Copying quantum computer makes NP-complete problems tractable

Mika Hirvensalo

Turku Centre for Computer Science
TUCS Technical Report No 161
February 1998
ISBN 952-12-0158-4
ISSN 1239-1891

Abstract

Under the assumption that a quantum computer can exactly copy quantum superpositions, we show that **NP**-complete problems can be solved probabilistically in polynomial time. We also propose two methods that could potentially allow to avoid the use of a quantum copymachine.

Supported by the Academy of Finland under grant 14047.

To be presented at MCU'98, March 1998, Metz, France.

TUCS Research Group
Theory Group: Mathematical Methods in Computer Science

1 Introduction

It was conjectured by R. Feynman [5] in 1982 that it may be impossible to simulate quantum physical phenomena by an ordinary computer without an exponential slowdown in the efficiency of the simulation. In his work, Feynman also suggested that the slowdown could be avoided by allowing the computer run according to rules of quantum mechanics, thus introducing the idea of *quantum computer*. However, quantum computation remained quite a marginal phenomenon in the theory of computing until 1994, when Peter W. Shor discovered his famous algorithms for factoring integers and finding discrete logarithms in polynomial time by a quantum computer [10]. Both tasks play an essential role in public-key cryptography and are believed to be classically intractable. However, after Shor's results, there has been surprisingly little progress in the field of quantum computation. One remarkable result was given by Bennett & al. in [2], where the authors suggest that **NP**-complete problems cannot be solved by a quantum computer in polynomial time. On the other hand, Berthiaume and Brassard [3] argued that quantum computation may be exponentially more powerful than the classical computation. This apparent discrepancy becomes understandable when we notice that both of these results were relative, i.e. they were obtained using oracle computations. The strongest non-relative result so far is the quadratic speed-up given by Grover [6], which tells us that **NP**-complete problems can be solved by a quantum computer in time $\sqrt{2^n}p(n)$, where $p(n)$ is a polynomial depending on the problem.

2 Quantum computations briefly

In this section we will shortly outline the basic features of quantum computation. No previous knowledge about quantum physics is needed, nor any connections to physics are given here, but the formalism of quantum computation is given in a purely mathematical way.

The main difference between quantum and classical computation is that quantum bits, *qubits* can appear in *superpositions* of classical states. Quantum bits are described by orthonormal basis vectors in two-dimensional complex Hilbert space, say $|0\rangle$ and $|1\rangle$ (so called ket-notation $|\cdot\rangle$ is due to P. Dirac). This Hilbert space is called the *state space* and these two vectors are referred as *basis states* and their unit-length linear combinations as *superpositions* of basis states. A *quantum register* of length n consists of n quantum bits and is depicted by an n-fold tensor product of two-dimensional Hilbert spaces. We use notations

$$|x_1\rangle\otimes|x_2\rangle\otimes\ldots\otimes|x_n\rangle=|x_1\rangle\,|x_2\rangle\ldots|x_n\rangle=|x_1x_2\ldots x_n\rangle. \qquad (1)$$

The state space of a quantum register thus becomes a 2^n-dimensional complex Hilbert space with orthonormal basis states that can be expressed as

(replacing the binary strings with the numbers they represent)

$$|0\rangle, |1\rangle, |2\rangle, \ldots, |2^n - 1\rangle. \tag{2}$$

The unit-length linear combinations of these states are called superpositions as well.

The nature of quantum computation is linear: Quantum registers evolve via unitary mappings (recall that unitarity in finite dimension means that the rows and the columns of the matrix of the mapping both form an orthonormal set). The unitarity implies that quantum computation is reversible, but this is not a restriction: For any Turing Machine there is a reversible Turing Machine that does the same computation that the original one did (see [1] or [8]).

Quantum parallelism is a consequence of the linearity: Assume that there is a unitary mapping U that computes a function $f : \Sigma^n \to \{0, 1\}$ (this means that $U \,|\, j\rangle \,|\, 0\rangle = |\, j\rangle \,|\, f(j)\rangle$). Then

$$\begin{aligned} & U\frac{1}{\sqrt{2^n}}\big(\,|0\rangle\,|0\rangle + |1\rangle\,|0\rangle + \ldots + |2^n-1\rangle\,|0\rangle\big) \\ = \;& \frac{1}{\sqrt{2^n}}\big(\,|0\rangle\,|f(0)\rangle + |1\rangle\,|f(1)\rangle + \ldots + |2^n-1\rangle\,|f(2^n-1)\rangle\big), \end{aligned} \tag{3}$$

