Quantum Computing, Rieffel & Polak Chapter 3

Drs. Charles Tappert and Ron Frank

The information presented here, although greatly condensed, comes almost entirely from the textbook

Chapter 3 – Multiple-Qubit Systems

- The state space of a quantum system grows exponentially with the number of qubits
  - Large state spaces speed computation – main focus of book
- Entangled states are a critical ingredient of quantum computation
  - Most states in a multiple-qubit system are entangled
- Difference between the way classical and quantum states combine
  - Classical uses direct sum of two or more vector spaces
  - Quantum uses the tensor product of a set of vector spaces

Chapter 3 – Multiple-Qubit Systems
3.1 Quantum State Spaces

- In classical physics, the possible states of n objects can be described by vectors in a vector space of 2n dimensions
- In quantum physics, the state space of n quantum systems, each state modeled by a 2D vector, combined through the tensor product is 2^n dimensions

Chapter 3 – Multiple-Qubit Systems
3.1 Quantum State Spaces

The *tensor product* $V \otimes W$ of two vector spaces V and W with bases $A = \{|\alpha_1\rangle, |\alpha_2\rangle, \dots, |\alpha_n\rangle\}$ and $B = \{|\beta_1\rangle, |\beta_2\rangle, \dots, |\beta_m\rangle\}$ is an nm-dimensional vector space with a basis consisting of the nm elements of the form $|\alpha_i\rangle \otimes |\beta_j\rangle$

where $\otimes$ is the tensor product that satisfies

$$(|v_1\rangle + |v_2\rangle) \otimes |w\rangle = |v_1\rangle \otimes |w\rangle + |v_2\rangle \otimes |w\rangle$$

$$|v\rangle \otimes (|w_1\rangle + |w_2\rangle) = |v\rangle \otimes |w_1\rangle + |v\rangle \otimes |w_2\rangle$$

$$(a|v\rangle) \otimes |w\rangle = |v\rangle \otimes (a|w\rangle) = a(|v\rangle \otimes |w\rangle)$$

It is common to write $|v\rangle|w\rangle$ for $|v\rangle \otimes |w\rangle$

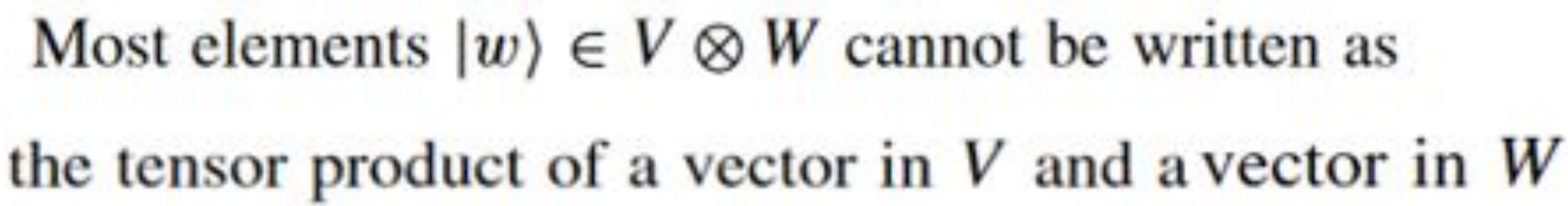
Chapter 3 – Multiple-Qubit Systems
3.1 Quantum State Spaces

If V and W are vector spaces corresponding to a qubit, each with standard basis $\{|0\rangle, |1\rangle\}$, then

