A quantum algorithm for solving systems of nonlinear algebraic equations

Peng Qian · Weicong Huang · Guilu Long

Received:

Abstract We propose a quantum algorithm to solve systems of nonlinear algebraic equations. In the ideal case the complexity of the algorithm is linear in the number of variables $n$, which means our algorithm’s complexity is less than $O(n^3)$ of the corresponding classical ones when the set of equations has many variables and not so high orders. Different with most popular way of representing the results by state vector, we get the results in computation basis which is readable directly.

Keywords nonlinear algebraic equations · quantum algorithm · dual quantum computing · quantum searching

1 Introduction

As one of the most important technology in the future of human beings, quantum computation has attracted more and more attention for its way to perform computation by harnessing quantum mechanics that classical computations
can not. It is well known that in some problems quantum algorithm supply a remarkable speedup over their classical counterpart, for example, Shor’s factoring algorithm[1], Grover’s searching algorithm[2,3], simulating various quantum systems[4,5,6], HHL’s algorithm for linear equations system[7] and so on.

In recent years, a number of researches concentrate on simulating Hamiltonian or solving linear system problems by quantum algorithm[8,9,10]. Notice that these algorithms solving linear systems tend to represent results by the state vector evolved by quantum computer instead of computation basis used in early times. On one hand this way saves amounts of computing resource for saving lots of qubits. On the other hand it is hard to extract and read out numerical information. More than that, it’s hard to realize nonlinear functions acted on these state vector since unitary operators transform the probability amplitudes linearly. Therefore for nonlinear problems, we still do not get appropriate algorithms yet.

In fact Shor in his famous and great algorithm used computation basis to represent results to solve the nonlinear problem — order finding[1]. We learn that in this way it is easy to realize nonlinear function operation and extract results by just measuring computation basis and reading out digital numbers. Based on these, we develop a new methods to solve systems of nonlinear algebra equations. In essence it searches the whole space of computation basis to find approximation solutions to equations. However thanks to superposition principle it finds solution much faster than ever. It’s kind of similar with Grover’s algorithm while our method finds out multi-variables that satisfy multiple conditions.

Actually, our method is an application of duality quantum computation paradigm proposed first by Long[11,12] which realizes the non-unitary operator by combining several unitary gates through a number of ancilla qubits. The main idea comes from Double-slit interference. It imagines the state in quantum computation is a wave function in real space, passing through the multi-slits each of which corresponds to one unitary operator acting on the wave function, then intervening at some point behind multi-slits. Many algorithms can be realized through this paradigm, especially for non-unitary operator that can be decomposed into sum of unitary ones[13,14,15]. We use this paradigm to make solution found quickly and enhance the probability amplitude of the corresponding computation basis in total state vector. We also use some oracles based on the equations to be solved. In general, basic arithmetic operations have been realized in computation basis[16]. We treat them as feasible and reliable. What we concern is complexity of them and how they influence the total speed of the algorithm.

The rest of article is organized as follows: we first give the details of our algorithm. Then we analyze the complexity of our algorithm and compare it with the classical ones. In the end we will discuss possible extension of our algorithm and potential problems in practice before conclusion.
2 Main algorithm

Assume we want to solve a group of algebraic equations:

\[ \{ f_i(x_0, x_1, \ldots, x_{n-1}) = 0 \}, \quad i = 0, 1, 2, \ldots, n - 1 \]  

First, we prepare \( n \) registers to represent every variable \( x_i, i = 0, 1, \ldots, n - 1 \), that is, for initial state we set it as:

\[ |\psi_0\rangle = \begin{cases} N_0 \ldots N_0 & \text{if } N < m \\ N_0^{-m} \ldots N_0^{-m} & \text{if } N > m \end{cases} \]  

Here, we make this set according to what accuracy we need and the range for finding the solutions. If range is \((0, 2^m)\), then every register represents an integer if \( N < m \) and a rational number if \( N > m \) and latter \( N - m \) digits represent decimal.