Which means that we can compute *exponentially many values* of f with a cost of one single computation. But this is not the whole truth: *Observation* of (3) will give us just one of states $|\, j\rangle \,|\, f(j)\rangle$, where $j \in \{0, 1, \ldots, 2^n - 1\}$, each with probability $\frac{1}{2^n}$. Moreover, the observation procedure shall cause (3) to collapse into state $|\, j\rangle \,|\, f(j)\rangle$ that was observed, *destroying the rest of (3) irreversibly.*

In general, observation of k:th qubit when the register of length n is in state

$$\alpha_0 \,|\, x_0\rangle + \alpha_1 \,|\, x_1\rangle + \ldots + \alpha_{2^n-1} \,|\, x_{2^n-1}\rangle, \tag{4}$$

will yield 1 or 0 with probabilities

$$P(1) = \sum_{j \in J} |\alpha_j|^2, \quad \text{where } J = \{j \mid \text{the } k\text{th qubit of } x_j \text{ is } 1\}, \tag{5}$$

$$P(0) = \sum_{j \in J'} |\alpha_j|^2, \quad \text{where } J' = \{j \mid \text{the } k\text{th qubit of } x_j \text{ is } 0\}. \tag{6}$$

Moreover, the post-observation state will be

$$\frac{1}{\sqrt{\sum_{j \in J} |\alpha_j|^2}} \sum_{j \in J} \alpha_j \,|\, x_j\rangle \quad \text{or} \quad \frac{1}{\sqrt{\sum_{j \in J'} |\alpha_j|^2}} \sum_{j \in J'} \alpha_j \,|\, x_j\rangle, \tag{7}$$

depending on which one of values 1 or 0 was seen.

The reduction of the state during the observation procedure seems to destroy the advantage obtained in superposition (3), namely that all 2^n

values of f were computed simultaneously. So we cannot directly reveal features of f that may interest us: We may ask, for example, is f a constant function? Consider, for instance, superposition (3) with $f(j) = 0$ for all j:

$$\frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} |j\rangle\, |0\rangle \tag{8}$$

and with a function $f(k) = 1$ but $f(j) = 0$ for $j \neq k$:

$$\frac{1}{\sqrt{2^n}} \big(\sum_{j \neq k} |j\rangle\, |0\rangle + |k\rangle\, |1\rangle \big). \tag{9}$$

If we observe the last qubit of superposition (9), the probabilities of seeing 1 is only $\frac{1}{2^n}$, so 1 is too "faint" to be seen. In the next section we introduce an iterative method for "amplifying" this 1. On the other hand, the distance of (8) and (9) in the state space is only $\frac{1}{2^{n-1}}$ and the *unitary mappings always preserve the distance*, so we may believe that it is extremely difficult to find out any rapid amplification procedure based only on the unitary mappings (the procedure introduced in [6] does the amplification in $\sqrt{2^n}$ iterations). Therefore, we will try somehow to utilize the state reductions in the observations.

3 Amplification procedure

In this section we consider problem *"generalized satisfiability"*, GSAT: Let $\Sigma = \{0, 1\}$ be the binary alphabet and f a completely defined *blackbox function* $f : \Sigma^* \to \Sigma$. The concept "blackbox function" here means that the value $f(x)$ is obtained in a single computation step and that the "inner structure" of f is not known - we do not assume that f is a computable function. We shall again denote the restriction of f into Σ^n by f. The problem GSAT is to decide whether, for a "given" blackbox function there is a word $x \in \Sigma^n$ such that $f(x) = 1$.

If we assume that f is a given function computable in polynomial time, the problem above is **NP**-complete, since satisfiability of a propositional expression would clearly become a subcase of GSAT.

Let us first consider how to tell the difference between the cases

1° $f(k) = 1$ but $f(j) = 0$ for all $k \neq j \in \Sigma^n$ and

2° $f(j) = 0$ for all $j \in \Sigma^n$.