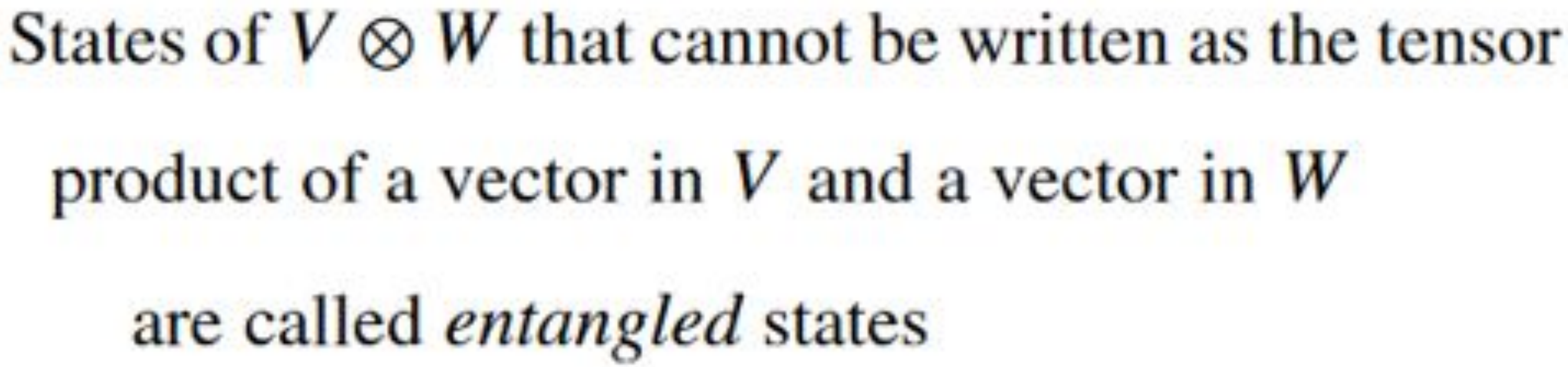
$V \otimes W$ has $\{|0\rangle \otimes |0\rangle, |0\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle, |1\rangle \otimes |1\rangle\}$ as basis

Tensor product of two single-qubit states $a_1|0\rangle + b_1|1\rangle$ and $a_2|0\rangle + b_2|1\rangle$ is $a_1a_2|0\rangle \otimes |0\rangle + a_1b_2|0\rangle \otimes |1\rangle + a_2b_1|1\rangle \otimes |0\rangle + a_2b_2|1\rangle \otimes |1\rangle$

Chapter 3 – Multiple-Qubit Systems
3.1 Quantum State Spaces

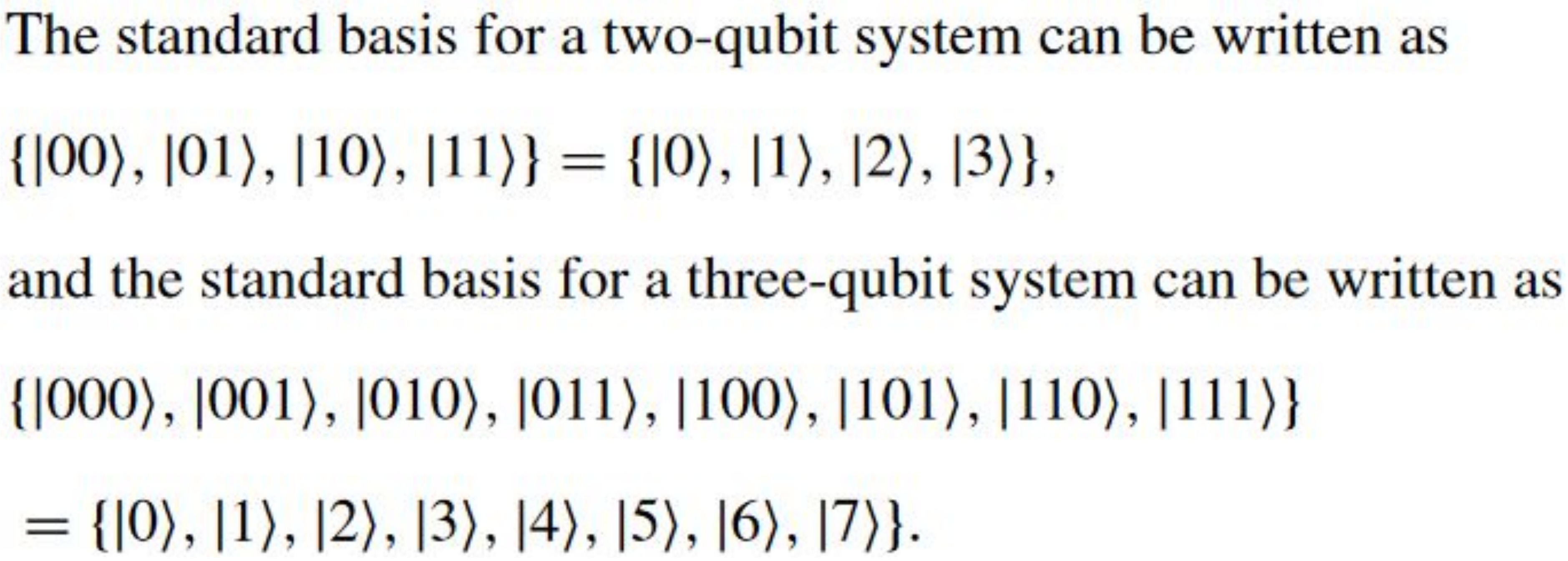


Most elements $|w\rangle \in V \otimes W$ cannot be written as the tensor product of a vector in V and a vector in W



