Defining and Measuring Multipartite Entanglement

Yishai Shimoni, Daniel Shapira, and Ofer Biham

Racah Institute of Physics, The Hebrew University of Jerusalem

Quantum entanglement between many qubits plays a crucial role in quantum algorithms. The structure of this entanglement cannot be fully described by bipartite entanglement measures. It is thus important to develop ways to characterize and evaluate such entanglement. Here, we consider an operational measure of multipartite entanglement and demonstrate its relevance to quantum algorithms.

The Groverian measure of entanglement

Consider a quantum algorithm A which is designed to operate on an initial state $|i\rangle$, and result in a final state $|f\rangle$. The operation of such an algorithm can be described as

$$A|i\rangle = |f\rangle.$$

In general, the algorithm is applied to any initial state $|n\rangle$. In order to define an entanglement monotone, we introduce a set of local unitary operators, which are applied to the initial state $|n\rangle$ before applying the algorithm. The aim of these local unitary operators is to maximize the probability of success of the algorithm.

Applying these operators to the initial state is equivalent to applying these operators (to the left) on the original initial state of the algorithm $|i\rangle$ (see box on the right).

We assume without loss of generality that any algorithm is designed so that $|i\rangle$ is a tensor product state. This leads to the realization that the unitary operators simply change $|i\rangle$ to another tensor product state, and so we get that the maximal probability of success is

$$P_{max} = \max |\langle t|n\rangle|^2,$$

where the maximization is over all tensor product states $|t\rangle$. The Groverian entanglement measure is defined as

$$G(|n\rangle) = (1-P_{max})^{1/2}$$

which is easily proved to be an entanglement measure.

Requirements for entanglement measures:

1. Invariant under local unitary operations
2. Cannot increase under local operations.
3. Vanishes for non-entangled states.

Success probability of a quantum algorithm:

If algorithm A has an initial state $|i\rangle$ and a final state $|f\rangle$, then the operation of the algorithm can be described as
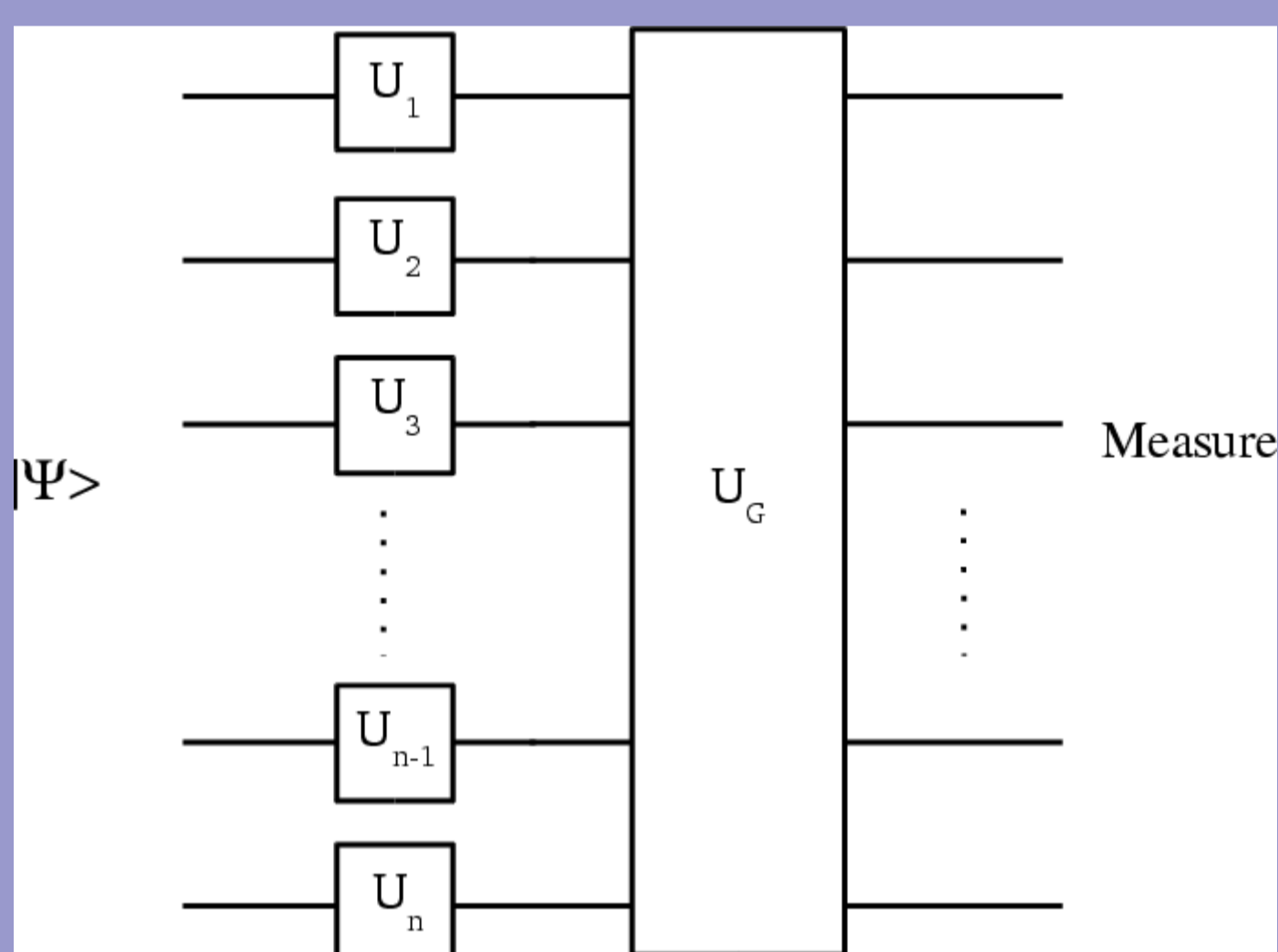
$$A|i\rangle = |f\rangle.$$