If we assume f to be a blackbox function, we suppose that the value $f(j)$ can be "called" instantaneously, when qubits represent the value j. We also assume that f will respect linear nature of quantum physics, that is, a single call of f on superposition

$$\frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} |j\rangle\ |0\rangle \tag{10}$$

will produce

$$\frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} |j\rangle\ |f(j)\rangle. \tag{11}$$

If, on the other hand, we assume that f is computable in polynomial time, then there is a matrix U (see [7] or [13]) that is a product of polynomially many unitary matrices that operate on subspaces of bounded dimension and performs the computation

$$U\ |j\rangle\ |0\rangle = |j\rangle\ |f(j)\rangle. \tag{12}$$

Moreover, U can be efficiently found. Let also

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{13}$$

be the *Hadamard transformation* and

$$D = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 & 0 \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{14}$$

be a matrix that acts on computational basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$, so $|00\rangle$ is mapped into $\frac{1}{\sqrt{2}}\ |00\rangle + \frac{1}{\sqrt{2}}\ |01\rangle$ and $|11\rangle$ is a fixed point.

We will introduce the procedure while studying case 1°. In the beginning we prepare the quantum superposition

$$\frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} |j\rangle\ |00\rangle \tag{15}$$

using Hadamard transformations (see [11]). Function f is then applied on the n-qubit string $|j\rangle$ to obtain

$$\frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} |j\rangle\ |f(j)f(j)\rangle = \frac{1}{\sqrt{2^n}} \Big(\sum_{j\neq k} |j\rangle\ |00\rangle + |k\rangle\ |11\rangle \Big) \tag{16}$$

Applying D on the last two qubits will yield

$$\frac{1}{\sqrt{2^n}}\Big(\sum_{j\neq k}\big(\tfrac{1}{\sqrt{2}}\left|j\right\rangle\left|00\right\rangle+\tfrac{1}{\sqrt{2}}\left|j\right\rangle\left|01\right\rangle\big)+\left|k\right\rangle\left|11\right\rangle\Big) \tag{17}$$

and it is easy to see that, if we observe the last qubit, the probabilities of seeing one and zero are $\frac{2^n+1}{2\cdot 2^n}$ and $\frac{2^n-1}{2\cdot 2^n}$ respectively. *If* the observation yields one, then the post-observation state is

$$\frac{1}{\sqrt{2^n+1}}\Big(\sum_{j\neq k}\left|j\right\rangle\left|01\right\rangle+\sqrt{2}\left|k\right\rangle\left|11\right\rangle\Big), \tag{18}$$

as easily calculated. The procedure continues by adding two extra qubits thus obtaining state (we can as well think that these extra qubits existed in the beginning)

$$\frac{1}{\sqrt{2^n+1}}\Big(\sum_{j\neq k}\left|j\right\rangle\left|01\right\rangle\left|00\right\rangle+\sqrt{2}\left|k\right\rangle\left|11\right\rangle\left|00\right\rangle\Big). \tag{19}$$

Then we compute the function f again, this time saving the result in the new qubits. The resulting state is

$$\frac{1}{\sqrt{2^n+1}}\Big(\sum_{j\neq k}\left|j\right\rangle\left|01\right\rangle\left|00\right\rangle+\sqrt{2}\left|k\right\rangle\left|11\right\rangle\left|11\right\rangle\Big). \tag{20}$$

Applying D on last two qubits will now yield

$$\frac{1}{\sqrt{2^n+1}}\Big(\sum_{j\neq k}(\tfrac{1}{\sqrt{2}}\left|j\right\rangle\left|01\right\rangle\left|00\right\rangle+\tfrac{1}{\sqrt{2}}\left|j\right\rangle\left|01\right\rangle\left|01\right\rangle)+\sqrt{2}\left|k\right\rangle\left|11\right\rangle\left|11\right\rangle\Big). \tag{21}$$

If we now observe the last qubit, the probabilities of seeing one and zero are $\frac{2^n+3}{2(2^n+1)}$ and $\frac{2^n-1}{2(2^n+1)}$ respectively and the resulting state, *if one were observed*, will be

$$\frac{1}{\sqrt{2^n+3}}\Big(\sum_{j\neq k}\left|j\right\rangle\left|01\right\rangle\left|01\right\rangle+2\left|k\right\rangle\left|11\right\rangle\left|11\right\rangle\Big). \tag{22}$$

We continue again adding two extra qubits, applying D and measuring the last qubit. *Supposing that the measurement always yields* 1, we see using induction that the state after $l-1$th iteration is

$$\frac{1}{\sqrt{2^n+2^{l-1}-1}}\Big(\sum_{j\neq k}\left|j\right\rangle\left|01\right\rangle^{l-1}+\sqrt{2^{l-1}}\left|k\right\rangle\left|11\right\rangle^{l-1}\Big), \tag{23}$$

where $\mid a_0a_1\rangle^{l-1}$ means $l-1$ copies of $\mid a_0a_1\rangle$. Again we add two extra qubits, compute f and apply D on the last qubits. It is easy to see that the probabilities of seeing 1 and 0 are then

$$P_l(1) = \frac{2^n + 2^l - 1}{2(2^n + 2^{l-1} - 1)} \quad \text{and} \quad P_l(0) = \frac{2^n - 1}{2(2^n + 2^{l-1} - 1)}. \tag{24}$$

