Variational Quantum Factoring

Siddhant Midha & Neelkanth Rawat

Factoring as a Binary Optimization problem

- Consider factoring of $m = p \cdot q$, where their binary representation is:

Factoring as a Binary Optimization problem

- Consider factoring of $m = p \cdot q$, where their binary representation is:

$$m = \sum_{k=0}^{n_m-1} 2^k m_k; \, p = \sum_{k=0}^{n_p-1} 2^k p_k; \, q = \sum_{k=0}^{n_q-1} 2^k q_k$$

with $m_k, p_k, q_k \in \{0, 1\}$

Factoring as a Binary Optimization problem

- Consider factoring of $m = p \cdot q$, where their binary representation is:

$$m = \sum_{k=0}^{n_m - 1} 2^k m_k; p = \sum_{k=0}^{n_p - 1} 2^k p_k; q = \sum_{k=0}^{n_q - 1} 2^k q_k$$

  with $m_k, p_k, q_k \in \{0, 1\}$
- Without loss of generality:

Factoring as a Binary Optimization problem

- Consider factoring of $m = p \cdot q$, where their binary representation is:

$$m = \sum_{k=0}^{n_m - 1} 2^k m_k; \; p = \sum_{k=0}^{n_p - 1} 2^k p_k; \; q = \sum_{k=0}^{n_q - 1} 2^k q_k$$

with $m_k, p_k, q_k \in \{0, 1\}$

- Without loss of generality: $p \geqslant q$; $n_p = n_m$ and $n_q = \left\lceil \frac{n_m}{2} \right\rceil$

Factoring as a Binary Optimization problem

- Consider factoring of $m = p \cdot q$, where their binary representation is:

$$m = \sum_{k=0}^{n_m-1} 2^k m_k ; p = \sum_{k=0}^{n_p-1} 2^k p_k ; q = \sum_{k=0}^{n_q-1} 2^k q_k$$

with $m_k, p_k, q_k \in \{0, 1\}$

- Without loss of generality: $p \geqslant q$; $n_p = n_m$ and $n_q = \left\lceil \frac{n_m}{2} \right\rceil$

Generic Idea

[Ans+18]

- If one carries out the binary multiplication $p \cdot q$, bits representing m, p, and q satisfies a set of $n_c = n_p + n_q - 1 \in O(n_m)$ equations:

Generic Idea

[Ans+18]

- If one carries out the binary multiplication $p \cdot q$, bits representing m, p, and q satisfies a set of $n_c = n_p + n_q - 1 \in O(n_m)$ equations:

$$\underbrace{\sum_{j=0}^{i} q_i p_{i-j}}_{E_1^i} + \underbrace{\sum_{j=0}^{i-1} z_{j,i}}_{E_2^i} - m_i - \underbrace{\sum_{j=1}^{n_c} 2^j z_{i,j+i}}_{E_3^i} = 0 \tag{1}$$

Generic Idea

[Ans+18]

- If one carries out the binary multiplication $p \cdot q$, bits representing m, p, and q satisfies a set of $n_c = n_p + n_q - 1 \in O(n_m)$ equations:

$$\underbrace{\sum_{j=0}^{i} q_i p_{i-j}}_{E_1^i} + \underbrace{\sum_{j=0}^{i-1} z_{j,i}}_{E_2^i} - m_i - \underbrace{\sum_{j=1}^{n_c} 2^j z_{i,j+i}}_{E_3^i} = 0 \tag{1}$$

where $0 \leqslant i < n_c$, $z_{i,j} \in \{0, 1\}$: Carry from *i'th* bit position to *j'th* bit position

Generic Idea

[Ans+18]

- If one carries out the binary multiplication $p \cdot q$, bits representing m, p, and q satisfies a set of $n_c = n_p + n_q - 1 \in O(n_m)$ equations:

$$\underbrace{\sum_{j=0}^{i} q_i p_{i-j}}_{E_1^i} + \underbrace{\sum_{j=0}^{i-1} z_{j,i}}_{E_2^i} - m_i - \underbrace{\sum_{j=1}^{n_c} 2^j z_{i,j+i}}_{E_3^i} = 0 \qquad (1)$$

where $0 \leqslant i < n_c$, $z_{i,j} \in \{0,1\}$: Carry from *i'th* bit position to *j'th* bit position

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

Generic Idea

[Ans+18]