We apply Hadamard matrix \( H^{\otimes Nn} \) to transform initial state to:

\[ |\psi_1\rangle = H^{\otimes Nn} |\psi_0\rangle = \left( \sqrt{\frac{1}{2^n}} \right)^n \sum_{x_0 \cdots x_{n-1}=0}^{2^{N-1}} |x_0\rangle \cdots |x_{n-1}\rangle \]  

We now add an ancilla register to make preparation for computation of oracle in the later computation:

\[ |\psi_1\rangle \rightarrow \left( \sqrt{\frac{1}{2^n}} \right)^n \left( \sqrt{\frac{1}{N_0}} \right) \sum_{x_0 \cdots x_{n-1}=0}^{2^{N-1}} |x_0\rangle \cdots |x_{n-1}\rangle \sum_{a=0}^{N_0-1} e^{i2\pi a/N_0} |a\rangle \]  

This register can be prepared by applying a quantum Fourier transformation on a log \( N_0 \) qubits state \( |0\cdots 0\rangle \) which is easy to see.

For some oracle, we apply it on one state to get:

\[ U_f |\Phi\rangle \rightarrow \sqrt{\frac{T}{x}} \sum_{x} |x\rangle \sqrt{\frac{T}{N_0}} \sum_{a=0}^{N_0-1} e^{i2\pi a/N_0} |a \oplus f(x)\rangle \]  

and redefine \( a \) and get a extra common phase which reads:

\[ \sqrt{\frac{T}{x}} \sum_{x} |x\rangle e^{i2\pi f(x)/N_0} \sqrt{\frac{T}{N_0}} \sum_{a=0}^{N_0-1} e^{i2\pi a/N_0} |a\rangle \]  

The procedure described above is so-called "phase kickback" [17], in which \( N_0 \) is chosen to be fit with our computation.

Now we put this aside for a moment and apply \( U_{f_i} \) into the initial state for \( i = 0, \ldots, n - 1 \). Before doing that we first insert two zero registers into
the state for storage of the computation results. Besides we add some control qubits for further application of oracles. Here, we take $N_0 = 2$:

$$|\psi_1\rangle \rightarrow \left(\frac{1}{\sqrt{2^N}}\right)^n \left(\frac{1}{\sqrt{2}}\right)^{n+1} \sum_{0}^{2^N-1} |x_0\rangle \cdots |x_{n-1}\rangle |0\rangle |0\rangle \sum_{a=0}^{1} e^{i\pi a} |a\rangle \sum_{\eta_0=0}^{1} |\eta_0\rangle \cdots \sum_{\eta_{n-1}=0}^{1} |\eta_{n-1}\rangle$$

and then apply the unitary operator:

$$\prod_{i=0}^{n-1} \{U^{-1}_{f_i} U^{-1}_{f_i} \left(\sum_{j_i=0}^{1} M_{j_i} |j_i\rangle \langle j_i|\right) U_{f_i} U_{f_i}\},$$

where each $i$ corresponds a equation. For distinction we will write "1" as imaginary unit and "i" as index number.

Here, we take $U_{f_i}$ which makes computation of corresponding equation function $f_i$ and put the result into the first zero register, which reads $U_{f_i} |x\rangle |y\rangle \cdots |0\rangle = |x\rangle |y\rangle \cdots |f_i(x,y,\cdots)\rangle$. We take a oracle $f_i$ we name with "check oracle" which counts whether the first few $\lambda$ digits of results are zero on range of solution and power of equation. If it is, the second zero register will not change. If not, the second zero register becomes $|1\rangle$. $M_{j_i}$ adds this result to ancilla register $\sum_{a=0}^{1} e^{i\pi a} |a\rangle$, changing it to $\sum_{a=0}^{1} e^{i\pi a} (|a \oplus j_i \cdot f_i\rangle)$. Then we use $U_{f_i}$ and $U_{f_i}^{-1}$ to restore the zero register.

