left((q_2 + p_2 + c_3) + 2(1 + c_4) - 4\right)^2$$

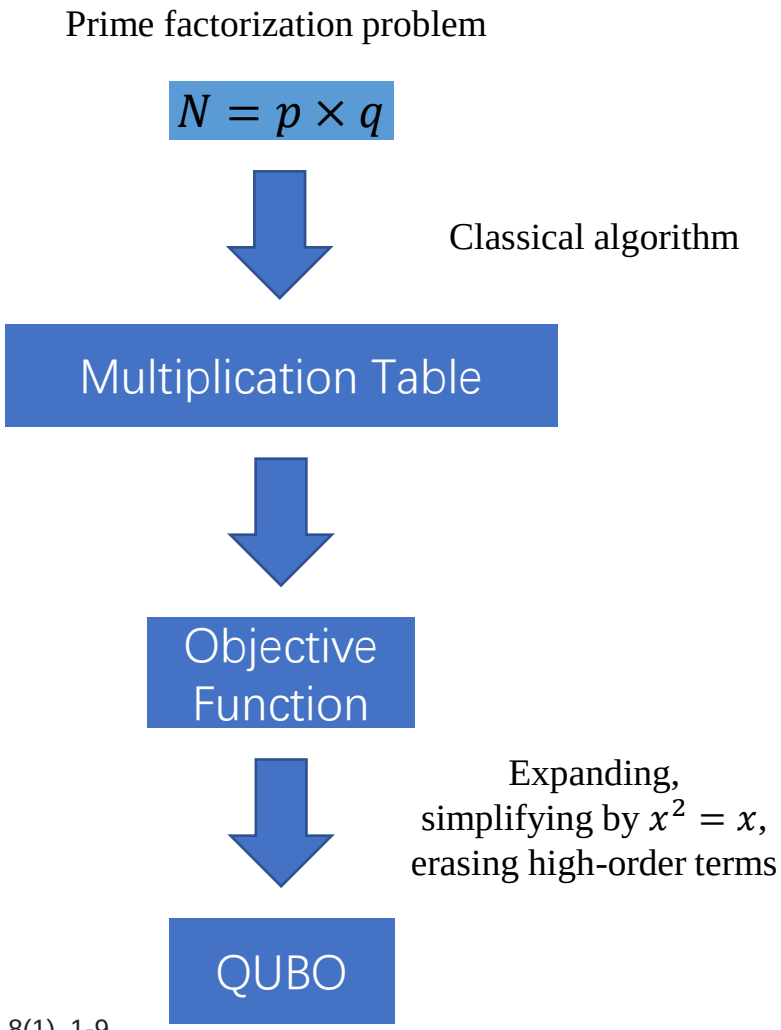
Expanding, simplifying by $x^2 = x$, erasing high-order terms

QUBO

[4] Jiang, S., Britt, K. A., McCaskey, A. J., Humble, T. S., & Kais, S. (2018). Quantum annealing for prime factorization. Scientific reports, 8(1), 1-9.

Related Work: Modified Multiplication Table Method with Optimized Parameters [5]

- Based on Modified Multiplication Method [4]
- To further reduce the number of carry variables
  - Employing a classical algorithm to generate carry variables, considering
    - The generation of carries is restricted by the target value
    - Carry-ins are usually smaller than assigning all carry variables to 1
- Factoring up to 1005973 (20-bit number) using 89 variables
- There needs a method to reduce variables for factoring larger numbers



[4] Jiang, S., Britt, K. A., McCaskey, A. J., Humble, T. S., & Kais, S. (2018). Quantum annealing for prime factorization. Scientific reports, 8(1), 1-9.

[5] Peng, W., Wang, B., Hu, F., Wang, Y., Fang, X., Chen, X., & Wang, C. (2019). Factoring larger integers with fewer qubits via quantum annealing with optimized parameters. SCIENCE CHINA Physics, Mechanics & Astronomy, 62(6), 60311.

Proposed Method: Multi-Step Quantum Annealing with Combination

- Construct QUBOs block by block and solve independently
  - Several groups of solutions obtained after annealing
- To obtain the correct solutions
  - Classical algorithm employed to combining several groups into one group
    - Same variables in the different groups should have same values

3 QUBOs are solved independently
(This is called as multi step)
3 solutions are obtained

Blocks	Ⅲ			Ⅱ		Ⅰ		
p					1	p_2	p_1	1
q					1	q_2	q_1	1
$p \cdot q$					1	p_2	p_1	1
				q_1	p_2q_1	p_1q_1	q_1	
			q_2	p_2q_2	p_1q_2	q_2		
		1	p_2	p_1	1			
$Carries$		c_4	c_3	c_2	c_1			
N	1	0	0	0	1	1	1	1

$$\left((q_2 + p_2 + c_3) + 2(1 + c_4) - 4\right)^2$$

$$\left((1 + p_2q_1 + p_1q_2 + 1 + c_1) + 2(q_1 + p_2q_2 + p_1 + c_2) - (8c_4 + 4c_3) - 1\right)^2$$

$$\left((p_1 + q_1) + 2(p_2 + p_1q_1 + q_2) - (8c_2 + 4c_1) - 3\right)^2$$

Implementation and Evaluation

- QUBO construction system is made based on
  - python 3.8.5 with
  - PyQUBO 0.4.0 [6] and
  - dwave-Qbsolv 0.3.1 [7]
- Dividing position
  - The position of the first bit of every block
- The data of Modified Multiplication Table Method and Modified Multiplication Table Method are from [5]

