Quantum Physics Letters
An International Journal

http://dx.doi.org/10.18576/qpl/080102

A Simple Rank Testing Procedure and Complexity Analysis for the Factorization Algorithm

Dhananjay P. Mehendale and Pramod S. Joag*

Department of Physics, Savitribai Phule University of Pune, Pune,India-411007.

Received: 7 Jan. 2019, Revised: 21 Mar. 2019, Accepted: 23 Mar. 2019
Published online: 1 Apr. 2019

Abstract: The problem of characterizing entanglement status of a multipartite pure quantum state was completely solved through the factorization algorithm in [1]. This factorization algorithm for systematically extracting factors is based on utilizing the following criterion: One has a factorization for the given N-qubit pure quantum state as tensor product of an m-qubit state and an n-qubit state, where $m+n=N$, if and only if the rank of the associated matrix, A, of size $2^m \times 2^n$ is equal to unity. The main computational effort for factoring is thus centered around checking whether or not the rank of the associated matrices that arise during extraction of factors is equal to unity. This paper is about proposing a smart procedure to check this. Due to this smart procedure the maximum number of arithmetical operations one needs to carry out to extract one factor, when it exists, become of the order of the cardinality of $\mathbb{B}$, $|\mathbb{B}| = 2^N$, where $\mathbb{B}$ denotes the corresponding computational basis. Further, for finding full factorization one just needs to repeat the rank testing procedure at most N times as the given $N-$qubit state can have at most N factors, and thus the overall complexity of complete factorization is of the order $N|\mathbb{B}|$. In this paper we carry out our discussion for the $N-$qubit case for the sake of simplicity of presentation. The extension to the N-qudit case is straightforward and the computational complexity remains the same.

Keywords: Multipartite pure quantum states, A simple rank testing procedure, Complexity analysis for factorization

1 Introduction

One of the central issues in quantum information theory is whether a given multiqubit pure quantum state is separable or entangled [2,3,4]. This important problem was completely solved in [1] in terms of the factorization algorithm proposed there. This factorization algorithm consists of a systematic procedure for extracting all possible factors of the given pure quantum state. This algorithm finally expresses the given quantum state as a product of factor states such that these factor states are not further factorisable. As the main result of the present paper we show that in order to completely factorize an arbitrary N-qubit pure quantum state, the number of arithmetical operations required by this algorithm is of the order $N|\mathbb{B}| = N2^N$, where $|\mathbb{B}|$ denotes the cardinality of the corresponding computational basis $\mathbb{B}$. As shown in [1], for the given $N-$qubit pure quantum state to be a product of an $m-$ qubit state and an $n-$qubit state where $m+n=N$, one requires that certain "associated matrix" has rank equal to unity. Here it should be noted that one does not require to find out the exact value of this rank but only whether it is equal to unity or not.

In this paper we carry out our discussion for the N-qubit case instead of an N-qudit case for the sake of simplicity of presentation. The extension to the case of N-qudit pure quantum state is straightforward. For N-qudit case the arithmetical operations required to extract one factor, when it exists, are of the order $|\mathbb{E}| = d^N =$ the cardinality of the corresponding computational basis $\mathbb{E}$, where d denotes the number of single qudit states, $\{|0\rangle, |1\rangle, \cdots, |d-1\rangle\}$. Again there can be at most N factors for an $N-$qudit state. Therefore, in order to completely factorize an arbitrary N-qudit pure quantum state the the number of arithmetical operations required by the algorithm is of the order $N|\mathbb{E}| = Nd^N$.

2 Notation, Definitions, and Some Useful Results

Let $|\psi\rangle$ be an N-qubit pure state :

* Corresponding author e-mail: dhananjay.p.mehendale@gmail.com

$$|\psi\rangle = \sum_{s=1}^{2^N} a_{r_s}|r_s\rangle \tag{1}$$

expressed in terms of the computational basis. Here the basis vectors $|r_s\rangle$ are ordered lexicographically. That is, the corresponding binary sequences are ordered lexicographically: $r_1 = 00\cdots00$, $r_2 = 00\cdots01$, $\ldots$, $r_{2^N} = 11\cdots11$, so that $|r_1\rangle = |00\cdots00\rangle$, $|r_2\rangle = |00\cdots01\rangle$, $\ldots$, $r_{2^N} = |11\cdots11\rangle$. Let m,n be any integers such that $1 \leq m,n < N$ and $m+n = N$. Let the corresponding two sets of computational basis vectors ordered lexicographically be $|i_1\rangle,\ldots,|i_{2^m}\rangle$ (each of length m) and $|j_1\rangle,\ldots,|j_{2^n}\rangle$ (each of length n). Rewrite $|\psi\rangle$ thus :

$$|\psi\rangle = \sum_{u=1}^{2^m}\sum_{v=1}^{2^n} a_{i_u j_v}|i_u\rangle \otimes |j_v\rangle. \tag{2}$$

Here in the symbol $a_{i_u j_v}$, the suffix $i_u j_v$ is the juxtaposition of the binary sequences i_u and j_v in that order. Thus we get a $2^m \times 2^n$ matrix $A = [a_{i_u j_v}]$ which will be called the $2^m \times 2^n$ *matrix associated to* $|\psi\rangle$.