If the algorithm is applied to a different initial state $|n\rangle$, then the probability of obtaining the correct result is

$$\Pr(|n\rangle)=|\langle f|A|n\rangle|^2,$$

If $|f\rangle$ is a computational basis state, then this in turn translates to

$$\Pr(|n\rangle)=|\langle i|n\rangle|^2.$$

The quantum circuit that exemplifies the operational meaning of the Groverian entanglement measure for a pure quantum state.
The state is entered into the circuit, then a set of local unitary operators are applied to it in order to maximize the probability of success of the quantum algorithm which follows.

O. Biham, M. Nielsen, and T.J. Osborne, Phys. Rev. A 65, 062312 (2002)
O. Biham, D. Shapira, and Y. Shimoni, Phys. Rev. A 68, 022326 (2003)

Measuring entanglement in quantum algorithms

Here we use the Groverian measure, to evaluate the entanglement of the quantum states obtained during the simulation of quantum algorithms. This is of interest since it is believed that entanglement plays an important role in the speedup obtained by quantum algorithms over their classical counterparts.

Grover's search algorithm:

Grover's search algorithm is an iterative algorithm, which finds a marked state in an unsorted list, in time which is a square root of the time it takes classically.

This figure shows the evolution of the Groverian entanglement measure as a function of the number of iterations, for different number of quantum bits in the quantum register (6 to 12). It can be seen that during the operation of the algorithm entanglement is created, and then removed. It returns to zero exactly at the time when the measurement is performed. Also, it is seen that the maximal amount of entanglement does not depend on the number of bits used in the algorithm.
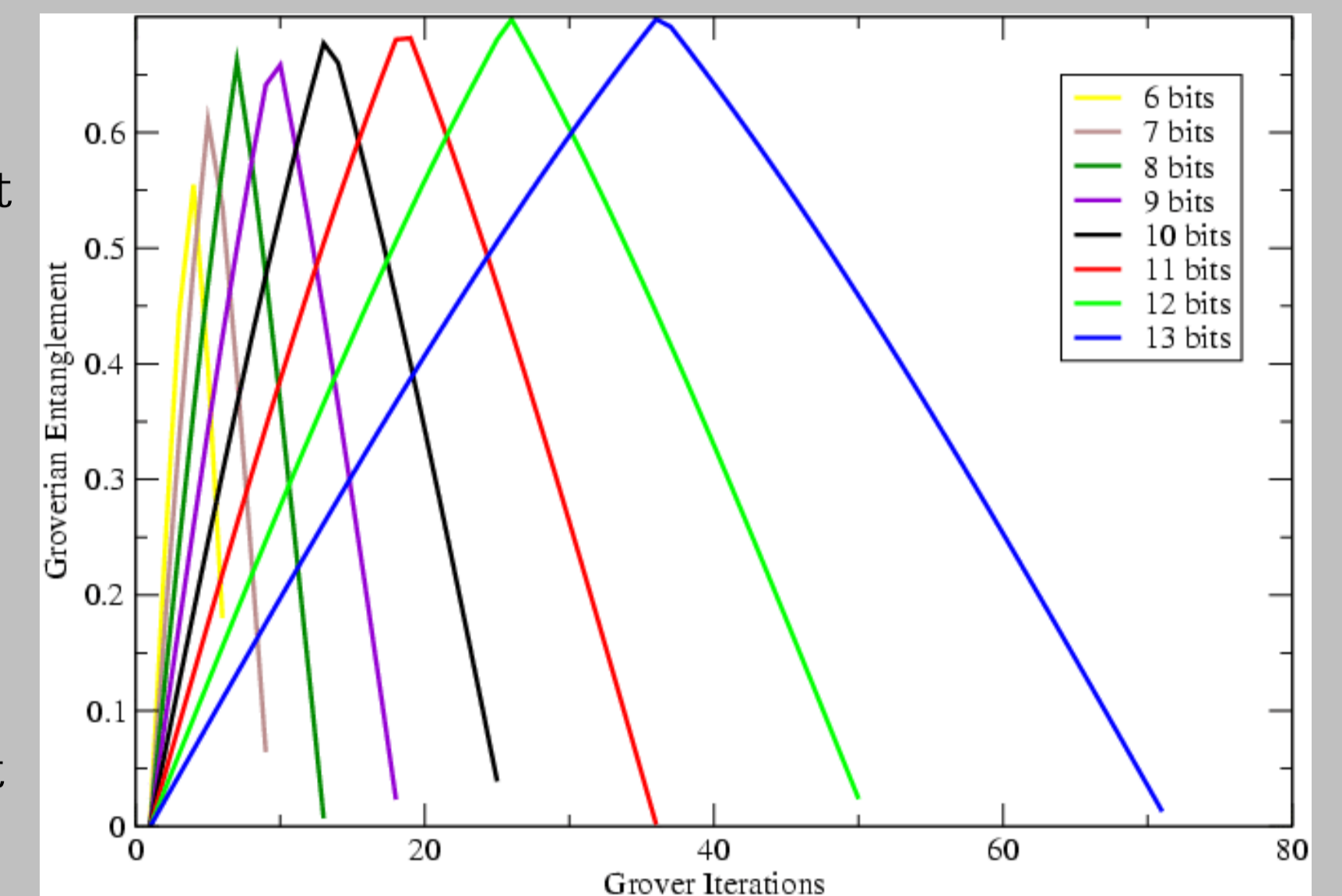

Shor's factorization algorithm:

Shor's algorithm finds the prime factors of any integer, in time which is polynomial in the number of bits needed to store the integer. The best known classical algorithm for this task is exponentially slower.

The algorithm is comprised of 3 parts. The first is the preprocessing stage, where a classical algorithm is performed using quantum parallelism The second part is a discrete Fourier transform, and the third is measurement and classical processing. Checking the development of entanglement during the Fourier transform, almost no change in the entanglement is seen.

