MINIMAL SETS OF BI-PRODUCT EQUALITIES CHARACTERIZE SEPARABLE PURE QUANTUM STATES

Philippe Jorrand [*] ***and Mehdi Mhalla*** [†]

1 Introduction

Quantum computing operates in three steps: (i) preparation of the initial states of the n qubits of a register, (ii) transformation of the state of this n-qubit register by a composition of unitary operators which constitute the quantum program, and (iii), measurement of all or part of the n qubits of the register. The existence of quantum algorithms which are exponentially less complex than their classical counterparts for some classes of problems (see [3, 6] for a thorough presentation of quantum computing) stems from entangled states established by multi-qubit operators within the quantum program. The state $|\psi\rangle$ of a quantum system composed of two quantum subsystems A and B is said to be entangled when $|\psi\rangle$ is not a pair $|\psi_A\psi_B\rangle$ of a state of A and a state of B: clearly, this definition shows that entanglement has no classical counterpart. In quantum theory, such a pair is denoted by a Kronecker product $|\psi_A\rangle \otimes |\psi_B\rangle$: $|\psi\rangle$ is entangled if it cannot be factorized into $|\psi_A\rangle \otimes |\psi_B\rangle$.

This paper defines conditions according to which it is possible to tell whether or not the pure state of an n-qubit register is entangled. The state of a single qubit is

[*]CNRS, Philippe.Jorrand@imag.fr, Leibniz Laboratory, 46 av Félix-Viallet Grenoble, 38000, France

[†]CNRS, Mehdi.Mhalla@imag.fr, Leibniz Laboratory, 46 av Félix-Viallet Grenoble, 38000, France

a vector $\alpha|0\rangle + \beta|1\rangle$ of unit norm in a 2-dimensional vector space, where $|0\rangle$ and $|1\rangle$ are the two basis states and where α and β are complex numbers, called amplitudes in quantum theory. Then, if both A and B are qubits, the most general form of the state of a 2-qubit register composed of A and B is a vector in a 4-dimensional space: $|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$. It is straightforward to prove that $|\psi\rangle$ can be factorized into $|\psi_A\rangle \otimes |\psi_B\rangle$ if and only if $\alpha\delta = \beta\gamma$. In such a case, $|\psi\rangle$ is said to be separable, i.e. not entangled. This paper generalizes this form of condition to n-qubit registers. If $|\psi\rangle$ is now the state of an n-qubit register, two different ways of asking whether $|\psi\rangle$ is separable are answered: (i) is $|\psi\rangle$ separable into a product $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \ldots \otimes |\psi_n\rangle$ of n single qubit states, and (ii), is $|\psi\rangle$ separable into a product $|\psi_A\rangle \otimes |\psi_B\rangle$ of the states of two subregisters A and B, respectively containing p and q adjacent qubits with $p+q=n$? These conditions have the form of the minimal sets of equalities among products of two amplitudes of $|\psi\rangle$ necessary and sufficient for $|\psi\rangle$ to be separable.

The mathematical structure of quantum entanglement is not yet fully understood. There still exist fundamental open problems, one of them being the characterization of separability. This problem has been most extensively studied by considering the decomposition of quantum systems states into convex combinations of product states of two subsystems. Even when the dimensions of the global system are so that it may actually be a composite system of more than two subsystems, there are a lot more results concerning this form of biseparability than results concerning more complex forms of separability, where the problem would be to find whether the global system state can be decomposed in terms of products of more than two subsystems states. For a review of the main results and still open questions in the study of bipartite and multipartite entanglement, the reader is referred to the tutorial by Dagmar Bruß [2], the survey by Jozef Gruska and Hiroshi Imai [4] and the primer by Maciej Lewenstein et al. [5].

This paper defines direct separabilty criteria for pure multipartite quantum states of systems of n qubits for any $n \geq 2$. Two forms of separability are considered, *full separability* and *p-q separability*:

Definition 1. *A pure state $|\psi_N\rangle \in \mathcal{H}_N$ of a quantum system composed of n qubits, where $\mathcal{H}_N$ is the Hilbert space of dimension $N = 2^n$, is fully separable iff it can be factorized into a tensor product of n qubit states, each of them in $\mathcal{H}_2$:*

$|\psi_N\rangle$ is fully separable $\iff$ $\exists\, |\psi_2\rangle_0, |\psi_2\rangle_1 \ldots |\psi_2\rangle_{n-1} \in \mathcal{H}_2$ such that $|\psi_N\rangle = |\psi_2\rangle_0 \otimes |\psi_2\rangle_1 \otimes \cdots \otimes |\psi_2\rangle_{n-1}$