We use "phase kickback" and give the detailed process:

$$\sum_{j_i=0}^{1} M_{j_i} |j_i\rangle \langle j_i| \rightarrow$$

$$\sum_{a=0}^{1} e^{i\pi a} |a \oplus 0 \cdot f_0\rangle |0\rangle + \sum_{a=0}^{1} e^{i\pi a} |a \oplus 1 \cdot f_0\rangle |1\rangle \sum_{\eta_1=0}^{1} |\eta_1\rangle \cdots$$

$$\rightarrow$$

$$\cdots$$

$$\rightarrow \sum_{a=0}^{1} e^{i\pi a} |a \oplus 1 \cdot f_0\rangle (|0\rangle + e^{i\pi f_0} |1\rangle) \sum_{\eta_1=0}^{1} |\eta_1\rangle \cdots$$

$$\cdots$$

$$\rightarrow \sum_{a=0}^{1} e^{i\pi a} |a \oplus 1 \cdot f_0\rangle (|0\rangle + e^{i\pi f_0} |1\rangle) \cdots (|0\rangle + e^{i\pi f_{n-1}} |1\rangle)$$
We again apply a Hadamard operator $H^\otimes n$ on ancilla qubits $|j_0\rangle \cdots |j_{n-1}\rangle$. For those qubits satisfy $\bar{f}_0 \cdots \bar{f}_{n-1} = 0$, it looks like this:

$$
\sum_{0}^{2N-1} |x_0^*\rangle \cdots |x_{n-1}^*\rangle |0\rangle |0\rangle \sum_{a=0}^{1} e^{i\pi a} |a\rangle |0\rangle.
$$

(10)

While qubits presenting other variable values will get an zero amplitude in this ancilla $|0\rangle$ for orthogonality. This can be seen easily that $(|0\rangle + |1\rangle) \cdots (|0\rangle + |1\rangle)$ (solutions’ ancilla qubits) is orthogonal to others like $(|0\rangle + |1\rangle) \cdots (|0\rangle - |1\rangle) \cdots$ and Hadamard rotation will not change this orthogonality so that qubits presenting other variable values will in ancilla qubits other than $|0\rangle$.

Actually, process above is a dual quantum computation in which we realize a complicated linear combination of unitary operators that cancel the undesired state and get the state we want.

Now we have to get into $|0\rangle$ in register so that only solution states are left behind. This can be done with amplitude amplification or measurement (repeating until success). Obviously the best way is amplitude amplification.

We repeat acting $U_0 = I - 2I \otimes |0\rangle \langle 0|$ and $U_1 = I - 2|\Psi\rangle \langle \Psi|$ where $|\Psi\rangle$ is the state we get in last step until we have a relatively large chance to measure $|0\rangle$ in ancilla qubits. If we first require the equations to be zero in first few $\lambda$ qubits then we loop these operations about $\sqrt{2^N}$ and measure the ancilla qubits to make sure it is in $|0\rangle$.

However, we only get to approximation solution. We will then use gradient descent to find accuracy solutions. For simplicity we ignore all the normalized factors and add $l-(N-m)$ zero qubits to every variable register if our accuracy requirement is $2^{-l}$.

$$
|0\cdots 0\rangle \sum_{l-(N-m)}^{N} e^{i\pi a/N'} |a\rangle.
$$

(11)
We add every register $|x^*_i\rangle$ to corresponding $|y_i\rangle$, which is a complete set of corresponding accuracy, and rewrite variable register $|x^*_i\rangle \otimes \cdots \otimes |0\rangle$ as $|x^*_i\rangle$.

We apply $U_F$ to get:

$$\sum_{y_0} |y_0 + x^*_0\rangle \cdots \sum_{y_{n-1}} |y_{n-1} + x^*_{n-1}\rangle \sum_{N'} e^{i\pi a/N'} |a\rangle,$$

(12)

where $F = \sum_i f_i^2$, $N'$ is a parameter suited with accuracy\cite{17}. We use "phase kickback" and do the quantum fourier transformation to get

$$\frac{2^{m+l}}{s} \frac{\partial F}{\partial x_0} x^*_0 \cdots \frac{2^{m+l}}{s} \frac{\partial F}{\partial x_{n-1}} x^*_{n-1},$$

(13)

where $s$ stands a range we set in oracle $U_F$ to bound derivatives of $F$. We multiply this by a small negative constant $\alpha$ and add it to register $|x^*_0\rangle \cdots |x^*_{n-1}\rangle$ to get new value $|x^*_{0}^*\rangle \cdots |x^*_{n-1}^*\rangle$.

$$|x^*_{0} + \alpha \frac{\partial F}{\partial x_0} x^*_0 \cdots |x^*_{n-1} + \frac{\partial F}{\partial x_{n-1}} x^*_{n-1}\rangle$$

(14)

We repeat the same procedure as above again and again until convergence. This is analogous to classical gradient descent. At last we just need measure register and read out the results.

