A factorisation algorithm in Adiabatic Quantum Computation

Tien D Kieu

Centre for Quantum and Optical Science, Swinburne University of Technology, Victoria, Australia

E-mail: tien.d.kieu@gmail.com and tdkieu@swin.edu.au

Keywords: Adiabatic Quantum Computation, Quantum Algorithms, factorisation problem

Abstract

The problem of factorising positive integer \( N \) into two integer factors \( x \) and \( y \) is first reformulated as an optimisation problem over the positive integer domain of either of the Diophantine polynomials
\[
Q_N(x, y) = N^2(N - xy)^2 + x(x - y)^2 \quad \text{or} \quad R_N(x, y) = N^2(N - xy)^2 + (x - y)^2 + x,
\]
each of which the optimal solution is unique with \( x \leq \sqrt{N} \leq y \), and \( x = 1 \) if and only if \( N \) is prime. An algorithm in the context of Adiabatic Quantum Computation is then proposed for the general factorisation problem.

Factoring an integer into its prime constituents has attracted much interest since the advance of the RSA public-private key encryption [1]. It is suspected that factorisation is NP-intermediate, that is, in the NP class but may be not quite NP-complete. While there does not yet exist any polynomial-time algorithm for the problem on a classical/Turing computer, the discovery of Shor’s quantum algorithm with quantum circuits [2] has been one of the main motivations for research into quantum computation and building of quantum computers.

In this paper we also consider the factorisation problem in the realm of quantum computation but with adiabatic processes, in complementary addition to the computation with quantum circuits. Also recently, the authors of [3] have considered the problem with quantum annealing. We first reformulate in the next section the factorisation into two integer factors as an optimisation of some corresponding Diophantine polynomials over the integer domain. The optimisation could also be repeatedly applied to any integer having more than two prime factors. Based on this reformulation, we then present an algorithm in the context of AQC (Adiabatic Quantum Computation) for the general factorisation problem. Following that are some numerical illustrations of the algorithm and discussion on the lower bound of the computing time with the help of an energy-time uncertainty relation. The paper is then concluded with some remarks.

Factorisation as an optimisation problem

We first consider the problem of factorising a natural integer \( N \) into two integer factors \( x \) and \( y \). We propose that this problem can be reformulated as an optimisation problem over the integer domain of the following Diophantine polynomial
\[
\min_{x,y \in \mathbb{N}} \{ Q_N(x, y) = N^2(N - xy)^2 + x(x - y)^2 \}.
\] (1)

Without the second term in \( Q_N \) above, the optimal solutions contain the trivial unity factor. We could eliminate this triviality with this second term replaced by \((x-y)^2\), but there still remains a symmetry between \( x \) and \( y \). We now show that the polynomial \( Q_N(x,y) \) in (1) is minimised if and only if \( xy = N \) where \( x \leq y \) and \( x \) is nearest to, but not exceeding, the integer part of \( \sqrt{N} \). The optimal solution thus has no trivial factor \( x = 1 \) unless \( N \) is prime.

For \( xy = N \) the first term on the rhs of (1) vanishes and the remaining second term is obviously smaller for \( 1 \leq x \leq \sqrt{N} \leq y \). In this case, the second term is a one-variable function \( x(x - N/x)^2 \), and it is not difficult to see that this term is a decreasing function for \( 1 \leq x \leq \sqrt{N} \). We then have
The second line results from the fact that $x(x - N/x)^2$ obtains its maximum value at the boundary where $x = 1$. The closer $x$ is to the integer part of $\sqrt{N}$ the smaller the value of $x(x - N/x)^2$.

Now if $xy = N$ then obviously $(N - xy)^2 \geq 1$ and the first term of (1) is consequently not less than $N^2$. Thus

$$Q_N(x, y) \big|_{xy=N} \geq N^2 + x(x - y)^2,$$

Combining (2) and (3), we have for $N > 1$

$$Q_N(x, y) \big|_{xy=N} > Q_N(x, y) \big|_{N=xy}.\quad (4)$$

The second term $x(x - y)^2$ of $Q_N(x, y)$ in (1) is thus designed to introduce an asymmetry between $x$ and $y$, enforcing $x \leq y$ at the optimum value, and to eliminate the trivial unity factor of $N$ unless $N$ is prime. The optimisation problem (1) thus has a unique solution $(x, y)$ for $xy = N$ with $x \leq \sqrt{N} \leq y$. In general, $x$ is the integer factor nearest to, but not exceeding, $\sqrt{N}$. Consequently, $x = 1$ if and only if $N$ is prime.

The optimisation of $Q_N(x, y)$ can thus also determine the primality of $N$.