Definition 2. *Given integers p and q such that $p+q=n$, $|\psi_N\rangle$ is $p-q$ separable iff it can be factorized into a tensor product of a subsystem state $|\psi_P\rangle \in \mathcal{H}_P$ with a subsystem state $|\psi_Q\rangle \in \mathcal{H}_Q$ where $P = 2^p$ and $Q = 2^q$ (i.e. the two subsystems are composed of p and q qubits respectively):*

$|\psi_N\rangle$ is $p-q$ separable $\iff$ $\exists\, |\psi_P\rangle \in \mathcal{H}_P, |\psi_Q\rangle \in \mathcal{H}_Q$ such that $|\psi_N\rangle = |\psi_P\rangle \otimes |\psi_Q\rangle$

The criterion for full separability is given in part 2 of the paper and the criterion for $p-q$ separability in section 3. The last section of the paper draws

attention to more refined questions which are worth studying further on the basis of these results about separability and entanglement in n qubit systems.

2 Full Separability

Let α_i, $0 \leq i \leq N-1$, $N = 2^n$, be the amplitudes of $|\psi_N\rangle \in \mathcal{H}_N$, with $\sum_{i=0}^{N-1} |\alpha_i|^2 = 1$: $|\psi_N\rangle = \sum_{i=0}^{N-1} \alpha_i |i\rangle$

Definition 3. *Pair product invariance is a property of $|\psi_N\rangle$ defined as follows: $|\psi_N\rangle$ is pair product invariant $\iff$ $\forall k \in [1,n], \exists$ a constant c_k such that $\forall i \in [0, K-1] \alpha_i \alpha_{K-i-1} = c_k$ where, for any integer k, K denotes 2^k.*

If $|\psi_N\rangle$ is pair product invariant, many other equalities among products of pairs of amplitudes are satisfied. The definition of pair product invariance provides a minimal set of such equalities from which all others can be obtained. Among the consequences of pair product invariance, equalities of the form $\alpha_{2i-1}\alpha_{2i} = \alpha_{2i-2}\alpha_{2i+1}$, with $1 \leq i \leq 2^{n-1}-1$, are of special interest for proving the conditions of full separability of $|\psi_N\rangle$. The following lemma shows that these equalities indeed hold whenever $|\psi_N\rangle$ is pair product invariant, provided that no amplitude of $|\psi_N\rangle$ is zero:

Lemma 4. *Let $|\psi_N\rangle$ be a state with no zero amplitude. Then: $|\psi_N\rangle$ is pair product invariant $\Longrightarrow \forall i \in [1, 2^{n-1}-1]\, \alpha_{2i-1}\alpha_{2i} = \alpha_{2i-2}\alpha_{2i+1}$*

Proof. By induction on index i. □

Lemma 5. *Let $|\psi_N\rangle \in \mathcal{H}_N$ be a state with no zero amplitude. Then:*
$|\psi_N\rangle$ is fully separable $\iff$ $|\psi_N\rangle$ is pair product invariant

Proof. By induction on n, the number of qubits, using lemma 4. □

States $|\psi_N\rangle = \sum_{i=0}^{N-1} \alpha_i |i\rangle \in \mathcal{H}_N$, where $N = 2^n$, are always considered to be normalized: $\sum_{i=0}^{N-1} |\alpha_i|^2 = 1$. If $|\psi_2\rangle \in \mathcal{H}_2$ and $|\psi_N\rangle$ is a fully separable state in $\mathcal{H}_N$ then $|\psi_2\rangle \otimes |\psi_N\rangle$, is a fully separable state in $\mathcal{H}_{2N}$. The subset $\mathcal{K}_N$ of all fully separable states in $\mathcal{H}_N$ is defined recursively as follows:

$$\begin{array}{lcl} \mathcal{K}_2 & = & \mathcal{H}_2 \\ \mathcal{K}_{2N} & = & \{|\psi_2\rangle \otimes |\psi_N\rangle \,|\, |\psi_2\rangle \in \mathcal{K}_2 \text{ and } |\psi_N\rangle \in \mathcal{K}_N\} \end{array}$$

With $|\psi_2\rangle = \begin{pmatrix} \delta_0 \\ \delta_1 \end{pmatrix}$, $|\psi_{2N}\rangle \in \mathcal{K}_{2N}$ is $|\psi_{2N}\rangle = \begin{pmatrix} \delta_0 \\ \delta_1 \end{pmatrix} \otimes |\psi_N\rangle$, i.e., for short: $|\psi_{2N}\rangle = \begin{pmatrix} \delta_0 |\psi_N\rangle \\ \delta_1 |\psi_N\rangle \end{pmatrix}$.