3 One simple example

Here, we take a simple example to see how our method works. We take a ternary nonlinear systems of equations:

$$\begin{cases}
x^3 + y^2 - y + 2z = 35 \\
y^3 - x + 2xz = 50 \\
z^3 - z^2 + 2x - 2y = 20
\end{cases}$$

(15)

In real range $\{0,2^3\}$ with four decimal accuracy we have one solution $\{2.7689, 3.2834, 3.1370\}$. In our method, we first set accuracy to inter part which means we take $\lambda = 3$ just need the inter part bits of equation to be zero. That is to say we take $\mathcal{F}$ to check the inter part of results of function oracle are whether all equal to zero. We set $N = 6$, $m = 3$. Then we take three equation function oracle to act on, for example, the state $|010.110\rangle|011.010\rangle|011.001\rangle|0\rangle|0\rangle((0) - (1))((0) + (1))\otimes^3$(in decimal system $2.75, 3.25, 3.125$), an approximation solution). We found the qubit is unchanged after action. Here, we drop the normalization constant for simplicity. Then after Hadamard gate acted on last three ancilla qubits to get $|010.110\rangle|011.010\rangle|011.001\rangle|0\rangle|0\rangle((0) - (1))|0\rangle$. While for the other
A quantum algorithm for solving systems of nonlinear algebraic equations

state, for example, $|011.010\rangle|010.010\rangle|011.100\rangle|0\rangle|0\rangle((0) - |1\rangle)(|0\rangle + |1\rangle)\otimes^3$(in decimal system {3.25, 2.25, 3.125})

$|011.010\rangle|010.010\rangle|011.000\rangle|0\rangle|0\rangle((0) - |1\rangle)(|0\rangle + |1\rangle)\otimes^3\quad(16)$

$U_f^+\rightarrow|011.010\rangle|010.010\rangle|011.100\rangle|0\rangle|0\rangle((0) - |1\rangle)(|0\rangle + |1\rangle)\otimes^3$ (17)

$M_0|1\rangle(1 + M_0)|0\rangle$

$|011.010\rangle|010.010\rangle|011.100\rangle|0\rangle|0\rangle((0) - |1\rangle)(|0\rangle + |1\rangle)\otimes^2$

Therefore the second zero register becomes $|1\rangle$. $M_0$ add this result to ancilla $|(0) - |1\rangle\rangle$, changing it to $- (|0\rangle - |1\rangle)$ while $M_0$ is equivalent to $I$:

$\rightarrow|011.010\rangle|010.010\rangle|011.000\rangle|0\rangle|0\rangle((0) - |1\rangle)(|0\rangle + |1\rangle)\otimes^2$

$+|011.010\rangle|010.010\rangle|011.100\rangle|0\rangle|0\rangle((0) - |1\rangle)(|0\rangle + |1\rangle)\otimes^2$

$\rightarrow|011.010\rangle|010.010\rangle|011.100\rangle|0\rangle|0\rangle((0) - |1\rangle)(|0\rangle - |1\rangle)(|0\rangle + |1\rangle)\otimes^2$ (18)

$U_{f_1}U_{f_1}^{-1}\rightarrow|011.010\rangle|010.010\rangle|011.100\rangle|0\rangle|0\rangle((0) - |1\rangle)(|0\rangle - |1\rangle)(|0\rangle + |1\rangle)\otimes^3$

...$

\rightarrow|011.010\rangle|010.010\rangle|011.100\rangle|0\rangle|0\rangle((0) - |1\rangle)(|0\rangle - |1\rangle)\otimes^3$

After Hadamard gate action, the state becomes $|011.010\rangle|010.010\rangle|011.100\rangle|0\rangle|0\rangle((0) - |1\rangle)|1\rangle).$ Obviously, as we have proposed, all approximation solutions are in subspace $|0\rangle$. If it is not, then it will be in other subspace. From this we find we can quickly find approximation solution after amplitude amplification we describe above. Then we just need to run few iteration of gradient descent to get accurate solution.

