Science Symposium 2011
pp 6: Oral Presentations
http://www.sci.ruh.ac.lk/
ISSN :1391-8796

A numerical study of Shor's algorithm for large integer factorization

Perera MWS[1]. And Yapage N.[2]

Department of Mathematics, Faculty of Science, University of Ruhuna, Sri Lanka
[1]sanjaya_mw@yahoo.com, [2]nihal@maths.ruh.ac.lk.

Reducing a composite number into its prime factors has long been a well-known problem in Mathematics and Computer Science. Particularly, this is very important in present day public key crypto systems because these rely on the difficulty of factoring a large composite integer. The present day computers take enormous amount of time to factorize a large composite number. The lack of an efficient algorithm for this purpose had long been another problem up to 1994. In 1994, Peter Shor, a mathematician working for the AT&T Bell laboratory in USA, designed an algorithm to factorize a large composite number on a so called hypothetical quantum computer.

In the factorization process, we reduce the problem into a period finding problem of a function. A period finding method based on the quantum Fourier transform acts the main role of the quantum part while the continued fraction algorithm acts the main role of the classical part. Thus the algorithm consists of a classical and a quantum part.

In this work, we simulate this algorithm for fairly small integers on a classical computer and discuss the efficiency of the algorithm in terms of time taking for factoring a number. Given a number n, choose a randomly fixed number x which is co-prime to n. The major task in the algorithm is to find the period r of the function $f_n(a) = x^a \bmod n$. That is, given $1 < x < n$, the period of $x \bmod n$ is the smallest value of r, where $r \geq 1$, $x^r \bmod n = 1$; n is the integer to be factorized. As mentioned earlier, quantum Fourier transform and continued fraction algorithm are used to find period r. Here, for instance, the composite number 21 is chosen as n for the purpose of demonstration. Then each integer between 1 and 21 has been selected, as the fixed number x, which is co-prime to 21. The code for the Shor's algorithm is written using the Wolfram Mathematica 5.0 package. It is run on a computer with a 2.0GHz Core2Duo CPU and a 2 GB RAM. Furthermore, we give an example where the Shor's algorithm fails to produce positive results.

Keywords: Prime factorization, Period of a function, Quantum Fourier transform, Continued fraction algorithm, Quantum computer.