An amplitude abstraction function $f : \mathcal{H}_N \to \{0,1\}^N$, a set of *well-formed bit strings*, a set of *well-formed states* $\mathcal{V}_N \subset \mathcal{H}_N$ and a family of *zero deletion functions*

$g_K : \mathcal{V}_N \to \mathcal{H}_K$, with $K = 2^k$ for $1 \leq k \leq n$, will be useful for characterizing the general case of full separability of $|\psi_N\rangle$, when some amplitudes in $|\psi_N\rangle$ may be zero.

Definition 6. *When applied to* $|\psi_N\rangle = \sum_{i=0}^{N-1} \alpha_i |i\rangle \in \mathcal{H}_N$*, the amplitude abstraction function* $f : \mathcal{H}_N \to \{0,1\}^N$ *yields a bit string* $x \in \{0,1\}^N$*, with* $x = x_0 x_1 \ldots x_{N-1}$ *such that, for* $0 \leq i \leq N-1$*:*

$$\begin{array}{rcll} x_i & = & 0 & \text{iff} \quad \alpha_i = 0 \\ x_i & = & 1 & \text{otherwise} \end{array}$$

Definition 7. *The set* $\mathcal{B}_N \subset \{0,1\}^N$ *of well-formed bit strings of length* N *is defined recursively as follows:*

$$\begin{array}{rcl} \mathcal{B}_2 & = & \{01, 10, 11\} \\ \mathcal{B}_{2N} & = & \{0^N x, x0^N, xx \,|\, x \in B_N\} \end{array}$$

where 0^N *is a string of* N *0s.*

The number of 1s in $x \in \mathcal{B}_{2N}$ is either the number of 1s in $y \in \mathcal{B}_N$ if $x = 0^N y$ or $x = y0^N$, or twice that number if $x = yy$. Therefore, the number of 1s in $x \in \mathcal{B}_N$ is $K = 2^k$, with $k \leq n$: this number will be denoted by $|x|$. It is also useful to notice that the distributions of the 0s in the string x when $x = yy$ are identical in both halves of x. One may also notice that there are 3^n different bit strings in $\mathcal{B}_{2^n}$. The bit strings in $\mathcal{B}_N$ are said to be well-formed because they are amplitude abstractions of fully separable states. This is the purpose of the next lemma:

Lemma 8. $\forall\, |\psi_N\rangle \in \mathcal{K}_N : f(|\psi_N\rangle) \in \mathcal{B}_N$

Proof. By induction on n, the number of qubits. □

According to this simple lemma, the bit strings in $\mathcal{B}_N$ tell where the 0s must be for a state $|\psi_N\rangle \in \mathcal{H}_N$ to be fully separable. But not all $|\psi_N\rangle \in \mathcal{H}_N$ such that $f(|\psi_N\rangle) \in \mathcal{B}_N$ are fully separable. There is indeed a set of states $\mathcal{V}_N$, with $\mathcal{K}_N \subset \mathcal{V}_N \subset \mathcal{H}_N$, and such that $\forall\, |\psi_N\rangle \in \mathcal{V}_N f(|\psi_N\rangle) \in \mathcal{B}_N$:

Definition 9. *The set of well-formed states is:* $\mathcal{V}_N = \{|\psi_N\rangle \in \mathcal{H}_N \,|\, f(|\psi_N\rangle) \in \mathcal{B}_N\}$

When a well-formed state $|\psi_N\rangle \in \mathcal{V}_N$ has a number of zero amplitudes, these are placed correctly for this state to be a candidate to full separability.

But being well formed is not enough for $|\psi_N\rangle$ to be fully separable, there must also be conditions satisfied by the non-zero amplitudes of $|\psi_N\rangle$, and by them only. Since $f(|\psi_N\rangle) \in \mathcal{B}_N$, there are $K = 2^k$ non-zero amplitudes in $|\psi_N\rangle$, with $k \leq n$. If $K = 1$, $|\psi_N\rangle$ is not a superposition, hence not entangled: this trivial case will not be considered in what follows. For $K \geq 2$, only the K non-zero amplitudes of $|\psi_N\rangle$

have to be considered. For this, all zero amplitudes will be eliminated from $|\psi_N\rangle$, yielding a state $|\psi_K\rangle \in \mathcal{H}_K$ with no zero amplitudes:

