Research Article

Unique factorization theorem for pure quantum states

Dhananjay P Mehendale*

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

Abstract

In this paper we establish a unique factorization theorem for pure quantum states expressed in computational basis. We show that there always exists unique factorization for any given N-qubit pure quantum state in terms of the tensor product of non-factorable or ``prime" pure quantum states. This result is based on a simple criterion: Given N-qubit pure quantum state in computational basis can be factorized as the tensor product of an m-qubit pure quantum state and an n-qubit pure quantum state, where (m + n) = N, if and only if the rank of the certain associated matrix is equal to one. This simple criterion leads to a factorization algorithm which when applied to an N-qubit pure quantum state factorizes that state into the tensor product of non-factorable or ``prime" pure quantum states. This paper shows that for any given N-qubit pure quantum state the said factorization always ``exists" and is ``unique". We demonstrated our work here on a computational basis.

PACS Number: 03.67.Mn, 03.65.Ca, 03.65.Ud

Introduction

A well-known unique factorization that plays a crucial role in number theory is the unique factorization of natural numbers in terms of the product of its prime factors [1]. This is the well-known Fundamental Theorem of Arithmetic. There are also other Fundamental Theorems, e.g. the Fundamental Theorem of Calculus, the Fundamental Theorem of Algebra, the Fundamental Theorem of Linear Algebra, etc. These fundamental theorems have far-reaching implications and have played a significant role in shaping the respective branches of mathematics to which they belong. Fundamental theorems are useful tools to solve complex problems.

One more unique factorization is the one that we will develop in this paper. This unique factorization is related to quantum information theory. This is about finding unique factorization of an *N*-qubit pure quantum state in terms of the tensor product of non-factorable or ``prime'' pure quantum states. We

work here on a computational basis. This unique factorization is useful to decide the entanglement status of multi-qubit pure quantum states. One more important application of this unique factorization is in the process of synthesizing a multi-qubit pure quantum state in the laboratory with exponential speedup when the unique factorization obtained for a given multi-qubit pure quantum state has large many factors [2].

Entanglement present in a quantum state is one of the main distinguishing features that separates quantum mechanics from classical mechanics. Schrodinger described it as follows: ``I would not call [entanglement] one but rather the characteristic trait of quantum mechanics, the one that enforces its entire departure from classical lines of thought'' [3]. Entanglement is a resource of great utility in quantum computation and quantum information and its characterization is an important problem [4-7]. Determining whether a given multi-qubit pure quantum state is separable or entangled is one of the important problems in quantum information theory [8-10]

and this problem was successfully tackled using factorization algorithms in [11,12]. Entanglement describes a correlation between different parts of a quantum system that exceeds anything that is possible classically. This leads to many highly counterintuitive phenomena [13-18]. Quantum entanglement is a counterintuitive, strange, and challenging topic of research and many remarkable achievements have been made through its extensive study [19-50].

A factorization algorithm based on checking the rank of certain associated matrices was developed in [11]. The algorithm developed in [11] for factorization of an arbitrary N-qubit pure quantum state into non-factorable or ``prime'' factors was developed using the following Simple Criterion: For a given N-qubit pure quantum state there exist two pure quantum states, namely, an m-qubit pure state made up from first m qubits and an n-qubit pure state made up from next n qubits, where $m + n = N$, as factors of given N-qubit pure quantum state if and only if the rank of the corresponding associated matrix of size $2^m \times 2^n$ obtained from given N-qubit pure quantum state should be of rank equal to one.

Therefore, as per that criterion, it is enough to check whether the value of the rank of a certain associated matrix is equal to one or not in order to check the existence or non-existence of certain factorization.

An alternative factorization algorithm proposed in [12] for factorization of an arbitrary N-qubit pure quantum state into non-factorable or ``prime'' factor states was developed using the Schmidt decomposition technique. It was shown in [12] that a factorization of an N-qubit state in terms the tensor product of an m-qubit state and an n -qubit state, where $N = m + n$, exists when the value of Schmidt rank of certain bipartite state is equal to one, where this bipartite state is constructed from the given N-qubit state by expressing the m-qubit state made up from first m qubits as an m-dimensional vector and the n -qubit state made up from next n qubits as an n-dimensional vector. Thus in [12] the given N-qubit state is needed to be expressed as a bipartite state, with the first part an m dimensional vector and the second part an n dimensional vector, and the Schmidt decomposition of the thus formed bipartite state is then needed to be carried out and the corresponding Schmidt rank is then needed to be determined and the desired factorization will exist if and only if the value of the Schmidt rank will be equal to one.