If we succeed to measure 1 at n consecutive iterations, then the probability of seeing 1 at the $n+1$th measurement is given by

$$P_{n+1}(1) = \frac{2^n + 2^{n+1} - 1}{2(2^n + 2^n - 1)} = \frac{3 - 2^{-n}}{4 - 2^{1-n}} \geq \frac{3}{4}. \tag{25}$$

On the other hand, let us look at what happens in case 2°. The state corresponding to (17) will be

$$\begin{aligned} & \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} \left(\tfrac{1}{\sqrt{2}} \mid j\rangle \mid 00\rangle + \tfrac{1}{\sqrt{2}} \mid j\rangle \mid 01\rangle \right) \\ = \; & \frac{1}{\sqrt{2^{n+1}}} \sum_{j=0}^{2^n-1} \left(\mid j\rangle \mid 00\rangle + \mid j\rangle \mid 01\rangle \right) \end{aligned} \tag{26}$$

Here the probabilities of seeing 1 and 0 in the last qubit are both $\frac{1}{2}$, and the post-measurement state, if 1 were observed, will be

$$\frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} \mid j\rangle \mid 01\rangle \tag{27}$$

We see immediately that the procedure described above does not change the probability of seeing 1 in the last qubit - it will be $\frac{1}{2}$ each time.

So, if we could "force" 1 to be observed in the first n iterations, we could differ the cases 1° and 2° by the property that after nth iteration the second case gives 1 with probability $\frac{1}{2}$ but the first one case with probability at least $\frac{3}{4}$. In the next section it will be shown that these cases can be distinguished reliably by constant number of trials. Moreover, we can immediately see that *if there are more than one value k giving $f(k) = 1$, then the probability of seeing 1 after n iterations is at least $\frac{3}{4}$.*

However, this procedure will not work, since we cannot force 1 to be observed every time. In fact, the probability of observing 1 at n consecutive measurements is given by (see equations (24))

$$P_1(1)P_2(1)\ldots P_n(1) = \frac{2 \cdot 2^n - 1}{2^{2n}} = \frac{1}{2^{n-1}} - \frac{1}{2^{2n}}, \tag{28}$$

which is exponentially small (with respect to n). Therefore, we propose three ways how we could try to avoid this problem (the first one being the extension of model, the last two ones remain as future research):

- If we had a quantum copymachine, which could produce a copy of each superposition (23) we could after an unsuccessful measurement (0 was observed) restore (23), copy it, and observe again. This would not lengthen the expected running time essentially (details are left to reader), since the probability of seeing m zeros consecutively is at most $\left(\frac{1}{2}\right)^m$. Unfortunately, exact quantum copymachines do not exist [12], but maybe we could somehow utilize approximate copying [4].

- Maybe a clever quantum error-correction scheme could do the restoration after an unsuccessful measurement *without* an assumption of quantum copymachine.

- In fact, we *can* force 1 to be observed each time: We should first prepare superposition

$$\frac{1}{n}\,|1\rangle\,\Big(\frac{1}{\sqrt{2^n}}\sum_{j=0}^{2^n-1}|j\rangle\,|00\rangle^n\Big)+\sqrt{1-\frac{1}{n^2}}\,|0\rangle\,|0^n\rangle\,|01\rangle^n \tag{29}$$

  that would correspond to (15). Then we would run the protocol described in the previous section, using the qubit added in the front as a control bit: The computing is done only if the control bit is 1, so the latter, heavily-weighted part of (29) will not change during the protocol, but the 1's on suitable places there will ensure that the probability of seeing 1 on each measurement will be at least $1-\frac{1}{n^2}$. Now, the probability of seeing 1 in n consecutive measurements is at least $(1-\frac{1}{n^2})^n \geq 1-\frac{1}{n}$ by Bernoulli's inequality. The great difficulty in this approach is how to "annihilate" the heavily-weighted part of (29) after n iterations.

4 Fair and fake coins

The problem of telling the difference between cases 1° and 2° after n successful iterations is equivalent to the following one: We have a pile of coins, where some coins are fair but some give head with probability at least $\frac{3}{4}$. If we choose arbitrarily a coin, how many tosses we need to tell, with probability $1-\varepsilon$, whether the coin was fair or fake?