Definition 10. *For all sets $\mathcal{V}_N$ of well-formed states, there exists a family of zero deletion functions $\{g_K : \mathcal{V}_N \to \mathcal{H}_K | K = 2^k, 1 \leq k\ n\}$ defined as follows:*
$\forall\, |\psi_N\rangle = \sum_{i=0}^{N-1} \alpha_i\, |i\rangle$ *with* $|f(|\psi_N\rangle)| = K$ *and* $K \geq 2$, $g_K(|\psi_N\rangle) = \sum_{i=0}^{N-1} \alpha'_j\, |j\rangle$, *where* $\alpha'_j = \alpha_i$ *such that* $|\{\alpha_l |\, l < i \text{ and } \alpha_l \neq 0\}| = j$

The stage is now set for characterizing full separability of $|\psi_N\rangle$ in the general case:

Theorem 11. *Let $|\psi_N\rangle \in \mathcal{H}_N$ be a state with $|f(|\psi_N\rangle)| = K$ and $2 \leq K \leq N$. Then: $|\psi_N\rangle$ is fully separable $\iff$ $|\psi_N\rangle$ is well-formed and $g_K(|\psi_N\rangle)$ is pair product invariant.*

Proof.
Case $\Longrightarrow$: by induction on n, the number of qubits.
Base case: for $n = 2$, if $|\psi_4\rangle$ is fully separable, then $|\psi_4\rangle$ is well formed since $|\psi_4\rangle \in \mathcal{K}_4 \subset \mathcal{V}_4$ by definition of these sets. If $K = 2$, $g_K(|\psi_4\rangle) \in \mathcal{H}_2$ is trivially pair product invariant. If $K = 4$, the full separability of $|\psi_4\rangle$ implies $\alpha_1\alpha_2 = \alpha_0\alpha 3$, which is precisely the pair product invariance of $g_K(|\psi_4\rangle) \in \mathcal{H}_4$.
Induction step: assume the $\Longrightarrow$ property holds for $2, 3, \ldots n$ qubits. Let $|\psi_{2^{n+1}}\rangle = |\psi_{2N}\rangle$ be a state fully separable into a product of $n + 1$ component qubit states, i.e. $|\psi_{2N}\rangle \in \mathcal{K}_{2N}$. Then, by definition of well-formedness, $|\psi_{2N}\rangle$ is indeed well-formed: $f(|\psi_{2N}\rangle) \in \mathcal{B}_{2N}$. Being fully separable, $|\psi_{2N}\rangle$ can in particular be separated into:

$$|\psi_{2N}\rangle = \begin{pmatrix} \delta_0 \\ \delta_1 \end{pmatrix} \otimes |\psi_N\rangle = \begin{pmatrix} \delta_0\, |\psi_N\rangle \\ \delta_1\, |\psi_N\rangle \end{pmatrix}$$

where $\begin{pmatrix} \delta_0 \\ \delta_1 \end{pmatrix} \in \mathcal{H}_2$ is normalised.
If $\delta_0 = 0$, since $\delta_1 = 1$ and $|f(|\psi_{2N}\rangle)| = |f(|\psi_N\rangle)| = K$ in this case, then $g_K(|\psi_{2N}\rangle) = g_K(|\psi_N\rangle)$: by induction hypothesis on $|\psi_N\rangle$, $g_K(|\psi_{2N}\rangle)$ is pair product invariant. Same reasoning when $\delta_1 = 0$.
If neither δ_0 nor δ_1 is zero, and since $|f(|\psi_{2N}\rangle)| = 2\,|f(|\psi_N\rangle)| = 2K$ in this case:

$$g_K(|\psi_{2N}\rangle) = \begin{pmatrix} \delta_0 \\ \delta_1 \end{pmatrix} \otimes g_K(|\psi_N\rangle) = \begin{pmatrix} \delta_0 g_K(|\psi_N\rangle) \\ \delta_1 g_K(|\psi_N\rangle) \end{pmatrix}$$

Then, it is easy to verify that the induction hypothesis on $|\psi_N\rangle$, i.e. the pair product invariance of $g_K(|\psi_N\rangle)$, implies the pair product invariance of $g_{2K}(|\psi_{2N}\rangle)$.
Case $\Longleftarrow$: also by induction on n.
Base case: for $n = 2$, $|\psi_4\rangle$ being well-formed means that $f(|\psi_4\rangle) \in \{0011, 1100, 1010, 0101\}$ when $K = 2$, and that $f(|\psi_4\rangle) = 1111$ when $K = 4$. Then, when $K = 2$, $\alpha_1\alpha_2 = \alpha_0\alpha_3$, and when $K = 4$, the pair product invariance of $g_K(|\psi_4\rangle) \in \mathcal{H}_4$ is $\alpha_1\alpha_2 = \alpha_0\alpha_3$: in both cases, $|\psi_4\rangle$ is indeed fully separable.