The aim of the present paper is to prove that the said ``factorization'' in terms of non-factorable or ``prime'' factors always ``exists'' and is ``unique'', and can be obtained using the factorization algorithm developed in [11](or [12]). To establish the unique factorization we follow here the criterion and the factorization algorithm developed in [11] due to its simplicity.

Factorization algorithm

Let us now state in brief the criterion given in [11] for the existence of factorization and the steps of the factorization algorithm that follows from it for the sake of completeness.

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

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

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: $r_1 = 00\cdots00$, $r_2 = 00\cdots01$, $\cdots$, $r_{2^N} = 11\cdots11$, so that $|r_1\rangle = |00\cdots00\rangle$, $|r_2\rangle = |00\cdots01\rangle$, $\cdots$, $r_{2^N} = |11\cdots11\rangle$.

Let m, n be any integers such that $1 \le m, n < N$ 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 :

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

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* $|\psi\rangle$.

Criterion ([11]): The state $|\psi\rangle$ given by (1) can be factored as the tensor 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 with $|\psi\rangle$ is of rank 1.

A brief description of Factorization Algorithm:

Step 1: The factorization algorithm checks whether the given pure state $|\psi\rangle$ given by (1) can be factored as the tensor product, $|\psi_1\rangle \otimes |\psi_2\rangle$, of a 1-qubit state $|\psi_1\rangle$ and an $(N - 1)$-qubit state $|\psi_2\rangle$ by checking whether the $2^1 \times 2^{(N-1)}$ matrix A associated to $|\psi\rangle$ is of rank 1 and when the given state $|\psi\rangle$ has a linear (1-qubit) factor on the left and an $(N - 1)$-qubit factor on the right as per the above criterion.

Step 2: If yes, then one goes back to step 1, this time with $|\psi\rangle = |\psi_2\rangle$.

Step 3: If no, then one proceeds to check whether the given pure state $|\psi\rangle$ given by (1) can be factored as the tensor product, $|\psi_1\rangle \otimes |\psi_2\rangle$, of a 2-qubit factor on the left and an $(N - 2)$-qubit factor on the right by checking whether the $2^2 \times 2^{(N-2)}$ matrix A associated to $|\psi\rangle$ is of rank 1 and when so the given state $|\psi\rangle$ has a quadratic (2-qubit) factor on the left and an $(N - 2)$-qubit factor on the right as per the above criterion.

Step 4: If yes, then one goes back to step 1, this time with $|\psi\rangle = |\psi_2\rangle$.

Step 5: If no, then one proceeds to check whether the given pure state $|\psi\rangle$ given by (1) can be factored as the tensor product, $|\psi_1\rangle \otimes |\psi_2\rangle$, of a 3-qubit factor on the left and an $(N - 3)$-qubit factor on the right by checking whether the $2^3 \times 2^{(N-3)}$ matrix A

associated to $|\psi\rangle$ is of rank 1 and when so the given state $|\psi\rangle$ has a cubic (3-qubit) factor on the left and an (N – 3)-qubit factor on the right as per the above criterion, and so on.

Thus, as above the algorithm continues until the factorization of $|\psi\rangle$ is completely done.

We now proceed to settle the main aim of this paper, namely to show that such complete factorization of $|\psi\rangle$ ``exists'' and it is ``unique''.

Existence and uniqueness of the factorization

We now proceed to discuss the main result of this paper. We will show here that the factorization for every N-qubit normalized pure quantum state expressed in computational basis ``exists'' and is ``unique'', in terms of the tensor product of non-factorable or ``prime'' pure quantum states.

Let $|\psi\rangle$ be an N-qubit normalized pure quantum state expressed in the computational basis.

Definition 3.1: An N-qubit pure quantum state expressed in the computational basis, $|\psi\rangle$, is called a non-factorable or ``prime'' state if there do not exist any integers m, n satisfying $1 \leq m, n < N$ and $m + n = N$ such that m, n satisfy the criterion given in section II above, namely, the associated matrix of size $2^m \times 2^n$ obtained from $|\psi\rangle$ has rank equal to one.

Theorem 3.1 (Unique Factorization Theorem): There exists factorization for every N-qubit pure quantum state, $|\psi\rangle (\||\psi\rangle\| = 1)$, expressed in computational basis in terms of the tensor product of non-factorable (prime) pure quantum states and this factorization is unique (up to normalization).

Proof: We first establish the existence of the factorization. It is to be seen that every N-qubit pure quantum state is either (i) a non-factorable or ``prime'' state or (ii) it can be expressed as a tensor product of some non-factorable or ``prime'' pure states containing less than N-qubits such that the sum of the number of qubits present in each of these non-factorable or ``prime'' pure states will be equal to N.