We now quote some results from [1]:

Lemma 1: The state $|\psi\rangle$ given by (1) can be factored as the product, $|\psi_1\rangle \otimes |\psi_2\rangle$, of an $m-$qubit state $|\psi_1\rangle$ and an $n-$qubit state $|\psi_2\rangle$ if and only if the $2^m \times 2^n$ matrix A associated to $|\psi\rangle$ can be expressed as $B^T C$ where B is a 1×2^m matrix, C is a 1×2^n matrix and B^T is the transpose of B.

Lemma 2: An $a \times b$ non-zero matrix A over the field $\mathbb{C}$ of complex numbers can be expressed as $B^T C$ for some $1 \times a$ matrix B and $1 \times b$ matrix C if and only if rank$(A) = 1$. By combining Lemmas 1 and 2 we have

Theorem 1: The state $|\psi\rangle$ given by (1) can be factored as the product, $|\psi_1\rangle \otimes |\psi_2\rangle$, of an $m-$qubit state $|\psi_1\rangle$ and an $n-$qubit state $|\psi_2\rangle$ if and only if the $2^m \times 2^n$ matrix A associated to $|\psi\rangle$ is of rank 1.

For convenience, we make the following two definitions :

Definition 1. Let A be a $p \times q$ matrix over the field $\mathbb{C}$. Two non-zero rows of A, say $[a_1 \cdots a_p]$ and $[b_1 \cdots b_p]$, are said to be **proportional** if their non-zero elements *correspond* i.e. $a_i \neq 0$ if and only if $b_i \neq 0$, $1 \leq i \leq p$ and these elements have *the same* constant ratio i.e. there is a constant $k \neq 0$ such that $a_i/b_i = k$ whenever $a_i \neq 0$, $1 \leq i \leq p$.

Definition 2. The non-zero rows of a matrix A are said to be **mutually proportional** if any two non-zero rows of A are proportional.

Lemma 3: Let A be a $p \times q$ matrix over the field $\mathbb{C}$. Then rank $(A) = 1$ if and only if the non-zero rows of A are mutually proportional.

Proof: Let rank $(A) = 1$. It then follows that any two rows of A are linearly dependent. Hence if $[a_1 \cdots a_p]$ and $[b_1 \cdots b_p]$ are any two non-zero rows of A, then there is a non-zero constant k such that $a_i = kb_i$, $1 \leq i \leq p$. Hence these rows are proportional. Hence the non-zero rows of A are mutually proportional. The converse is clearly valid. Hence the lemma.

With the help of Lemma 3, Theorem 1 above can be restated as follows:

Theorem 1a: The state $|\psi\rangle$, given by (1), can be factored as the product $|\psi_1\rangle \otimes \psi_2\rangle$, of an m-qubit state $|\psi_1\rangle$ and an n-qubit state $\psi_2\rangle$ if and only if the non-zero rows of the $2^m \times 2^n$ matrix A associated to $|\psi\rangle$ are mutually proportional.

Remark 1: It is easy to see that for all the nonzero rows to be mutually proportional it is enough to have any one of the nonzero row to be "proportional"to each of the other nonzero rows. Thus, if there are some p nonzero rows in the matrix then it is enough to check that any one of these p nonzero rows is proportional to each of the remaining $(p-1)$ nonzero rows of that matrix.

Hence with the above notation we can now determine the computational effort required to check whether the given pure quantum state $|\psi\rangle$ can be factored as the product $|\psi_1\rangle \otimes |\psi_2\rangle$.

Lemma 4: If $t_m(N)$ denotes the maximum number of arithmetical operations one needs to carry out, i.e. the number of ratios one needs to evaluate, to determine whether the N-qubit state $|\psi\rangle$ has an m-qubit factor $|\psi_1\rangle$, then $t_m(N) = O(2^N)$.

Proof: The associated matrix, A, in this case contains 2^m rows. Each of these rows contains 2^n elements. Now, suppose all the rows of A are nonzero. By remark 1 above, we may take first row of A and pair it with second, third, $\cdots$ 2^m-th row. Thus, we will have $2^m - 1$ such pairs of nonzero rows. We now proceed to check whether the first row is proportional to the second row and *if so,* then we proceed with checking the next pair for proportionality, *otherwise* we stop; and so on. Now, for testing a pair of rows for proportionality, we need to evaluate 2^n ratios and such pairs of rows are in all $(2^m - 1)$ in number. Thus for testing whether rank$(A) = 1$ we need to carry out *at most* $2^m \times 2^n = 2^N$ arithmetical operations. Hence the lemma.