- If one carries out the binary multiplication $p \cdot q$, bits representing m, p, and q satisfies a set of $n_c = n_p + n_q - 1 \in O(n_m)$ equations:

$$\underbrace{\sum_{j=0}^{i} q_i p_{i-j}}_{E_1^i} + \underbrace{\sum_{j=0}^{i-1} z_{j,i}}_{E_2^i} - m_i - \underbrace{\sum_{j=1}^{n_c} 2^j z_{i,j+i}}_{E_3^i} = 0 \qquad (1)$$

where $0 \leqslant i < n_c$, $z_{i,j} \in \{0,1\}$: Carry from *i'th* bit position to *j'th* bit position

- $C_i = \sum_{j=0}^{i} q_i p_{i-j} + \sum_{j=0}^{i-1} z_{j,i} - m_i - \sum_{j=1}^{n_c} 2^j z_{i,j+i}$
- Hence the problem of factoring is equivalent to solving for binary variables p_i, q_i and z_i which solves:

Generic Idea

[Ans+18]

- If one carries out the binary multiplication $p \cdot q$, bits representing m, p, and q satisfies a set of $n_c = n_p + n_q - 1 \in O(n_m)$ equations:

$$\underbrace{\sum_{j=0}^{i} q_i p_{i-j}}_{E_1^i} + \underbrace{\sum_{j=0}^{i-1} z_{j,i}}_{E_2^i} - m_i - \underbrace{\sum_{j=1}^{n_c} 2^j z_{i,j+i}}_{E_3^i} = 0 \quad (1)$$

where $0 \leqslant i < n_c$, $z_{i,j} \in \{0, 1\}$: Carry from *i'th* bit position to *j'th* bit position

- $C_i = \sum_{j=0}^{i} q_i p_{i-j} + \sum_{j=0}^{i-1} z_{j,i} - m_i - \sum_{j=1}^{n_c} 2^j z_{i,j+i}$
- Hence the problem of factoring is equivalent to solving for binary variables p_i, q_i and z_i which solves:

$$\sum_{i=0}^{n_c} C_i^2 = 0$$

Illustrative Example

[Xu+12]

	b_7	b_6	b_5	b_4	b_3	b_2	b_1	b_0
Multiplier					1	p_2	p_1	1
					1	q_2	q_1	1
Binary-multiplication					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			
Carry	z_{67}	z_{56}	z_{45}	z_{34}	z_{23}	z_{12}		
	z_{57}	z_{46}	z_{35}	z_{24}				
Product	1	0	0	0	1	1	1	1

$$
\begin{aligned}
p_1 + q_1 &= 1 + 2z_{12} \\
p_2 + p_1q_1 + q_2 + z_{12} &= (m_2 = 1) + 2z_{23} + 2^2 z_{24} \\
1 + p_2q_1 + p_1q_2 + 1 + z_{23} &= (m_3 = 1) + 2z_{34} + 2^2 z_{35} \\
q_1 + p_2q_2 + p_1 + z_{34} + z_{24} &= (m_4 = 0) + 2z_{45} + 2^2 z_{57} \\
1 + z_{56} + z_{46} &= (m_6 = 0) + 2z_{67} \\
z_{67} + z_{57} &= 1
\end{aligned}
$$

Figure: (Left) binary multiplication (Right) Factoring equations

Further Simplification

Classical pre-processing

Let $x, y, z \in \mathbb{F}_2$ and let $a, b \in \mathbb{Z}^+$. Note the following

$$xy - 1 = 0 \implies x = y = 1 \tag{2}$$

$$x + y - 1 = 0 \implies xy = 0 \tag{3}$$

$$a - bx = 0 \implies x = 1 \tag{4}$$

$$\sum_i x_i = 0 \implies x_i = 0 \forall i \tag{5}$$

$$\sum_{i=1}^{a} x_i - a = 0 \implies x_i = 1 \forall i \tag{6}$$

Further Simplification

Truncation of the last term

Recall,

Further Simplification

Truncation of the last term

Recall,

$$\underbrace{\sum_{j=0}^{i} q_i p_{i-j}}_{E_1^i} + \underbrace{\sum_{j=0}^{i} z_{j,i}}_{E_2^i} - m_i - \underbrace{\sum_{j=1}^{n_c} 2^j z_{i,j+i}}_{E_3^i} = 0 \tag{7}$$

Fix i.