States of $V \otimes W$ that cannot be written as the tensor product of a vector in V and a vector in W are called *entangled* states

Chapter 3 – Multiple-Qubit Systems
3.1 Quantum State Spaces



The standard basis for a two-qubit system can be written as

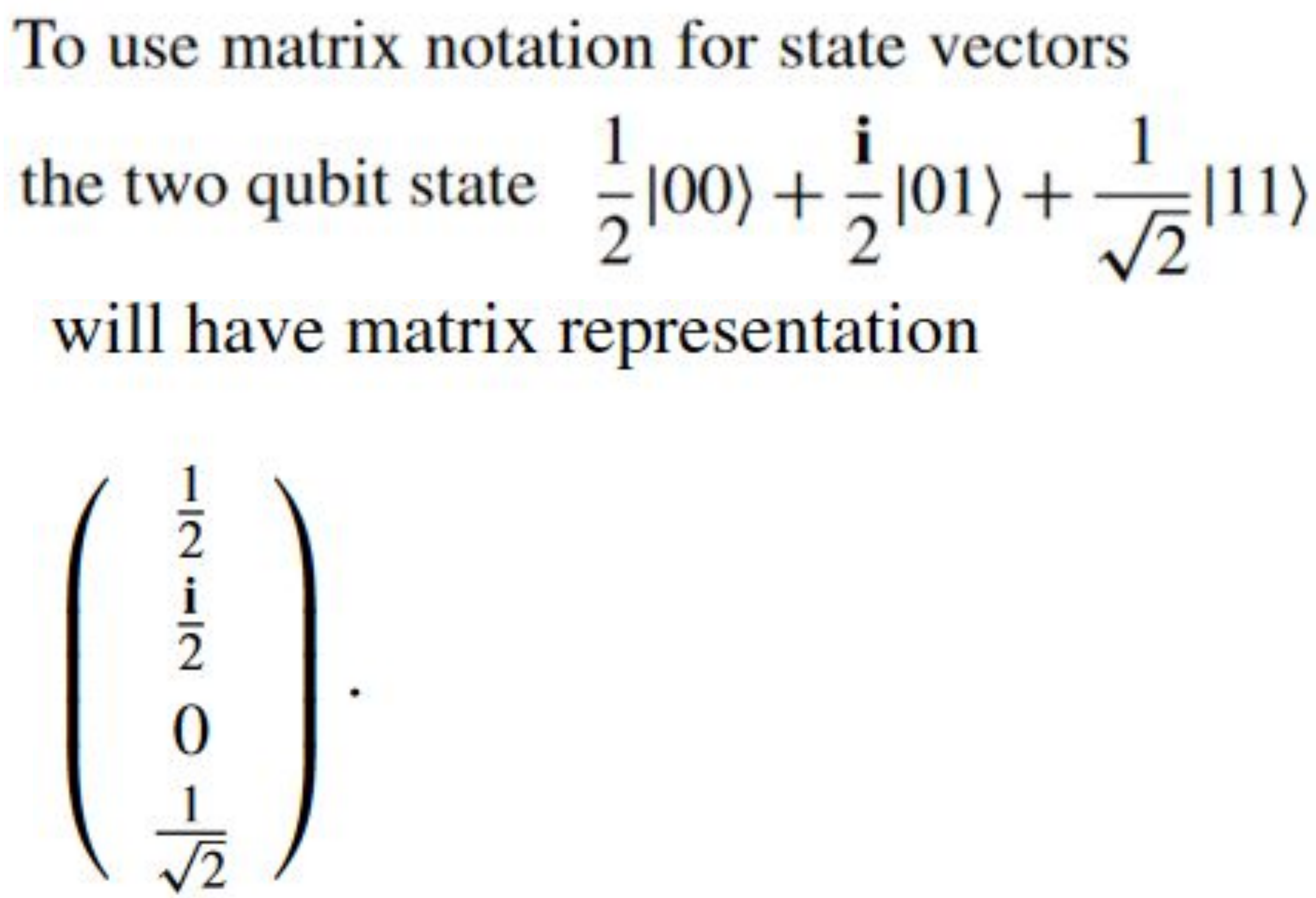
$$\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\} = \{|0\rangle, |1\rangle, |2\rangle, |3\rangle\},$$

and the standard basis for a three-qubit system can be written as

$$\{|000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, |101\rangle, |110\rangle, |111\rangle\}$$

$$= \{|0\rangle, |1\rangle, |2\rangle, |3\rangle, |4\rangle, |5\rangle, |6\rangle, |7\rangle\}.$$