4 Complexity of the algorithm

For discussing the complexity of our algorithm, we need to count computing source each oracle costs. For basic arithmetic oracles like multiply we treat its complexity as $O(N^2)$ [10]. Where $N$ is the size of our input. Note the highest order of group of equation is $h$ and the maximum number of terms of equations $t$, then the total number of basic operations we need for one equation oracle is $O(thN^2)$. The operator $\bigotimes^2$ will need $O(nthN^2)$ elementary operations. Of course this analysis depends on how the elementary operation is defined and which oracle for $f_i$ we choose. Here we just estimate the complexity order in ideal cases. After this we use amplitude amplification to get the
approximate value. We need about \( \mathcal{O}(2^{\lambda/2}) \) rotations. Therefore we need total \( \mathcal{O}(2^{\lambda/2}n^{th}N^2) \) operations.

In gradient descent process, oracle \( U_F \) costs \( \mathcal{O}(n^{th}(l + m)^2) \). We may set iteration times as a small number \( c \) since we have got approximation solution.

At last we find that the total number of elementary operations in procedure will be \( \mathcal{O}(2^{\lambda/2}n^{th}N^2 + cn^{th}(l + m)^2) \). \( \lambda \) is close to \( hn \). Therefore complexity is linear in \( n \) but exponential in \( h \). For high order systems of equations we need to lower down approximation in first process to reduce complexity.

Now let’s get a look at number of qubits our algorithm needs. For gradient descent process, we need \( 2n(l + m) \) qubits for registers. The ancilla qubits for oracle to make “phase kick-back” depend on oracle \( U_F \). We note it as \( \log N' \).

For accuracy it needs to be almost equal to \( \mathcal{O}(2h(m + l)) \). The control qubits corresponding to the operator \( [8] \) need about \( \mathcal{O}(n) \) qubits. What’s more, there is a need of \( \mathcal{O}(hN) \) qubits for temporary store for computation results of function oracle of equations \( f_i \). In sum, we need \( \mathcal{O}(4h(m + l) + hN) \) qubits for total store. The number depends heavily on the highest order of equations and accuracy requirement. Therefore for large order equations we may not obtain solution because computation result of function oracle is out of our computation source. However this situation is not so common for it means relatively large solution.

What about classical ones? The most common numerical method to solve these equations is Newton’s iterative method which requires to solve the inverse matrix of Jacobian matrix for derivatives of each function with respect to each variable. This will cost about \( \mathcal{O}(n^3) \) operators for \( n \) variables. For further consideration, we still need to count complexity for each operator consisting of elementary arithmetic computation as for our quantum one. Then one will cost \( \mathcal{O}(ht(l + m)^2) \) computations. In total it will have a complexity of \( \mathcal{O}(htn^3(l + m)^2) \) at one iteration. Considering that it will iterate many times until it converges to some point and this depends on choice of initial values sensitively, we think our algorithm will have a better performance when we have many number of variables.

In general our algorithm is similar to Grover’s searching algorithm[2]. While in his algorithm it searches one solution to one condition. We think we extend to multi-variable problems. Notice that when the highest order is 1, equations reduce to linear equations which have been researched frequently in recent year. In this case our algorithm will have a complexity of \( \mathcal{O}(ntN^2) \) better than classical ones, although it is not so well as HHL’s[7].

| equation type | non linear | linear |
|---------------|------------|--------|
| quantum       | \( \sqrt{2}mnN^2 + m(l + m)^2 \) | \( mN^2 \) |
| classical     | \( n'th(l + m)^2 \) | \( n'N^2 \) |
| HHL           | /          | \( \log(n)N^2 \) |
We show a suitable way to solve nonlinear equations. However we know that there are many possible solution for one group of nonlinear equations and we may also meet the situation that we don’t get the solution at all. In the former case, we have to repeat computation and measurement to get full solution. While in the latter case we may need to change the range for our initial register. That may cost more sources and we will hope that future’s quantum computer may give us a enough powerful computation source.

