Note on Non-Unitary Quantum Gates in Quantum Computing

Aleksander Zujev
Physics Department, University of California, Davis, California 95616, USA

We study possible advantage of using non-unitary quantum gates in quantum computing. Our particular goal is to investigate the application of non-unitary quantum gates for solving NP-complete problems. In this note, we specifically study an example of non-unitary quantum computing, advanced by Nordin Zakaria.

I. INTRODUCTION

Quantum computing, while very promising, didn't so far quite fulfill its initial expectations. Most spectacular result in quantum computing is Shor's algorithm for integer factoring. But it isn't proven yet that integer factoring in polynomial time is impossible by classical computer.

Grover's algorithm of database search gives square root speed-up. This is very good improvement - the time of search is proportional to the square root of the number of entries in database, down from being proportional to the number of entries in classical search. But the more ambitious goal is time of search polynomial of the length of search string. Such algorithm could work as a universal problem solver, and would be used for many applications. E.g., automatic theorem proving: We can encode any derivation as a sequence of statements, obeying some logical rules; together, this sequence is a string of characters. We search all such strings of length N for a string starting with the set-up statements, and ending with the conclusion statement. If we find such string, then it is our proof. If not, then we'll know that the theorem can't be proved in less or equal to N characters.

There were in the literature various suggestions of extending quantum computing beyond standard for solving NP-complete problem in polynomial time [1–3]. Solving NP-complete problem in polynomial time generally in quantum computing community is considered as probably impossible. But the potential rewards in case of success are very high - in principle, it may mean universal problem solver, easy solving of many difficult problems. The problem is worth investigating even if the perceptive probability of success is low.

Among the more promising directions is using non-unitary gates. Particularly interesting is the work of Zakaria [1], who suggests search algorithm using non-unitary gates. The work uses the proposal by Terashima and Ueda [4] of application of a non-unitary operator as a quantum measurement operator.

The main goal of this project is to study the possibility of practical realization of non-unitary quantum computing and its application for solving NP-complete problems.

II. APPLICATION OF NON-UNITARY GATES IN SEARCH ALGORITHM

A. ZTU Search Algorithm

Zakaria[1] suggested an algorithm for quantum search, using non-unitary quantum gates. The algorithm uses non-unitary gates constructed by quantum measurement as defined by Terashima and Ueda [4]. We'll call it Zakaria-Terashima-Ueda (ZTU) algorithm.

For simplicity, we use N being a power of 2, $N = 2^n$. The heart of the algorithm is the part which differentiates between one qubit states $y = |0\rangle$ and

$$x = \sqrt{1 - \frac{1}{N}}|0\rangle + \frac{1}{\sqrt{N}}|1\rangle. \tag{1}$$

To achieve this, the algorithm uses non-unitary quantum gate

$$D = \begin{pmatrix} 1 & -\sqrt{N-1} \\ 0 & \sqrt{N} \end{pmatrix}, \tag{2}$$

which, applied to the states y and x results respectively in the states $|0\rangle$ and $|1\rangle$.

D is decomposed using Singular Value Decomposition

$$D = QVR^{\dagger}, \tag{3}$$

where Q and $R^\dagger$ are unitary, and V is diagonal non-unitary. For large N

$$V \approx \begin{pmatrix} \sqrt{2N} & 0 \\ 0 & \frac{1}{\sqrt{2}} \end{pmatrix} \tag{4}$$

V is decomposed into a product of matrices V_i, such that their first diagonal element is less than 2. For large n the number of resulting matrices V_i is $m \approx \frac{n+1}{2}$, and

$$V_i \approx \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \tag{5}$$

V_i then is normalized to

$$M_0 \approx \begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{2} \end{pmatrix}, \tag{6}$$

where M_0 now is used as measurement operator.

To successfully apply operator D, we need successfully (i.e. with success) apply measurement M_0 m times.

B. Quantum Measurement in ZTU Algorithm

Does ZTU algorithm indeed work in polynomial time? The reason for the doubt is quantum measurement, which has probability of success less than 1. As a result, while using non-unitary gates gives speed-up for the search, the measurement gives slow-down. Will the resulting time of search be polynomial, or due to measurement slow-down, exponential?