Remark 2: Note that the order of number $t_m(N)$ is *independent* of m. In fact, $t_m(N) = O(|\mathbb{B}|)$ where $|\mathbb{B}| = 2^N$ is the cardinality of the corresponding computational basis $\mathbb{B}$.

3 Complexity Analysis of the Factorization Algorithm

We now proceed to estimate the complexity of the factorization algorithm proposed in [1], our main aim of this paper. At various steps of the algorithm we try to find out whether the state has an m-qubit factor, $m \geq 1$.

Lemma 4 of section 2 gives an estimate of the number $t_m(N)$ of arithmetical operations required to do this. So repeatedly applying Lemma 4 we obtain the following result:

Theorem 2: If $T(N)$ denotes the maximum number of arithmetical operations one needs to carry out to completely factorize an $N-$qubit pure quantum state, then $T(N) = O(N2^N)$.

Proof: We are given an N-qubit pure state $|\psi\rangle$ in terms of the computational basis as

$$|\psi\rangle = \sum_{s=1}^{2^N} a_{r_s}|r_s\rangle$$

where the basis vectors $|r_s\rangle$ are ordered lexicographically. As first step the algorithm checks whether $|\psi\rangle$ factors as $|\psi_1\rangle \otimes |\psi_2\rangle$ where $|\psi_1\rangle$ is a $1-$qubit state. By Lemma 4, by applying $t_1(N) = O(2^N)$ arithmetical operations we determine whether (I) such a factor $|\psi_1\rangle$ exists or (II) it does not exist. As second step of the algorithm, in case (I), we check whether $|\psi_2\rangle$ has a $1-$qubit factor and in case (II), we check whether $|\psi\rangle$ has a $2-$qubit factor. In either of these cases we again need to carry out $t_1(N) = O(2^N), t_2(N) = O(2^N)$ arithmetical operations. The same estimate holds for each step of the algorithm. Now an $N-$qubit state $|\psi\rangle$ can have at the most N factors. Hence the total number, $T(N)$ say, of arithmetical operations required to completely factorize an $N-$qubit state is $T(N) = Nt_m(N)$. Thus $T(N) = O(N2^N)$. Hence the result follows.

4 Conclusion:

Since in order to determine whether a particular factor exists we just need to know whether or not the rank of the associated matrix is equal to unity (and we do not need to actually evaluate the rank) and further, since for an $N-$qubit state we can have at most N factors, therefore, the complexity of the factorization algorithm is $T(N) = O(N2^N)$. For an $N-$qudit state it remains similar as it just changes to $O(Nd^N)$.

Acknowledgement

One of us (DPM) thanks Dr. M. R. Modak, S. P. College, Pune-411030, India, for useful discussion.

References

[1] D. P. Mehendale, P. S. Joag, *A Simple Algorithm for Complete Factorization of an N-Partite Pure Quantum State*, Quant. Phys. Lett. 6, No. 1, pp 73-77,(2017).

[2] R. F. Werner, *Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model*, Phys.Rev.A 40, 4277 (1989).

[3] G. Alber, T. Beth, M. Horodecki, P. Horodecki, R. Horodecki, M. Rotteler, H. Weinfurter, R. Werner, A. Zeilinger, *An Introduction to Basic Theoretical Concepts and Experiments*, Berlin : Springer (2001).

[4] A. Nielsen, I. Chuang, *Quantum Computation and Quantum Information*, Cambridge : Cambridge university Press (2000).

Dhananjay P. Mehendale served as associate professor in S. P. College, affiliated to Savitribai Phule University of Pune, Pune, India-411007. The subjects of his interest and study are Physics, Mathematics, and Engineering and students of science and engineering have successfully completed their project work under his supervision. He taught various courses in Physics, Electronic Science, and Computer Science departments, and has done research in various areas of these subjects. He worked on various science and engineering projects and one of his projects won award in the national science projects competition organized by Department of Science and Technology. His research interest these days is topics in Quantum Computation and Quantum Information and this paper is an outcome of this new interest.

Pramod S. Joag served as a professor of Physics at Savitribai Phule University of Pune, Pune, India-411007. He is presently with Indian Institute of Science Education and Research, Pune. His research interests include quantum correlations, nonlocality issues and foundations of quantum mechanics. He has proposed geometric measures of entanglement and quantum discord in n-partite quantum states and states of n-partite fermionic systems. He has given separability criteria for n-partite quantum states including mixed states. He has given a combinatorial approach to the quantum correlations in multipartite quantum systems and used it to prove the degree conjecture for the separability of multipartite quantum systems. He has found an algorithm to classically simulate spin s singlet state for an infinite sequence of spins.