Induction step: assume the $\Longleftarrow$ property holds for $2, 3, \ldots n$ qubits. $|\psi_{2N}\rangle$ is well-formed and, for some K, $g_K(|\psi_{2N}\rangle)$ is pair product invariant. The $2N$ amplitudes of $|\psi_{2N}\rangle$ can be divided in two halves: the first N amplitudes will be viewed as $\gamma_0 |\phi_N\rangle$ where $|\phi_N\rangle \in \mathcal{H}_N$ and the N remaining ones as $\gamma_1 |\chi_N\rangle$ where $|\chi_N\rangle \in \mathcal{H}_N$. The only purpose of the complex coefficients γ_0 and γ_1 is to keep $|\psi_{2N}\rangle$ normalized: $|\gamma_0|^2 + |\gamma_1|^2 = 1$, since both $|\phi_N\rangle$ and $|\chi_N\rangle$ are themselves normalized. This will be summarized visually with the use of the (abusive) notation: $|\psi_{2N}\rangle = \begin{pmatrix} \gamma_0 |\phi_N\rangle \\ \gamma_1 |\chi_N\rangle \end{pmatrix}$.

The well-formedness of $|\psi_{2N}\rangle$ distinguishes three possible distributions of its zero amplitudes:

(i) $f(|\phi_N\rangle) = 0^N$ and $f(|\chi_N\rangle) \neq 0^N$ with $f(|\chi_N\rangle) \in \mathcal{B}_N$. In this case, $\gamma_1 = 1$, $|f(|\psi_{2N}\rangle)| = |f(|\chi_N\rangle)| = K$ and $g_K(|\psi_{2N}\rangle) = g_K(|\chi_N\rangle)$, which implies that $g_K(|\chi_N\rangle)$ is pair product invariant. Thus, by induction hypothesis, $|\chi_N\rangle$ is fully separable, and so is also $|\psi_{2N}\rangle$ since $|\psi_{2N}\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes |\chi_N\rangle$.

(ii) $f(|\psi_N\rangle) \neq 0^N$ and $f(|\chi_N\rangle) = 0^N$ with $f(|\psi_N\rangle) \in \mathcal{B}_N$. Same reasoning as for case (i).

(iii) $f(|\phi_N\rangle) = f(|\chi_N\rangle) \neq 0^N$ with $f(|\phi_N\rangle), f(|\chi_N\rangle) \in \mathcal{B}_N$. In this case, $\gamma_0 \neq 0$, $\gamma_1 \neq 0$ and $|f(|\psi_{2N}\rangle| = 2|f(|\phi_N\rangle)| = 2K$. By theorem 5, since $g_{2K}(|\psi_N\rangle)$ has no zero amplitude and is pair product invariant, it is fully separable:

$$g_{2K}(|\psi_{2N}\rangle) = \begin{pmatrix} \delta_0 \\ \delta_1 \end{pmatrix} \otimes |\omega_K\rangle = \begin{pmatrix} \delta_0 |\omega_K\rangle \\ \delta_1 |\omega_K\rangle \end{pmatrix} \text{ for } \begin{pmatrix} \delta_0 \\ \delta_1 \end{pmatrix} \in \mathcal{H}_2$$

with $\delta_0, \delta_1 \neq 0$ and $|\omega_K\rangle \in \mathcal{H}_K$ fully separable and with no zero amplitude.

$f(|\phi_N\rangle) = f(|\chi_N\rangle)$ means that the positions of the 0s within $|\phi_N\rangle$ are the same as the positions of the 0s within $|\chi_N\rangle$. It is always possible to find $|\psi_N\rangle$ having all its 0s at the same positions as those of both $|\phi_N\rangle$ and $|\chi_N\rangle$ and such that $g_K(|\psi_N\rangle) = |\omega_K\rangle$. Therefore $\gamma_0 |\phi_N\rangle = \delta_0 |\psi_N\rangle$ and $\gamma_1 |\chi_N\rangle = \delta_1 |\psi_N\rangle$, hence:

$$|\psi_{2N}\rangle = \begin{pmatrix} \delta_0 |\psi_N\rangle \\ \delta_1 |\psi_N\rangle \end{pmatrix} = \begin{pmatrix} \delta_0 \\ \delta_1 \end{pmatrix} \otimes |\psi_N\rangle$$

where $|\psi_N\rangle$, a kind of common divisor of $|\phi_N\rangle$ and $|\chi_N\rangle$, is well-formed by construction and is such that $g_K(|\psi_N\rangle) = |\omega_K\rangle$ is pair product invariant by lemma 5, since it is fully separable and with no zero amplitude. In conclusion, the induction hypothesis applies to $|\psi_N\rangle$: $|\psi_N\rangle$ is fully separable and so is also $|\psi_{2N}\rangle$. □