Further Simplification

Truncation of the last term

Recall,

$$\underbrace{\sum_{j=0}^{i} q_i p_{i-j}}_{E_1^i} + \underbrace{\sum_{j=0}^{i} z_{j,i}}_{E_2^i} - m_i - \underbrace{\sum_{j=1}^{n_c} 2^j z_{i,j+i}}_{E_3^i} = 0 \tag{7}$$

Fix i. Note that

- $E_1^i, E_2^i \leqslant i + 1$

Further Simplification

Truncation of the last term

Recall,

$$\underbrace{\sum_{j=0}^{i} q_i p_{i-j}}_{E_1^i} + \underbrace{\sum_{j=0}^{i} z_{j,i}}_{E_2^i} - m_i - \underbrace{\sum_{j=1}^{n_c} 2^j z_{i,j+i}}_{E_3^i} = 0 \tag{7}$$

Fix i. Note that

- $E_1^i, E_2^i \leqslant i + 1$
- Best case if $m_i = 0$, if $\exists j_0 \leqslant n_c$ s.t. $2^{j_0} > 2(i+1) \equiv j_0 > \log_2(2i+2)$ then we cannot solve the equation (7). Thus, we will have to set $z_{i,i+j} := 0$ for all $j \geqslant j_0$.

Back to the Example

Simplified Clauses

$$
\begin{aligned}
p_1 + q_1 &= 1 + 2z_{12} \\
p_2 + p_1q_1 + q_2 + z_{12} &= (m_2 = 1) + 2z_{23} + 2^2z_{24} \\
1 + p_2q_1 + p_1q_2 + 1 + z_{23} &= (m_3 = 1) + 2z_{34} + 2^2z_{35} \\
q_1 + p_2q_2 + p_1 + z_{34} + z_{24} &= (m_4 = 0) + 2z_{45} + 2^2z_{57} \\
1 + z_{56} + z_{46} &= (m_6 = 0) + 2z_{67} \\
z_{67} + z_{57} &= 1
\end{aligned}
$$

Simplified equations:

$$
\begin{aligned}
p_1 + q_1 = 1 &\implies p_1 + q_1 - 1 = 0 \\
p_2 + q_2 = 1 &\implies p_2 + q_2 - 1 = 0 \\
p_2q_1 + p_1q_2 = 1 &\implies p_2q_1 + p_1q_2 - 1 = 0
\end{aligned}
$$

Ising Hamiltonian for the problem

- Let C_i' be the clauses obtained after the pre-processing step. The solution to equation $C_i' = 0$ corresponds to the minimization of the energy function (classical scalar function)

Ising Hamiltonian for the problem

- Let $C_i^{'}$ be the clauses obtained after the pre-processing step. The solution to equation $C_i^{'} = 0$ corresponds to the minimization of the energy function (classical scalar function)

$$E = \sum_{i}^{n_c} {C_i^{'}}^2$$

Ising Hamiltonian for the problem

- Let $C_i^{'}$ be the clauses obtained after the pre-processing step. The solution to equation $C_i^{'} = 0$ corresponds to the minimization of the energy function (classical scalar function)

$$E = \sum_{i}^{n_c} C_i^{'2}$$

- Note: The minimum value of $C_i^{'2}$ would be 0.

Ising Hamiltonian for the problem

- Let $C_i^{'}$ be the clauses obtained after the pre-processing step. The solution to equation $C_i^{'} = 0$ corresponds to the minimization of the energy function (classical scalar function)

$$E = \sum_{i}^{n_c} C_i^{'\,2}$$

- Note: The minimum value of $C_i^{'\,2}$ would be 0.
- (Classical)$E = \sum_{i}^{n_c} C_i^{'\,2} \rightarrow$ Quantum Hamiltonian $H = \sum_{i} \hat{C}_i^{'\,2}$

$$\text{replace } b_k \rightarrow \frac{1}{2}\left(1 - \sigma^z_{b,k}\right)$$

. This is because eigenvalues of $\sigma^z_{b,k} = \pm 1$

References

[Ans+18] Eric R. Anschuetz et al. *Variational Quantum Factoring*. 2018. DOI: 10.48550/ARXIV.1808.08927. URL: https://arxiv.org/abs/1808.08927.

[Xu+12] Nanyang Xu et al. "Quantum Factorization of 143 on a Dipolar-Coupling Nuclear Magnetic Resonance System". In: *Phys. Rev. Lett.* 108 (13 2012), p. 130501. DOI: 10.1103/PhysRevLett.108.130501. URL: https://link.aps.org/doi/10.1103/PhysRevLett.108.130501.