Suppose we divide a system into two parts, with normalized basis elements $|i\rangle$ and $|j\rangle$, respectively ($i = 1, \ldots, n$ and $j = 1, \ldots, m$), and consider the most general state

$$|\Psi\rangle = \sum_{ij} M_{ij} |i\rangle |j\rangle$$

expanded in terms of the direct product basis. M is a set of complex coefficients (normalized so that $1 = \langle\Psi|\Psi\rangle = \mathrm{tr} M^\dagger M$). The question is whether or not the two parts of the system are entangled, or if there is some change of basis in terms of which the above state is a simple product of states in the two component parts. The answer to this question is provided by the "Schmidt decomposition" (a.k.a. the SVD = singular value decomposition) of M, considered as an $n \times m$ matrix (where n, m are the dimensions of the two subsystems, not necessarily equal).

Recall that a Hermitian matrix H (i.e., $H = H^\dagger$) can be written $H = U \Lambda U^\dagger$, where Λ is a real diagonal matrix of eigenvalues and U is unitary ($UU^\dagger = U^\dagger U = \mathbf{1}$).[1]

This generalizes to a complex $n \times m$ matrix M by writing the Hermitian matrices $MM^\dagger$ and $M^\dagger M$ in diagonal form as $MM^\dagger = U \Lambda U^\dagger$ and $M^\dagger M = V \tilde{\Lambda} V^\dagger$. Here U, V are unitary matrices, the non-zero entries of the $n \times n$ and $m \times m$ diagonal matrices Λ and $\tilde{\Lambda}$ coincide[2], and are real and positive.[3] The general complex M_{ij} can therefore be written[4]

$$M = U \Sigma V^\dagger \ ,$$

where the diagonal matrix Σ has "singular values" s_i taken by convention[5] as the positive square roots of the eigenvalues λ_i in Λ: $s_i = +\sqrt{\lambda_i}$.

In components, the above formula can be written $M_{ij} = \sum_{k=1}^{\min(n,m)} U_{ik} s_k V^*_{jk}$, so that

$$|\Psi\rangle = \sum_{ij} M_{ij} |i\rangle |j\rangle = \sum_k s_k U_{ik} V^*_{jk} |i\rangle |j\rangle = \sum_k s_k |u_k\rangle |v^*_k\rangle,$$

in terms of the rotated basis vectors $|u_k\rangle = \sum_i U_{ik} |i\rangle$, $|v^*_k\rangle = \sum_j V^*_{jk} |j\rangle$.
$|\Psi\rangle$ is evidently a product state if and only if a single s_k is non-zero.
Otherwise the two subsystems are necessarily entangled.

If $n = m$ and $s_i = 1/\sqrt{n}$ for all i, then the two systems are "maximally entangled".[6]

---

[1] A real symmetric matrix S (i.e., $S = S^T$) can be written $S = O \Lambda O^T$, where Λ is a real diagonal matrix of eigenvalues and O is orthogonal ($OO^T = O^T O = \mathbf{1}$).

[2] The maximum number of non-zero values is equal to the smaller of n and m, i.e., the rank of M.

[3] Since $MM^\dagger$ and $M^\dagger M$ are positive semi-definite.

[4] For an $n \times m$ real matrix M, the symmetric matrices MM^T and $M^T M$ can be written in diagonal form as $MM^T = U \Lambda U^T$ and $M^T M = V \tilde{\Lambda} V^T$, with U, V orthogonal matrices. It follows that $M = U \Sigma V^T$, where the "singular values" s_i of Σ are again given in terms of the eigenvalues λ_i of Λ as $s_i = +\sqrt{\lambda_i}$.

[5] The sign is a convention since it can be compensated by flipping either the sign of a column of U or a row of V, preserving unitarity. Note that Σ is an $n \times m$ matrix, with an $n \times n$ block of diagonal singular values and an $n \times (m - n)$ block of zeros to the right if $m > n$, or with an $m \times m$ of diagonal singular values and an $(n - m) \times m$ block of zeros below if $m < n$.

[6] The reduced density operator for either subsystem after tracing over the other has maximum entropy.

As in sec. 1.11 of text, consider a general 2-qubit state

$$\Psi = \sum_{i,j=0}^{1} \alpha_{ij} |i\rangle |j\rangle$$

where α_{ij} are complex numbers and $\sum_{i,j} |\alpha_{ij}|^2 = 1$. Considered as a 2×2 complex matrix, we can write α as

$$\alpha = u \Sigma v^\dagger \ ,$$

or in component form

$$\alpha_{ij} = \sum_k u_{ik} s_k v^*_{jk} \ .$$

Recall[*] that $\mathbf{u}|i\rangle = \sum_j |j\rangle\langle j|\mathbf{u}|i\rangle = \sum_j u_{ji}|j\rangle$, so we can write

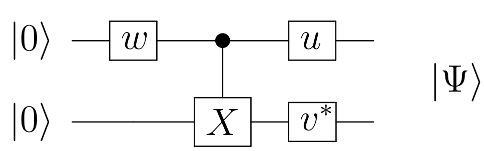
$$\begin{aligned} |\Psi\rangle &= \sum_{i,j,k} u_{ik} s_k v^*_{jk} |i\rangle|j\rangle = \sum_k (\mathbf{u} \otimes \mathbf{v}^*) s_k |k\rangle|k\rangle = (\mathbf{u} \otimes \mathbf{v}^*)\big(s_0|0\rangle|0\rangle + s_1|1\rangle|1\rangle\big) \\ &= (\mathbf{u} \otimes \mathbf{v}^*)\mathbf{C}_{10}\big(s_0|0\rangle + s_1|1\rangle\big)|0\rangle \end{aligned}$$

We see that the entanglement between the two qubits is provided entirely[†] by the cNOT $\mathbf{C}_{10}$. $|\Psi\rangle$ by assumption has unit norm, so the overall transformation above must be unitary, and since everything else is unitary then $s_0|0\rangle + s_1|1\rangle = \mathbf{w}|0\rangle$ for some[‡] unitary $\mathbf{w}$.

The result is

$$|\Psi\rangle = (\mathbf{u} \otimes \mathbf{v}^*)\mathbf{C}_{10}(\mathbf{w} \otimes \mathbf{1})|0\rangle|0\rangle = \mathbf{u}_1 \mathbf{v}^*_0 \mathbf{C}_{10} \mathbf{w}_1 |0\rangle|0\rangle \ ,$$

showing that an arbitrary 2-qubit state can be realized in terms of a single cNOT and three 1-qubit gates. Here is the equivalent circuit diagram[††]:



[*] By definition $u_{ji} \equiv \langle j|\mathbf{u}|i\rangle$ are the matrix elements of $\mathbf{u}$ with respect to the $|i\rangle$ basis. This means that $\mathbf{u}(\sum_i \alpha_i|i\rangle) = \sum_{i,j} \alpha_i u_{ji}|j\rangle = \sum_{i,j} u_{ij}\alpha_j|i\rangle$, and $\mathbf{u}$ acts to transform the components as $\alpha_i \to \sum_j u_{ij}\alpha_j$.

[†] This also clarifies that $|\Psi\rangle$ is unentangled if and only if one of s_0 or s_1 vanishes, i.e., $\det\alpha = 0$.

[‡] Equivalently, the normalization condition for α implies that $1 = \mathrm{tr}\,\alpha^\dagger\alpha = s_0^2 + s_1^2$

[††] Note that $\mathbf{u}^\dagger \to \mathbf{u}$ and $\mathbf{v} \to \mathbf{v}^*$ with respect to the conventions in the text.