Let us assume that the coin that was chosen gives head (1) with probability p and tail (0) with probability $q=1-p$. We examine the random variable X describing m tosses, say

$$X = x_1 + x_2 + \ldots + x_m, \tag{30}$$

where each x_i is 1 with probability p and 0 with probability q. The probability that the experiment gives k heads is given by

$$p_k = P(X=k) = \binom{m}{k} p^k q^{m-k}. \tag{31}$$

Moreover, the expected value and the variance of X are given by

$$E(X) = p_0 \cdot 0 + p_1 \cdot 1 + p_2 \cdot 2 + \ldots + p_m \cdot m = pm \tag{32}$$

and

$$\begin{aligned} \mathrm{Var}(X) &= E(X^2) - E(X)^2 \\ &= p_0 \cdot 0^2 + p_1 \cdot 1^2 + \ldots + p_m \cdot m^2 - (pm)^2 = pqm. \end{aligned} \tag{33}$$

By Chebyshev's Inequality [9] we have

$$P(|X - E(X)| \geq k) \leq \frac{\mathrm{Var}(X)}{k^2}, \tag{34}$$

which yields, for $k = \frac{m}{8}$ (this choise because $\frac{m}{2} + \frac{m}{8} = \frac{5m}{8} = \frac{3m}{4} - \frac{m}{8}$),

$$P(|X - pm| \geq \frac{m}{8}) \leq \frac{64pq}{m} \leq \frac{16}{m}. \tag{35}$$

After m tosses we look at the number of heads. If this number is closer to $\frac{m}{2}$ than to $\frac{3m}{4}$, we decide that the coin was fair, otherwise we conclude that the coin was fake. By (35), our conclusion is false with probability at most $\frac{16}{m}$. Taking $m > \frac{16}{\varepsilon}$ our decision is correct with reliability at least $1 - \varepsilon$.

References

[1] C. H. Bennett: *Logical Reversibility of Computation*, IBM journal of Res. Development 17, p. 525-532, Nov 1973.

[2] C. H. Bennett, Ethan Bernstein, G. Brassard and Umesh V. Vazirani: *Strengths and Weaknesses of Quantum Computation*, Los Alamos Preprint, Dec 1, 1994.

[3] André Berthiaume and Gilles Brassard: *Oracle Quantum Computation*, Proceedings of the Workshop on Physics and Computation - PhysComp'92, October 1992, IEEE Press, pp. 195-199.

[4] V. Bužek and M. Hillery: *Universal optimal cloning of qubits and quantum registers*, to be presented at the First NASA Conference of Quantum Computing and Quantum Communications, 17-20, February 1998, Palm Springs U. S. A.

[5] Richard P. Feynman: *Simulating Physics with Computers*, International Journal of Theoretical Physics, Vol 21, N 6/7, 1982.

[6] Lov K. Grover: *A fast quantum mechanical algorithm for database search*, Proceedings, STOC 1996, Philadelphia PA USA, pp. 212-219.

[7] Mika Hirvensalo: *On Quantum Computation*, Licentiate's Thesis, University of Turku, 1997.

[8] Mika Hirvensalo: *The Reversibility in Quantum Computation Theory*, Proceedings of DLT'97, to appear.

[9] Sheldon M. Ross: *Introduction to probability models*, 4th edition, Academic Press, Inc., USA, 1989.

[10] Peter. W. Shor: *Algorithms for Quantum Computation: Discrete Log and Factoring*, Proceedings of the 35th Annual Symposium on the Foundations of Computer Science, pp. 22-22, 1994.

[11] Daniel. R. Simon: *On The Power of Quantum Computation*, Proceedings of the 35th Annual Symposium on Foundations of Computer Science, pp. 116-123, 1994.

[12] W. K. Wootters and W. H. Zurek, Nature 299, 802 (1982)

[13] Andrew Chi-Chih Yao *Quantum Circuit Complexity*, FOCS (pp. 352-361) 1993.

Turku Centre for Computer Science
Lemminkäisenkatu 14
FIN-20520 Turku
Finland

http://www.tucs.abo.fi

University of Turku
- **Department of Mathematical Sciences**

Åbo Akademi University
- **Department of Computer Science**
- **Institute for Advanced Management Systems Research**

Turku School of Economics and Business Administration
- **Institute of Information Systems Science**