For $N$ having more than one pair of two prime factors, the optimisation of $Q_N(x, y)$ still admits only one unique solution to yield a non-trivial factoring pair of $N$. For $N$ having more than two prime factors we can apply the optimisation repeatedly for the successive factors to obtain the constituent prime factors.

It can be shown that the objective function in (1) is non-convex as depicted in figure 1 for a slice of the polynomial for $N = 6$ along the plane $y + x = 5$.

**An AQC algorithm for the factorisation problem**

AQC [5, 6] makes use of some appropriate time-varying Hamiltonians and an initial state. The computation starts with the readily constructible ground state $|g\rangle$ of an initial Hamiltonian $H_I$ which is then adiabatically extrapolated to the final target Hamiltonian $H_F$ whose ground state $|g\rangle$ encodes the desirable solution of the...
problem and could be then obtained with reasonably high probability. The interpolation between \( H_I \) and \( H_P \) is facilitated by a time-dependent Hamiltonian in the time interval \( 0 \leq t \leq T \),

\[
\mathcal{H}(t) = f(t/T)H_I + g(t/T)H_P,
\]

(5)
either in a temporally linear manner (that is, \( f(t/T) = (1 - t/T) \) and \( g(t/T) = t/T \)); or otherwise with \( f(0) = 1 = g(1) \) and \( f(1) = 0 = g(0) \). We also assume that both \( f \) and \( g \) are continuous, and \( g \) is semi-positive for all \( t \in [0, T] \). Such a time evolution is captured by the following Schrödinger equation in the time interval \([0, T]\)

\[
i\partial_t |\psi(t)\rangle = \mathcal{H}(t) |\psi(t)\rangle,
\]

\[
|\psi(0)\rangle = |g_i\rangle.
\]

(6)

As the rate of the evolution of the Hamiltonian approaches zero, the end state \( |\psi(T)\rangle \) asymptotically converges to the target state \( |g_j\rangle \) as asserted by the quantum adiabatic theorem [7].

The initial Hamiltonian \( H_I \) and its ground state \( |g_I\rangle \)

Corresponding to the variable \( x \), we introduce the operators \( a_x^\dagger \) and \( a_x \), which respectively create and annihilate the number states \( |n_x\rangle \), for \( n_x = 0, 1, \ldots \):

\[
[a_x, a_x^\dagger] = 1,
\]

\[
a_x^\dagger |n_x\rangle = \sqrt{n_x + 1} |n_x + 1\rangle,
\]

\[
a_x |n_x\rangle = \sqrt{n_x} |n_x - 1\rangle, \quad n_x \geq 1,
\]

\[
a_x |0\rangle = 0,
\]

(7)

and the number operators \( \hat{n}_x \) are constructed in the usual way:

\[
\hat{n}_x = a_x^\dagger a_x,
\]

\[
\hat{n}_x |n_x\rangle = n_x |n_x\rangle.
\]

(8)

Similarly for the variable \( y \) with \( a_y^\dagger, a_y \) and \( \hat{n}_y \).

We propose to start the AQC with the following initial Hamiltonian \( H_I \):

\[
H_I = (a_x^\dagger - \theta_x^\ast)(a_x - \theta_x) + (a_y^\dagger - \theta_y^\ast)(a_y - \theta_y),
\]

(9)

for some c-numbers \( \theta_x \) and \( \theta_y \). The states in the total Hilbert space can be now decomposed in terms of \( |n_x\rangle \otimes |m_y\rangle \), the direct products of the two bases of number states. This Hamiltonian admits the readily constructible direct product of coherent states as the ground state \( |g_I\rangle \):

\[
|g_I\rangle = |\theta_x\rangle \otimes |\theta_y\rangle, \quad \text{shortened as} \quad |\theta_x, \theta_y\rangle,
\]

(10)

with \( |\theta\rangle \) the canonical quantum coherent state

\[
|\theta\rangle = e^{-|\theta|^2} \sum_{n=0}^{\infty} \frac{\theta^n}{\sqrt{n!}} |n\rangle,
\]

where:

\[
a |\theta\rangle = \theta |\theta\rangle.
\]

The target Hamiltonian \( H_P \)

Building on (1), we introduce the target Hamiltonian \( H_P \),

\[
H_P = N^2 (N - \hat{n}_x \hat{n}_y)^2 + \hat{n}_x (\hat{n}_x - \hat{n}_y)^2,
\]

(11)

which has a unique ground state, i.e. no degeneracy. This ground state would give us the solution for the desirable optimisation problem (1) over the integer domain, thus solving the factorisation for the integer \( N \).

Our proposed AQC may be physically realised by quantum optics or other means, with some suitably chosen end time \( T \). Then the solution factors for \( N \) would be obtained from the final state \( |\psi(T)\rangle \) by its measurements in the number state basis. Even though such measurements only yield probabilities, any factor candidates so obtained could be verified straightforwardly and efficiently by a multiplication of \( n_x \) and \( n_y \), or by a division of \( N \) by \( n_x \) or by \( n_y \).