3 $p - q$ Separability

Given integers p and q such that $p + q = n$, $|\psi_N\rangle$ is $p - q$ separable iff it can be factorized into a tensor product: $|\psi_N\rangle = |\psi_P\rangle \otimes |\psi_Q\rangle$, where $|\psi_P\rangle \in \mathcal{H}_P$ and $|\psi_Q\rangle \in \mathcal{H}_Q$, with $P = 2^p$ and $Q = 2^q$ (i.e. the two subsystems are composed of p and q qubits respectively).

$$\text{Let } |\psi_N\rangle = \begin{pmatrix} \alpha_0 \\ \vdots \\ \alpha_{kQ+r} \\ \vdots \\ \alpha_{N-1} \end{pmatrix}, |\psi_P\rangle = \begin{pmatrix} \beta_0 \\ \vdots \\ \beta_k \\ \vdots \\ \beta_{P-1} \end{pmatrix} \text{ and } |\psi_Q\rangle = \begin{pmatrix} \gamma_0 \\ \vdots \\ \gamma_r \\ \vdots \\ \gamma_{Q-1} \end{pmatrix}$$

In other words, $|\psi_N\rangle$ is $p-q$ separable iff $\forall k \in [0, P-1]$ and $\forall r \in [0, Q-1]$, $\alpha_{kQ+r} = \beta_k \gamma_r$. This defines a structure for the N amplitudes in $|\psi_N\rangle$. There are P groups of Q amplitudes each: $\alpha_{kQ+r} = \beta_k \gamma_r$ is amplitude $r\,(r \in [0, Q-1])$ in group $k\,(k \in [0, P-1])$. This means that, if $\beta_k = 0$, all amplitudes in group k are equal to zero, and that the distributions of zeros within all groups obtained with $\beta_k \neq 0$ are the same and are identical to the distribution of zeros within $|\psi_Q\rangle$.

Theorem 12. *Let $|\psi_N\rangle \in \mathcal{H}_N$, with $N = PQ$, be a state such that for some $i_0 = k_0 Q + r_0 \in [0, N-1]$, $\alpha_{i_0} \neq 0$ and $\forall i < i_0$, $\alpha_i = 0$. Then: $|\psi_N\rangle$ is $p-q$ separable $\iff \forall k \in [k_0+1, P-1], \forall r \in [r_0+1, Q-1], \alpha_{k_0 Q+r_0} \alpha_{kQ+r} = \alpha_{kQ+r_0} \alpha_{k_0 Q+r}$*

Proof.

Case $\Longrightarrow$: $|\psi_N\rangle$ $p-q$ separable means that $\forall k \in [0, P-1], \forall r \in [0, Q-1], \alpha_{kQ+r} = \beta_k \gamma_r$. Then: $\forall k \in [k_0+1, P-1], \forall r \in [r_0+1, Q-1], \alpha_{k_0 Q+r_0} \alpha_{kQ+r} = \beta_{k_0} \gamma_{r_0} \beta_k \gamma_r = \beta_{k_0} \gamma_r \beta_k \gamma_{r_0} = \alpha_{kQ+r_0} \alpha_{k_0 Q+r}$.

Case $\Longleftarrow$: given $|\psi_N\rangle$ where $\alpha_{k_0 Q+r_0}$ is the first non zero amplitude, and such that $\forall k \in [k_0+1, P-1], \forall r \in [r_0+1, Q-1], \alpha_{k_0 Q+r_0} \alpha_{kQ+r} = \alpha_{kQ+r_0} \alpha_{k_0 Q+r}$, the problem is to prove that there exist quantum states $|\psi_P\rangle$ and $|\psi_Q\rangle$ such that $|\psi_N\rangle = |\psi_P\rangle \otimes |\psi_Q\rangle$. The proof goes by finding $|\psi_P\rangle$ and $|\psi_Q\rangle$ such that $\forall k \in [0, P-1], \forall r \in [0, Q-1], \alpha_{kQ+r} = \beta_k \gamma_r$, where $|\psi_N\rangle$ is given, and where $|\psi_P\rangle$ and $|\psi_Q\rangle$ are normalized quantum states.