The Figure on the right shows the entanglement created during the preprocessing stage of the algorithm, as a function of the integer which is being factorized. Since the preprocessing stage involves guessing another integer, every integer N has several different dots in the Figure. An exponential fit, which is an upper bound of the dots in the Figure, is also shown. This indicates that indeed the entanglement created during Shor's algorithm approaches 1 exponentially.
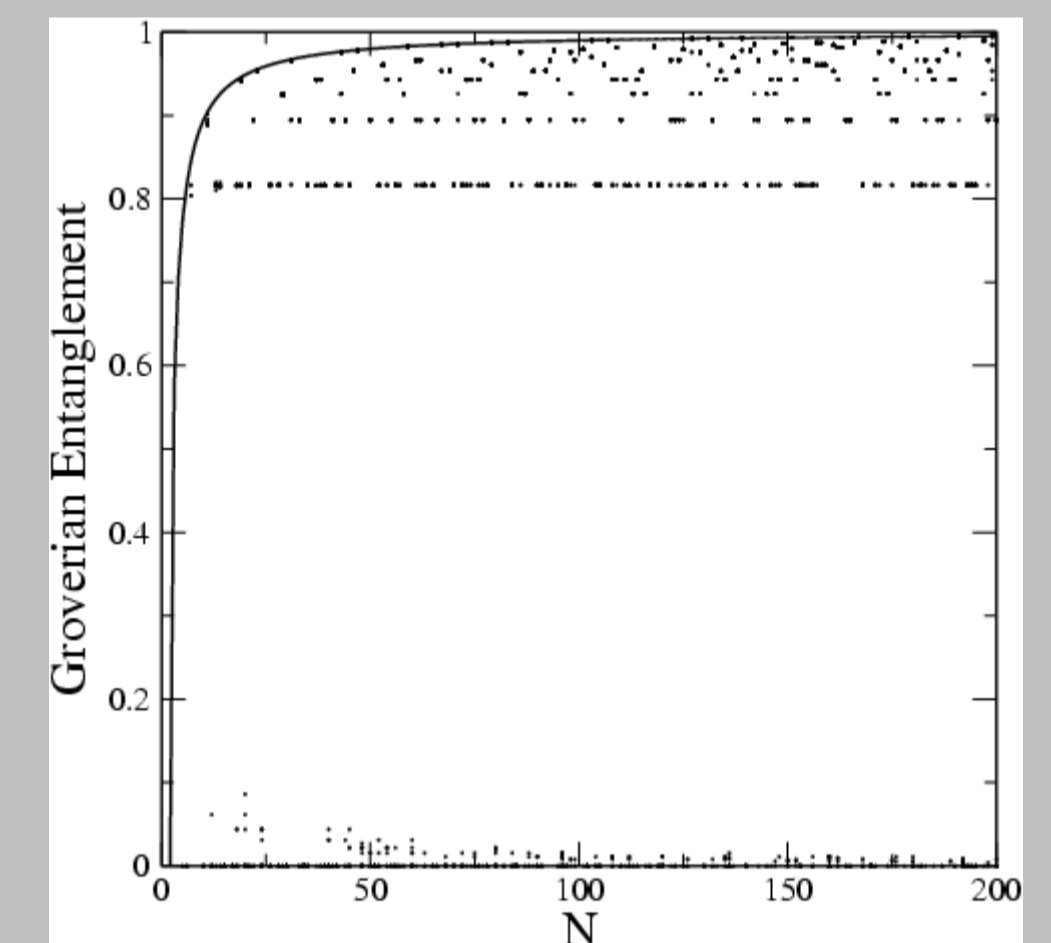
Y. Shimoni, D. Shapira, and O. Biham, Phys. Rev. A 69, 062303 (2004)
Y. Shimoni, D. Shapira, and O. Biham, Phys. Rev. A 72, 062308 (2005)

Measuring multipartite entanglement

It is tempting to relate to the Groverian entanglement measure as defined above as a property of the quantum state, without the need to define any partitioning. However, the truth is that the Groverian measure as defined above relates to each quantum bit as a separate partition. In the context of quantum algorithms it is indeed a natural way of partitioning the state, but there may be cases where this partitioning is not the natural one.