After the release of a draft of this present work, the algorithm presented herein has been physically implemented with qubits on D-Wave Systems [?].
Numerical simulations

For the purpose of illustration, we simulate the AQC algorithm for $N = 6$ by numerically solving the Schrödinger equation (6) in a suitably truncated Hilbert space of dimensions $23 \times 23$, with linear extrapolation in (5) and parameters $\theta_0 = \theta_1 = \sqrt{N}$ (so that $\langle \theta_0, \theta_1 | \theta_0, \theta_1 \rangle = N$).

Figure 2 depicts the spectral flow of $\mathcal{H}(t)$ with linear extrapolation in (5) for $N = 6$. The two lowest branches respectively correspond at $t = T$ to $|2_2, 3_y\rangle$ and $|3_2, 2_y\rangle$, both of which are non-trivial factor pairs.

Figure 3 shows the probabilities $|\langle \psi(T) | n_x, m_y \rangle|^2$ versus $T$ in the simulated AQC for the factorisation of $N = 6$ with a suitably truncated Hilbert space of dimensions $23 \times 23$. Only the two largest probabilities are shown.

For the purpose of illustration, we simulate the AQC algorithm for $N = 6$ by numerically solving the Schrödinger equation (6) in a suitably truncated Hilbert space of dimensions $23 \times 23$, with linear extrapolation in (5) and parameters $\theta_0 = \theta_1 = \sqrt{N}$ (so that $\langle \theta_0, \theta_1 | \theta_0, \theta_1 \rangle = N$).

Figure 2 depicts the spectral flow of $\mathcal{H}(t)$ with linear extrapolation in (5) for $N = 6$. The two lowest branches respectively correspond at $t = T$ to $|2_2, 3_y\rangle$ and $|3_2, 2_y\rangle$, both of which are non-trivial factor pairs.

Figure 3 shows the probabilities $|\langle \psi(T) | n_x, m_y \rangle|^2$ versus $T$ for the two largest probabilities. In all instances of $T$ there, the number state $|2_2, 3_y\rangle$ has the maximum probability among all the number states. This probability increases with $T$, the inverse of the evolution rate, in agreement with the quantum adiabatic theorem [7]. The next highest probability corresponds to the other solution $|3_2, 2_y\rangle$.

We note that the increased probability for $|3_2, 2_y\rangle$ at $T = 100$ compared to that at $T = 30$ is an artifact of our truncation of the Hilbert space. With a truncation at $|n_{\text{max}}\rangle$ such that $a^\dagger|n_{\text{max}}\rangle = 0$, the commutation relation (7) is violated.
\[ \langle n_{\text{max}} | a^d | n_{\text{max}} \rangle = 0, \]
\[ \langle n_{\text{max}} | a^a + 1 | n_{\text{max}} \rangle = n_{\text{max}} + 1. \]

The effect of such a truncation artifact becomes more prominent for larger \( T \), unless we increase \( n_{\text{max}} \) accordingly.

**Computational complexity**

We have presented elsewhere [8] a necessary condition for a lower time limit required in a general AQC for an initial state to evolve into an orthogonal state under the dynamics of \( \mathcal{H} \). Namely, it is necessary that the evolution time cannot be less than \( T_\perp \),

\[ T_\perp \sim \mathcal{O}\left( \frac{1}{\Delta \epsilon E_p} \int_0^1 g(\tau) d\tau \right), \]

where \( \Delta \epsilon E_p \) is the energy spread of the initial state \( |g_i\rangle \) in terms of the target Hamiltonian \( H_p \),

\[ \Delta \epsilon E_p \equiv \sqrt{\langle g_i | H_p^2 | g_i \rangle - \langle g_i | H_p | g_i \rangle^2}. \]

(13)

It is important to note that only the initial eigenstate \( |g_i\rangle \) (which is of course time-independent), and neither the instantaneous eigenstates nor the full time-dependent wave function at any other times, is required for the time condition (13). This hallmark of our results in [8] enables their wider applicability and usefulness.

We note that \( T_\perp \) is particularly a function of the parameters \( \{|\theta|\} \),

\[ T_\perp = T_\perp (|\theta|). \]

(15)

The parameters \( \theta \)'s give our proposed AQC algorithm some advantage that is denied or not evident elsewhere, and this could be exploited in order to reduce the lower time limit \( T_\perp \) for the computation to be \( \mathcal{O}(1) \) or even less! But this reduction would at the same time incur an appropriate increase in the energy cost

\[ E_{\text{cost}} = \max_{0 \leq \tau \leq T} |\langle g_i | \mathcal{H}(\tau) | g_i \rangle|_{g_i}. \]

For instance, for \( \theta \sim \mathcal{O}(1) \) the cost \( E_{\text{cost}} \) would be, as evident from (11), of order \( \mathcal{O}(N^4) \)—that is, exponentially in the number of bits in the binary representation of \( N \).