Instances of such states $|\psi_P\rangle$ and $|\psi_Q\rangle$ can be obtained by choosing, $\forall k \in [0, P-1]$, $\forall r \in [0, Q-1]$ a γ_{r_0} such that:

$$\gamma_{r_0} \gamma_{r_0}^* = \frac{1}{1 + \frac{\sum_{i=i_0+1}^{(k_0+1)Q-1} \alpha_i \alpha_i^*}{\alpha_{i_0} \alpha_{i_0}^*}}, \; \gamma_r = \frac{\gamma_{r_0} \alpha_{k_0 Q+r}}{\alpha_{i_0}}, \text{ and } \beta_k = \frac{\alpha_{kQ+r_0}}{\gamma_{r_0}}.$$

This choice implies that $|\psi_N\rangle = |\psi_P\rangle \otimes |\psi_Q\rangle$. Indeed, $\forall k \in [k_0+1, P-1]$:

- $\forall r \in [r_0+1, Q-1]$:

$$\begin{aligned} \beta_k \gamma_r &= \frac{\alpha_{kQ+r_0}}{\gamma_{r_0}} \frac{\gamma_{r_0} \alpha_{k_0 Q+r}}{\alpha_{i_0}} = \frac{\alpha_{k_0 Q+r} \alpha_{kQ+r_0}}{\alpha_{i_0}} \\ &= \frac{\alpha_{k_0 Q+r_0} \alpha_{kQ+r}}{\alpha_{i_0}} \quad \text{by the hypothesis of case } \Longleftarrow \\ &= \alpha_{kQ+r} \end{aligned}$$

- For $r = r_0$, $\beta_k \gamma_{r_0} = \alpha_{kQ+r_0}$ by definition of β_k and γ_{r_0}.

- $\forall r \in [0, r_0-1]$, $\alpha_{k_0 Q+r} = 0$. Then $\gamma_k = 0$ by its definition, and $\alpha_{kQ+r} = 0$ by the hypothesis of case $\Longleftarrow$. Hence: $\beta_k \gamma_r = \alpha_{kQ+r}$

For the other values of k : $k = k_0 \Longrightarrow \beta_{k_0}\gamma_r = \alpha_{k_0Q+r}$ by definition of β_{k_0} and γ_r, and, $\forall k \in [0, k_0 - 1]$, $\alpha_{kQ+r} = \beta_k\gamma_r$ since $\alpha_{kQ+r} = 0$ and $\beta_k = 0$ bnecause $\alpha_{kQ+r_0} = 0$.
Finally, since $|\psi_N\rangle = |\psi_P\rangle \otimes |\psi_Q\rangle$, $|\psi_P\rangle$ and $|\psi_Q\rangle$ are normalized quantum states:

$$\begin{aligned} \| \, |\psi_Q\rangle \, \|^2 &= \textstyle\sum_{r=0}^{Q-1} \gamma_r\gamma_r^* = \sum_{r=0}^{r_0-1-1} \gamma_r\gamma_r^* + \gamma_{r_0}\gamma_{r_0}^* + \sum_{r=r_0+1}^{Q-1} \gamma_r\gamma_r^* \\ &= \gamma_{r_0}\gamma_{r_0}^* + \textstyle\sum_{r=r_0+1}^{Q-1} \gamma_r\gamma_r^* \quad \text{because} \, \beta_{k_0} \neq 0 \\ &\qquad\qquad \text{and} \, \forall r < r_0, \alpha_{k_0Q+r} = 0 \Longrightarrow \forall r < r_0, \gamma_r = 0 \\ &= \gamma_{r_0}\gamma_{r_0}^* \left(1 + \textstyle\sum_{r=r_0+1}^{Q-1} \frac{\alpha_{k_0Q+r}\alpha_{k_0Q+r}^*}{\alpha_{i_0}\alpha_{i_0}^*}\right) = 1 \end{aligned}$$

$\| \, |\psi_P\rangle \, \|^2 = \frac{\| |\psi_N\rangle \|^2}{\| |\psi_Q\rangle \|^2} = 1$
Hence $|\psi_N\rangle$ is $p - q$ separable. □

4 Conclusion

The results presented in this paper for full separability and $p - q$ separability of pure states of n qubits are a broad generalization of a similar approach described by Rajagopal and Rendell. In [7], they analyze the robustness or fragility of three qubit entanglements, depending on their permutation symmetries, and characterize their full and $1-2$ separabilities by means of sets pair product equalities. But their characterizations are not of minimal size and concern implicitly only very limited situations, namely those where there are no zeros among the amplitudes of the state of the system. With a slightly different approach, Wang [8] arrives at very similar results for three qubits, with a specific and hard to generalize treatment of zero amplitudes, and proposes conjectures for the general case of n qubits.