We proceed by induction on N, the number of qubits. For $N = 1$ we have a 1-qubit pure quantum state and it is clearly a non-factorable or ``prime'' pure state, therefore the result holds for $N = 1$.

We assume by strong induction that the claim is true for all pure quantum states containing less than N qubits.

Now, let $|\psi\rangle$ be an N-qubit pure quantum state expressed in the computational basis. If $|\psi\rangle$ is a non-factorable or ``prime'' state then there is nothing more to prove. Otherwise, there will exist some m, n where $1 \leq m, n < N$ and $m + n = N$, such that

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \tag{3}$$

where $|\psi_1\rangle$ is an m-qubit pure state made up from first m qubits and $|\psi_2\rangle$ is an n-qubit pure state made up from next n qubits.

Now, we will have a factorization by induction hypothesis, for the m-qubit state, $|\psi_1\rangle$ and the n-qubit state, $|\psi_2\rangle$, in terms of the tensor product of non-factorable or ``prime'' states $|\theta_i\rangle$ and $|\phi_i\rangle$ respectively as given below:

$$|\psi_1\rangle = |\theta_1\rangle \otimes |\theta_2\rangle \otimes \cdots \otimes |\theta_p\rangle \tag{4}$$

and

$$|\psi_2\rangle = |\phi_1\rangle \otimes |\phi_2\rangle \otimes \cdots \otimes |\phi_q\rangle \tag{5}$$

Therefore, we have got the desired factorization of the pure quantum state, $|\psi\rangle$, under consideration in terms of the tensor product of non-factorable or ``prime'' pure quantum states, namely,

$$|\psi\rangle = |\theta_1\rangle \otimes |\theta_2\rangle \otimes \cdots \otimes |\theta_p\rangle \otimes |\phi_1\rangle \otimes |\phi_2\rangle \otimes \cdots \otimes |\phi_q\rangle \tag{6}$$

We now proceed to establish the uniqueness of such a factorization:

We proceed by induction on N, the number of qubits. For $N = 1$ we have 1-qubit pure quantum state and it is clearly a non-factorable or ``prime'' pure state, and so has unique factorization. Therefore the result holds for $N = 1$.

We assume by strong induction that the claim is true for all pure quantum states containing less than N qubits.

Now, let $|\psi\rangle$ be an N-qubit pure quantum state expressed in the computational basis. If $|\psi\rangle$ is a non-factorable or ``prime'' state then there is nothing more to prove. Otherwise, we apply the factorization algorithm described above step-by-step and determine the ``smallest'' m and corresponding $n = N - m$ such that these m, n satisfy the criterion given in section II above, i.e. for these m, n the associated matrix of size $2^m \times 2^n$ obtained from $|\psi\rangle$ has rank equal to one, and therefore, the state $|\psi\rangle$ can be factored as the tensor product, $|\psi_1\rangle \otimes |\psi_2\rangle$, where $|\psi_1\rangle$ is an m-qubit state and $|\psi_2\rangle$ an n-qubit state.

Now, it is easy to check that the m-qubit state $|\psi_1\rangle$ is a non-factorable or ``prime'' pure state. Because suppose not, then there will exist r, s satisfying $1 \leq r, s < m$ and $r + s = m$ such that r, s satisfy the criterion given in section II above, i.e. the associated matrix of size $2^r \times 2^s$ obtained from $|\psi_1\rangle$ has rank equal to one, and therefore we will have $|\psi_1\rangle = |\mu\rangle \otimes |\nu\rangle$ where $|\mu\rangle$ is an r-qubit state and $|\nu\rangle$ an s-qubit state. Now, let $|\phi\rangle = |\nu\rangle \otimes |\psi_2\rangle$. Therefore, $|\psi\rangle = |\mu\rangle \otimes |\phi\rangle$ where $|\mu\rangle$ is an r-qubit state, $r < m$, and $|\phi\rangle$ is an $p = (s + n)$-qubit state, $p > n$ such that we now have $r + p = N$, i.e. for these r, p there exists the associated matrix of size $2^r \times 2^p$ obtained from $|\psi\rangle$ having rank equal to one, and this is contrary to the supposition made above that m is the ``smallest'' integer such that this $m$ and the corresponding $n = N - m$ satisfy the criterion given in section II above. Thus, $|\psi_1\rangle$ is indeed a non-factorable or ``prime'' pure state as desired. Therefore, $|\psi\rangle$ can be factored as the tensor product, $|\psi_1\rangle \otimes |\psi_2\rangle$, where $|\psi_1\rangle$ is an m-qubit non-factorable or ``prime'' state and $|\psi_2\rangle$ an n-qubit state.