If the probability of success of measurement M_0 is p, then to get successful m measurements requires average number of measurements (see Appendix for derivation) $E(nmeas) = \frac{1}{1-p}\left(\frac{1}{p^m} - 1\right)$, and we need to do the procedure for every bit, n times. If we were doing measurements for every bit for the full N set, the total number of measurements would be $E(nmeas.total) \sim n\left(\frac{1}{p^m}\right)$, but we do binary division, so

$$E(nmeas.total) \approx \sum_{i=1}^{n} \frac{1}{1-p}\left(\frac{1}{p^{mi/n}} - 1\right) \approx \frac{1}{1-p}\frac{1}{p^m}\frac{1}{1-p^{m/n}} \sim \frac{1}{p^m} \tag{7}$$

If the probability of success of measurement M_0 p is approximately between $\left(\frac{1}{2}\right)^2 = \frac{1}{4}$ and $(1)^2 = 1$, then for the worst case $p = \frac{1}{4}$, and

$$E(nmeas.total) \sim (2)^n, \tag{8}$$

which is exponential time. For the best case of $p = 1$, measurement is always successful, and $E(nmeas.total) \sim n$, so the average time for a random search vector $\sim (2)^n$.

Seems different factorization of V doesn't much affect average number of measurements. If we increase m twice, $m' = 2m$, then

$$M_0 \approx \begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{\sqrt{2}} \end{pmatrix}, \tag{9}$$

so p changes: $p' = \sqrt{p}$, and number of measurements

$$E'(nmeas.total) \sim (p')^{-m'} \sim E(nmeas.total) \sim \frac{1}{p^m}, \tag{10}$$

the same as in (7).

C. Discussion

The reason for the lack of success of solving search in polynomial time:

The gain by non-unitary operation (amplitude amplification) is nullified by a loss by reduced probability of success of the operation.

The gain and loss can be both expressed in terms of the coefficients of the non-unitary matrix, and they match each other. Where computation time was exponential, $\sim 2^{an}$, it remains exponential, $\sim 2^{bn}$. There may be an improvement, if $b < a$. This improvement may possibly be considerable, but not as good as changing computation time from exponential to polynomial.

The study of one example is not enough for far reaching conclusions. We need to do systematic study of different algorithms involving non-unitary quantum gates. We may expect that either there are some instances of changing computation time from exponential to polynomial due to the non-unitary gates, or there are none, in which case it needs to be proven. The third possibility is that the problem is undecidable.

Appendix A: Derivation of the number of measurements

The problem is equivalent to the following: We have a biased coin, with probabilities of head and tails respectively $Pr(H) = p$ and $Pr(T) = q = 1 - p$. How many flips, X, are required on average to get m of heads (H) in a row?

We are using derivation by David Mitra[6]. For $1 \leq i \leq m$, let T_i be the event that the first tail occurs on flip i and let T_{m+1} be the event that the first m flips are all heads. We have conditional expectation $E(X|T_i) = i + E(X), \quad 1 \leq i \leq m$, if the first T occurs on flip i, then it's as if we are restarting: the expected number of flips to obtain m H in a row would be i plus the original expected number of flips. $E(X|T_{m+1}) = m$,

$$\begin{aligned} E(X) &= \sum_{i=1}^{m+1} P(T_i)\, E(X|T_i) \\ &= \sum_{i=1}^{m} p^{i-1} q\big(\, i + E(X)\,\big) + p^m m \\ &= \frac{1 - p^m - m p^m q}{q} + (1 - p^m) E(x) + p^m m \end{aligned} \tag{A1}$$

Solving for $E(X)$:

$$E(X) = \frac{1}{q}\left(\frac{1}{p^m} - 1\right) \tag{A2}$$

---

[1] M Nordin Zakaria, Binary Subdivision for Quantum Search, arXiv:1101.4703.

[2] M. Ohya and I. Volovich, A new quantum algorithm for studying NP-complete problems, Reports on Mathematical Physics, Vol. 52, Issue 1 (2003), 25-33.

[3] A. Leporati, S. Felloni, Three "quantum" algorithms to solve 3-SAT, Theoretical Computer Science 372 (2007) 218-241.

[4] Hiroaki Terashima and Masahito Ueda, Nonunitary Quantum Circuit, International Journal of Quantum Information, Vol. 3, No. 4 (2005), 633-647.

[5] Hiroaki Terashima and Masahito Ueda, Hermitian conjugate measurement, PRA 81, 012110 (2010)

[6] David Mitra, http://math.stackexchange.com/questions/95396/expected-number-of-tosses-for-two-coins-to-achieve-the-same-outcome-for-five-con