In order to be able to modify the Groverian measure to different partitioning we need to re-examine the meaning of "local operation". The locality of the operations comes from the fact that they are performed only within the partition. Therefore, all we need to do is change the definition of the local unitary operators so that they may operate on the whole partition, and not on single qubits. Using this definition, we can examine the entanglement of any desired partitioning.
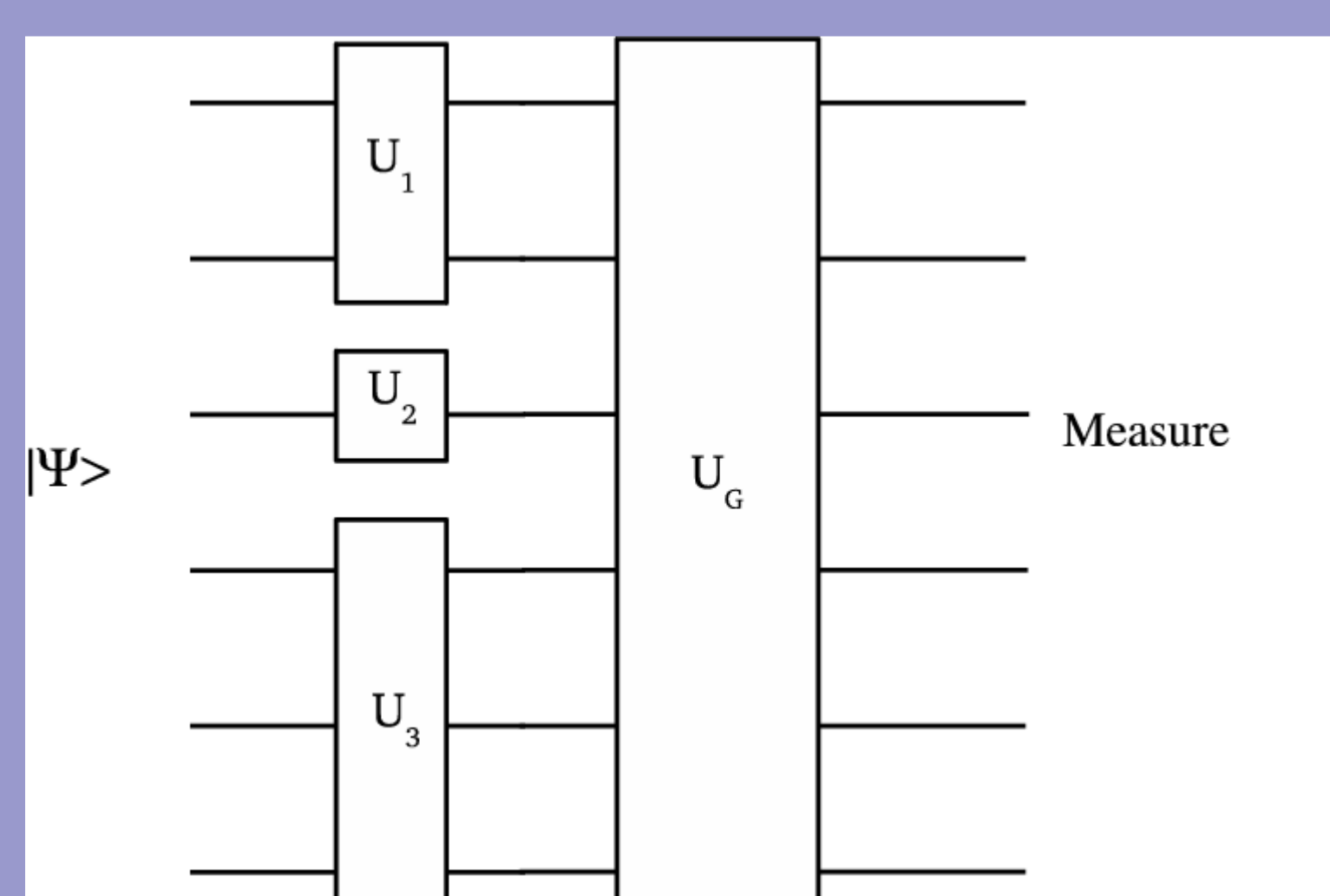
The quantum circuit that exemplifies the operational meaning of the Groverian entanglement measure for a pure quantum state with arbitrary partitioning.
The state is entered into the circuit, then a set of unitary operators, which are local to the partition, are applied to it in order to maximize the probability of success of the quantum algorithm which follows.

How entangled is a state?

Entanglement is considered to be a resource in many aspects, especially in encryption and communication protocols.

Given a pure quantum state, it is therefore of interest to know how entangled it is. This question depend, of course, on the partitioning. Using the Groverian measure it is possible to find the m-partitioning that gives the most entanglement. This means finding the partitioning to m groups that maximizes the probability of success of the quantum algorithm.

It is clear that using m-1 partitions it is possible to achieve at least the same as with m partitions. This can be seen by taking two of the m partitions and considering them as a single partition.

This procedure may be useful in determining suitable states for many party quantum communication, which may use more than just bipartite entanglement

The connection to bipartite entanglement:

When defining a multipartite entanglement measure, it must be consistent with existing bipartite entanglement measures.

Let us consider a state $|n\rangle$ where two partitions are defined. Using Schmidt decomposition, it is possible to write this state as a single sum over basis states from each partition, multiplied by their eigenvalue.

$$\sum_i \sqrt{p_i} |u\rangle_A |u\rangle_B$$

Since these basis vectors are orthonormal, the best the maximization process can do is match the two basis states with the maximal eigenvalue.

The maximization process therefore simply gives the maximal eigenvalue of the reduced density matrix of the partition, also know as the largest Schmidt coefficient, which is a known bipartite entanglement measure.

The Hebrew University of Jerusalem