Now, as seen above $|\psi_2\rangle$ an n-qubit state where $n < N$. Therefore, by the induction hypothesis, we can express this

state ``uniquely'' as a tensor product of non-factorable or ``prime'' pure states, $|\chi_j\rangle$ say, such that $j \in \{1,2,\cdots,k\}$, as given below:

$$|\psi_2\rangle = |\chi_1\rangle \otimes |\chi_2\rangle \otimes \cdots \otimes |\chi_k\rangle \qquad (7)$$

Therefore, we will have ``unique'' factorization for the given $N$-qubit state $|\psi\rangle$ as given below in terms of the tensor product of non-factorable or ``prime'' pure quantum states as given below:

$$|\psi\rangle = |\psi_1\rangle \otimes |\chi_1\rangle \otimes |\chi_2\rangle \otimes \cdots \otimes |\chi_k\rangle \qquad (8)$$

Hence the result.

Conclusion

This paper has established a unique factorization theorem for pure quantum states. This theorem assures that there always exists unique factorization for any given N-qubit pure quantum state in terms of the tensor product of non-factorable or ``prime'' pure quantum states. One can determine the entanglement status of any given N-qubit pure quantum state by carrying out the unique factorization in terms of the tensor product of non-factorable or ``prime'' pure quantum states as assured by this unique factorization theorem. An N-qubit pure quantum state is separable when it can be expressed as a tensor product of N number of 1-qubit pure quantum states. Therefore, by applying the above-mentioned unique factorization theorem if the given N-qubit state becomes a tensor product of N number of 1-qubit states then and only then it will be a separable state, otherwise, it will be an entangled state having at least one (or more) entangled factor(s).

Acknowledgements

References

1. Niven H. Zuckerman H. Montgomery. An introduction to the theory of numbers, John Wiley and Sons, Pvt. Ltd. 1991.

2. Mehendale D. Separable quantum states are easier to synthesize, Quant. Phys. Lett. 2017; 6: 2; 111-116.

3. Schrodinger E. Die gegenwartige Situation in der Quantenmechanik, Naturwissenschaften. 1935; 23, 807, 823, 844.

4. Peres A. Phys. Rev. Lett. 1997;76: 1413.

5. Horodecki M, Horodecki P, Horodecki R. Phys. Rev. Lett. 1997;78: 574.

6. Horodecki P. Phys.Lett. A. 1997; 232-233.

7. Horodecki R, Horodecki P, Horodecki M, Horodecki K. arXiv:quant-ph/0702225v2. 2007.

8. Werner R. Phys.Rev.A. 1989; 40: 4277.

9. Alber G, Beth T, Horodecki M, Horodecki P, Horodecki R, Rotteler M, Weinfurter H, Werner R, Zeilinger A. Quantum information, an introduction to basic theoretical concepts and experiments. Berlin: Springer. 2001.

10. Bouwmeester D, Ekert A, Zeilinger A. The physics of quantum information. Berlin: Springer. 2000.

11. Mehendale D, Joag P. A simple algorithm for complete factorization of an N-partite pure quantum state. Quant. Phys. Lett. 2017;6: 73-77.

12. Mehendale D. A new simple algorithm to determine the entanglement status of multipartite pure quantum states. Bulg. J. Phys. 2019;46: 174-188.

13. Einstein A, Podolsky B, Rosen N. Can quantum mechanical description of physical reality be considered complete? Phys. Rev. 1935; 47: 777.

14. Bell JH. On the Einstein-Podolsky-Rosen paradox, Physics. 1964; 1:195.

15. Bell JH. Speakable and unspeakable in quantum mechanics. Cambridge University Press. 1987.

16. Bertlmann RA, Zeilinger A. Quantum [un]speakables, from Bell to quantum information, Springer. Berlin Heidelberg New York. 2002.

17. Bennett C, Brassard G, Crepeau C, Jozsa R, Peres A, Wootters W. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. Phys. Rev. Lett. 1993; 70.

18. Hensen B. Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres. Nature. 2015; 526 (7575): 682-686. arXiv: 1508.05949.

19. Werner RF. Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model. Phys. Rev. A. 1989; 40:4277-4281.

20. Ekert AK. Quantum cryptography based on Bell's theorem. Phys. Rev. Lett. 1991; 67: 661-663.

21. Mattle K, Weinfurter H, Kwiat PG, Zeilinger A. Dense coding in experimental quantum communication. Phys Rev Lett. 1996; 76: 4656-4659.