What has been proved in this paper are necessary and sufficient criteria for the full and the $p-q$ separability of pure states of n qubits in general. Clearly, full separability implies $p-q$ separability, but the converse is not true, since $p-q$ separability does not tell anything about the separability properties of the subsystems, i.e. about the presence or absence of entanglement within each of the separated subsystems. What is more important is that $p - q$ separability relies on a proper ordering among the qubits: if the n qubits are numbered from 0 to $n - 1$, $|\psi_P\rangle$ is indeed the state of the subsystem composed of the qubits numbered from 0 to $p-1$, whereas $|\psi_Q\rangle$ is the state of the subsystem composed of qubits p to $n-1$. As a consequence a reordering among the qubits will in general be required for $p - q$ separability to appear provided that $|\psi_N\rangle$, as modified after reordering the qubits, is indeed $p - q$ separable. Searching for values of p and q such that $|\psi_N\rangle$ is $p - q$ separable could of course be tried by brute iterative force, going through all the $n!$ permutations. There may be more subtle approaches, by relying upon invariance properties of sets of pair product equalities when two qubits are swapped. Some such properties, rather elegant, have been found, but it is not clear yet if and how they can be exploited efficiently.

Both full separability and $p - q$ separability are invariant under unitary operations local to any of the subsystems. In [1], entanglement and separability are

studied by making explicit the consequences of such invariance properties: this is done first in the case of systems composed of two N-dimensional subsystems, then in the case of systems composed of three N-dimensional subsystems, after which a generalization to M N-dimensional subsystems is briefly presented. The approach taken here is different, but similar questions could be addressed. The results presented here for full separability rely essentially on the notion of pair product invariance. A similar notion can be extended to $p-q$ separability. It could be the case -this remains a conjecture- that this rather basic invariance bears some useful relations with entanglement measures.

A straightforward analysis of the computational complexity of the criterion for $p-q$ separability based upon theorem 12 shows that, in the worst case (i.e. when $\alpha_0 \neq 0$), $N-P-Q+1$ comparisons of $2(N-P-Q+1)$ products of two amplitudes are required. For full separabilty (theorem 11), the analysis is a little more complicated because, in addition to checking pair product invariance among non-zero amplitudes, it is necessary to check that the state is well-formed with respect to the distribution of its zero amplitudes: this results in a complexity of the order of N products and $2N$ comparisons for full separability.

Finally, there are strong indications that, for some broad classes of pure quantum states of n qubits, the characterization of $p-q$ separability could be a lot simpler than the characterization given here. It seems also that, for these classes, generalizations to $p-q-r-\ldots$ separability would be rather easy to obtain. An example of such a class are the states defined by stabilizers and closed under a small set of unitary operators.

Acknowledgements

The authors wish to thank Rémy Mosseri for a fruitful working session at a very early point in the development of this work, and Sylvain Gravier for stimulating discussions all along. This work was supported by the IMAG Project on Quantum Informatics, by an EPML grant from Centre National de la Recherche Scientifique and by a BQR grant from Institut National Polytechnique de Grenoble.

Bibliography

[1] S. Albeverio and S.M. Fei. A note on invariants and entanglement. *e-print quant-ph/0109073*, 2001.

[2] D. Bruß. Characterizing entanglement. *Journal of Mathematical Physics*, 43:4237, 2002.

[3] J. Gruska. *Quantum computing*. McGraw-Hill, 1999.

[4] J. Gruska and H. Imai. Power, puzzles and properties of entanglement. In *Proceedings of 3rd International Conference on Machines, Computations and Universality*, LNCS 2055, Springer, 2001.

[5] M. Lewenstein, D. Bruß, J.I. Cirac, B. Kraus, M. Kus, J. Samsonowicz, A. Sanpera, and R. Tarrach. Separability and distillability in composite quantum systems a primer. *e-print quant-ph/0006064*, 2000.

[6] M.A. Nielsen and I.L. Chuang. *Quantum computation and quantum information*. Cambridge University Press, 2000.

[7] A.K. Rajagopal and R.W. Rendell. Robust and fragile entanglement of three qubits: relation to permutation symmetry. *Physical Review A*, 65:032328, 2002.

[8] A.M. Wang. Separability criterion for pure states in multipartite and high dimensional systems. *e-print quant-ph/0207136*, 2002.