It is not that surprising that we could reduce the computation time with more energy resources. Other examples of this delicate balance between the energy required and the lower time limit for a well-known quantum algorithm are given elsewhere [8, 9].

**Another Diophantine polynomial**

We could also employ another Diophantine polynomial \( R_N(x, y) \), in addition to \( Q_N(x, y) \) of (1), to construct \( H_p \) in the search to find a pair of factors for \( N \),

\[ \min_{x, y \in \mathbb{N}} \{ R_N(x, y) \equiv N^2(N - xy)^2 + x(x - y) + x \}. \]

(16)

The proof that the optimisation of \( R_N(x, y) \) could yield a non-trivial pair of factors is similar to that for (1).

For \( xy \neq N \) then obviously \( (N - xy)^2 \geq 1 \) and the first term of (16) is consequently not less than \( N^2 \),

\[ R_N(x, y)|_{xy \neq N} \geq N^2. \]

(17)

For \( xy = N \) the first term on the rhs of (16) vanishes and the remaining terms, for \( x \leq \sqrt{N} \leq y \),

\[ R_N(x, y)|_{xy = N} = R_N(x, 1/x) = \left( x - \frac{N}{x} \right)^2 + x \]

(18)

form a convex function (i.e. having non-negative second derivative) for \( x \in [1, \sqrt{N}] \). It then follows that such a function is bounded by its maximum value obtained at one of the end points

\[ R_N(x, y)|_{xy = N} = R_N(x, 1/x) \leq \max \{ R_N(x, 1/x)|_{x = 1}, R_N(x, 1/x)|_{x = \sqrt{N}} \}, \]

\[ \leq \max \{ (1 - N)^2 + 1, \sqrt{N} \}, \]

\[ \leq (1 - N)^2 + 1, \]

\[ \leq N^2, \]

\[ \leq R_N(x, y)|_{xy = N}. \]

(19)

A pair of factors of \( N \) so obtained is not only unique but also non-trivial, because from (19) it follows that \( x > 1 \) when \( N \) is not prime. Only when \( N \) is prime then we would have \( x = 1 \).
Concluding remarks

We have mapped the factorisation problem into the optimisation over the integer domain of some corresponding Diophantine polynomials. The optimal solutions are unique, and contain the unity factor if and only if the integers to be factored are prime. Based on this, we then propose an algorithm in the context of Adiabatic Quantum Computation for the general factorisation. We also indicate that the lower bound on the running time could be reduced at the expense of more energy input in order to carry out the physical computation. Some numerical simulations of the algorithm for a simple case are also presented for illustration purpose.

After the release of a draft of this present work, the algorithm presented herein has been physically implemented with qubits on D-Wave Systems [2].

We are grateful for discussions with Peter Hannaford, Adolfo del Campo and Richard Warren, who also brought the work [3] to our attention after the completion of this paper. The publication fee for this work is covered by Swinburne University.

ORCID iDs

Tien D Kieu @ https://orcid.org/0000-0002-1551-6128

References

[1] Rivest R L, Shamir A and Adleman L 1978 Commun. ACM 21 120
[2] Shor P W 1994 Algorithms for quantum computation: Discrete logarithms and factoring, Proceedings of the 35th Annual Symposium on Foundations of Computer Science (Los Alamitos, CA: IEEE Computer Society Press)
[3] Jiang S, Britt K A, McCaskey A J, Humble T S and Kais S 2018 Quantum annealing for prime factorization arXiv:1804.02733 [quant-ph]
[4] De Loera J A, Hemmecke R, Köppe M and Weismantel R 2006 Math. Oper. Res. 31 147
[5] Farhi E, Goldstone J, Gutmann S, Lapan J, Lundgren A and Preda D 2001 Science 292 472
[6] Farhi E, Goldstone J and Gutmann S 2000 A numerical study of the performance of a quantum adiabatic evolution algorithm for satisfiability arXiv:quant-ph/0007071
[7] Messiah A 1966 Quantum Mechanics (New York, Dover Publications)
[8] Kieu T D 2017 A new class of time-energy uncertainty relations for time-dependent hamiltonians arXiv:1702.00603 [quant-ph]
[9] Kieu T D 2018 The travelling salesman problem and adiabatic quantum computation: an algorithm Quantum Inf Process arXiv:1801.07859 [quant-ph] (https://doi.org/10.1007/s11128-019-2206-9)