22. Kempe J. Quantum Decoherence. Springer, Berlin. 2007.

23. Steane A. Quantum computing. Reports on Progress in Physics. 1998;61: 117-173.

24. Ekert A, Jozsa R. Quantum computation and Shor's factoring algorithm. Reviews of Modern Physics. 1996;68: 733-753.

25. Grover LK. Quantum mechanics helps in searching for a needle in a haystack. Phys Rev Lett. 1997; 79: 325-328.

26. Schrodinger E. Die gegenw¨artige Situation in der Quantenmechanik, Naturwissenschaften. 1935; 23: 807-812.

27. Einstein A, Podolsky B, Rosen N. Can quantum-mechanical description of physical reality be considered complete? Phys. Rev. 1935; 47: 777-780.

28. Bell J. On the Einstein-Podolsky-Rosen paradox. Physics. 1964; 1: 195-200.

29. Beig S, Shor PW. Approximating the set of separable states using the positive partial transpose test. Journal of Mathematical Physics. 2010; 51: 042202-042213.

30. Choi J, Kiem YH, Kye SH. Entangled edge states of corank one with positive partial transposes. Journal of Mathematical Physics. 2020; 61: 062202-062216.

31. Zhang CJ, Zhang YS, Zhang S, Guo GC. Entanglement detection beyond the computable cross-norm or realignment criterion, Phys. Rev. A. 2008; 77: 060301-060305.

32. Guo Y, Hou JC. Realignment operation and CCNR criterion of separability for states in infinite-dimensional quantum systems. Reports on Mathematical Physics. 2013; 72: 25-40.

33. Horodecki M, Horodecki P, Horodecki R. Separability of Mixed Quantum States: Linear Contractions and Permutation Criteria. Open Syst. Inf. Dyn. 2006; 13: 103-111.

34. Wocjan P, Horodecki M. Characterization of Combinatorially Independent Permutation Separability Criteria. Open Syst. Inf. Dyn. 2005;12: 331-345.

35. Clarisse L, Wocjan P. On independent permutation separability criteria. Quantum Inf. Comput. 2006; 6: 277-288.

36. Li M, Wang Z, Wang J, Shen S, Fei S. Improved lower bounds of concurrence and convex roof extended negativity based on Bloch representations, Quantum Inf. Process. 2020; 19: 1-11.

37. Hofmann H, Takeuchi S. Violation of local uncertainty relations as a signature of entanglement. Phys. Rev. A. 2003; 68: 032103-032109.

38. Guhne O, Mechler M, Toth G, Adam P. Entanglement criteria based on local uncertainty relations are strictly stronger than the computable cross norm criterion. Phys. Rev. A. 2006; 74: 010301-010305.

39. Zhao Y, Xiang G, Hu X, Liu B, Li C, Guo G, Schwonnek R, Wolf R. Entanglement Detection by Violations of Noisy Uncertainty Relations: A Proof of Principle. Phys. Rev. Lett. 2019; 122: 220401-220407.

40. Zhang C, Nha H, Zhang Y , Guo G. Entanglement detection via tighter local uncertainty relations, Phys. Rev. A. 2010; 81:012324-012329.

41. Gittsovich O, Giihne O, Hyllus P, Eisert J. Covariance matrix criterion for separability. AIP Conference Proceedings. 2009; 1110: 63-66.

42. Zhang C, Zhang Y, Zhang S, Guo G. Optimal entanglement witness based on local orthogonal observables. Phys. Rew. A. 2007; 76: 012334-012340.

43. Ha K, Kye S. Optimality for indecomposable entanglement witnesses. Phys. Rew. A. 2012; 86: 034301-034305.

44. Rutkowski A, Horodecki R. Tensor product extension of entanglement witnesses and their connection with measurement-device-independent entanglement witnesses. Phys. Lett. A. 2014; 378: 2043-2047.

45. Shen S, Xu T, Fei S, Li M. Optimization of ultrafine entanglement witnesses. Phys. Rew. A . 2018; 97: 032343-032347.

46. Werner R, Wolf M. Bell inequalities and entanglement. Quantum Information Computation. 2001; 1: 1-25.

47. Zhang C, Zhang Y, Guo G. Genuine entanglement of generalized Bell diagonal states, Phys. Lett. A. 2007; 363: 57-56.

48. Li M, Fei SM, Li-Jost X, Bell inequality, separability and entanglement distillation, Chinese Science Bulletin. 2011; 56:945-954.

49. Lee H,Oh S, Ahn D . The entanglement criterion of multiqubits, arXiv:quant-ph. 2005; 0506127-0506135.

50. Alheverio, Fei SSM, Goswami D. Separability of rank two quantum states, Phys. Lett. A. 2001; 286:91-96.