Instance	Dividing Position	Model	No. of variables
143 = 11 × 13	[1, 3, 5]	[4]	12
		[5]	5
		Proposal	11
221 = 13 × 17	[1, 4, 6]	[4]	15
		[5]	9
		Proposal	11
247 = 13 × 19	[1, 4, 6]	[4]	15
		[5]	10
		Proposal	11
323 = 17 × 19	[1, 4, 6]	[4]	20
		[5]	13
		Proposal	16
437 = 19 × 23	[1, 4, 6]	[4]	20
		[5]	13
		Proposal	16
589 = 19 × 31	[1, 4, 7]	[4]	19
		[5]	12
		Proposal	18
667 = 23 × 29	[1, 4, 6]	[4]	20
		[5]	12
		Proposal	17
899 = 29 × 31	[1, 4, 6]	[4]	20
		[5]	13
		Proposal	17

[4] Jiang, S., Britt, K. A., McCaskey, A. J., Humble, T. S., & Kais, S. (2018). Quantum annealing for prime factorization. Scientific reports, 8(1), 1-9.

[5] Peng, W., Wang, B., Hu, F., Wang, Y., Fang, X., Chen, X., & Wang, C. (2019). Factoring larger integers with fewer qubits via quantum annealing with optimized parameters. SCIENCE CHINA Physics, Mechanics & Astronomy, 62(6), 60311.

[6] Tanahashi, K., Takayanagi, S., Motohashi, T., & Tanaka, S. (2019). Application of Ising machines and a software development for Ising machines. Journal of the Physical Society of Japan, 88(6), 061010.

[7] http://github.com/dwavesystems/qbsolv

Experimental Result 2

Instance	Dividing Position	Model	No. of variables
989 = 23 × 43	[1, 4, 7]	[4]	24
		[5]	16
		Proposal	22
1073 = 29 × 37	[1, 4, 7]	[4]	24
		[5]	18
		Proposal	23
1591 = 37 × 43	[1, 4, 7]	[4]	29
		[5]	22
		Proposal	27
2449 = 31 × 79	[1, 4, 7]	[4]	28
		[5]	23
		Proposal	26
59989 = 239 × 251	[1, 4, 7, 10, 13]	[4]	59
		[5]	52
		Proposal	38
376289 = 571 × 659	[1, 5, 8, 11, 14, 17]	[4]	95
		[5]	90
		Proposal	56
1005973 = 997 × 1009	[1, 4, 7, 10, 13, 16]	[4]	96
		[5]	89
		Proposal	56

Variables can be reduced on large numbers

[4] Jiang, S., Britt, K. A., McCaskey, A. J., Humble, T. S., & Kais, S. (2018). Quantum annealing for prime factorization. Scientific reports, 8(1), 1-9.

[5] Peng, W., Wang, B., Hu, F., Wang, Y., Fang, X., Chen, X., & Wang, C. (2019). Factoring larger integers with fewer qubits via quantum annealing with optimized parameters. SCIENCE CHINA Physics, Mechanics & Astronomy, 62(6), 60311.

[6] Tanahashi, K., Takayanagi, S., Motohashi, T., & Tanaka, S. (2019). Application of Ising machines and a software development for Ising machines. Journal of the Physical Society of Japan, 88(6), 061010.

[7] http://github.com/dwavesystems/qbsolv

Conclusions and Future Work

- A Multi-Step Quantum Annealing with Combination method is proposed
  - QUBOs are constructed block by block of modified multiplication table
  - Each QUBO is solved independently
  - Obtained solution sets are merged to one
- Proposed method is implemented in python and quantum annealing process is simulated using Qbsolv 0.3.1 provided by D-Wave
  - The number of variables for constructing QUBOs can be reduced for factorization of large numbers
- Merits
  - The number of variables of a QUBO can be reduced
- Demerits
  - Solutions of each QUBO might be large
- Future work
  - Reducing variables with reasonable number of solutions

Reference and Acknowledgement

[1] Goldreich, O., & Wigderson, A. (2008). IV. 20 Computational Complexity. In The Princeton Companion to Mathematics (pp. 575-604). Princeton University Press.

[2] Lucas, A. (2014). Ising formulations of many NP problems. Frontiers in Physics, 2, 5.

[3] Schaller, G., & Schützhold, R. (2007). The role of symmetries in adiabatic quantum algorithms. arXiv preprint arXiv:0708.1882.

[4] Jiang, S., Britt, K. A., McCaskey, A. J., Humble, T. S., & Kais, S. (2018). Quantum annealing for prime factorization. Scientific reports, 8(1), 1-9.

[5] Peng, W., Wang, B., Hu, F., Wang, Y., Fang, X., Chen, X., & Wang, C. (2019). Factoring larger integers with fewer qubits via quantum annealing with optimized parameters. SCIENCE CHINA Physics, Mechanics & Astronomy, 62(6), 60311.

[6] Tanahashi, K., Takayanagi, S., Motohashi, T., & Tanaka, S. (2019). Application of Ising machines and a software development for Ising machines. Journal of the Physical Society of Japan, 88(6), 061010.

[7] http://github.com/dwavesystems/qbsolv

A part of this work was performed for Council for Science, Technology and Innovation (CSTI), Cross-ministerial Strategic Innovation Promotion Program (SIP), “Photonics and Quantum Technology for Society 5.0”(Funding agency : QST).