5 Conclusion

In this paper we give a new algorithm to solve systems of nonlinear algebraic equations. Since we get a complexity linear in number of variable in systems of equations, we think our algorithm is better than classical ones. We can also change storage for results to adjust accuracy for results if we need as classical ones. Moreover, Based on computation basis we can read solution directly. One can also treat our algorithms as a multi-conditions and multi-variables search method. But for practice use we require future quantum computers to have enough qubits to store data in our algorithm. And for high order functions we’re going to improve our algorithm and the related research is undertaken.

Acknowledgements This work was supported by the National Basic Research Program of China under Grant Nos. 2017YFA0303700 and 2015CB921001, National Natural Science Foundation of China under Grant Nos. 61726801, 11474168 and 11474181.

References

1. P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Review, 41:1484–1509, 1997.
2. K. L. Grover. A fast quantum mechanical algorithm for data base search. Proceedings of the 28th Annual ACM Symposium on the Theory of Computing, pages 212–219, 1996.
3. G. L. Long. Grover algorithm with zero theoretical failure rate. Physical Review A, 64:022307, 2001.
4. S Lloyd. Universal quantum simulators. Science, 273(5278):1073–1078, 1996.
5. R Gerritsma, G Kirchmair, F Zähringer, E Solano, R Blatt, and C. F. Roos. Quantum simulation of the dirac equation. Nature, 463(7277):68–71, 2010.
6. S. P. Jordan, K. S. Lee, and J Preskill. Quantum algorithms for quantum field theories. Science, 336(6085):1130, 2011.
7. A. W. Harrow, A Hassidim, and S Lloyd. Quantum algorithm for linear systems of equations. Physical Review Letters, 103(15):150502, 2009.
8. S Lloyd, M Mohseni, and P Rebentrost. Quantum principal component analysis. Nature Physics, 10(9):108–113 vol. 1, 2014.
9. D. W. Berry, A. M. Childs, R Cleve, R Kothari, and R D. Somma. Exponential improvement in precision for simulating sparse hamiltonians. In Forty-Sixth ACM Symposium on Theory of Computing, pages 283–292, 2014.
10. D. W. Berry, A. M. Childs, A Ostrander, and G. M. Wang. Quantum algorithm for linear differential equations with exponentially improved dependence on precision. Communications in Mathematical Physics, 356(3):1057–1081, 2017.
11. G. L. Long. The general quantum interference principle and the duality computer. Communications in Theoretical Physics, 45(5):825–844, 2006.
12. G. L. Long. Duality quantum computing and duality quantum information processing. *International Journal of Theoretical Physics*, 50:1305–1318, 2011.

13. S. J. Wei, D Ruan, and G. L. Long. Duality quantum algorithm efficiently simulates open quantum systems. *Scientific Reports*, 6:30727, 2016.

14. S. J. Wei, Z. R. Zhou, D Ruan, and G. L. Long. Realization of the algorithm for system of linear equations in duality quantum computing. In *IEEE Vehicular Technology Conference: Vtc2017-Spring*, pages 1–4, 2017.

15. S. J. Wei, T Wang, D Ruan, and G. L. Long. Quantum computing. In *Scientia Sinica Informationis*, pages 1277–1299, 2017.

16. V Vedral, A Barenco, and A Ekert. Quantum networks for elementary arithmetic operations. *Physical Review A*, 54(1):147, 1996.

17. S. P. Jordan. Fast quantum algorithm for numerical gradient estimation. *Physical Review Letters*, 95(5):050501, 2005.

18. G Brassard, P Hoyer, M Mosca, and A Tapp. Quantum amplitude amplification and estimation. [arXiv:quant-ph/0005055](https://arxiv.org/abs/quant-ph/0005055) 2000.