Chapter 3 – Multiple-Qubit Systems
3.1 Quantum State Spaces



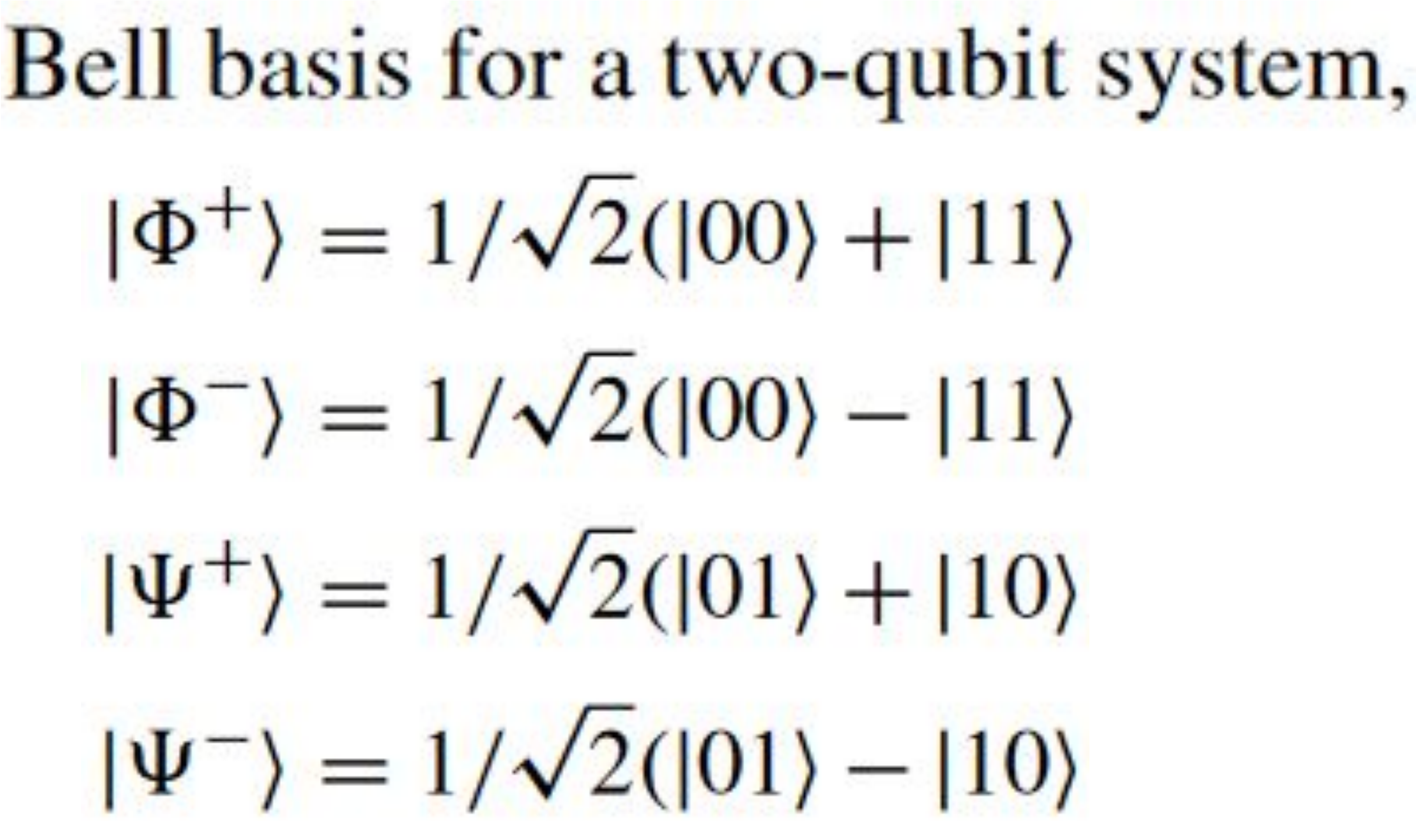
To use matrix notation for state vectors

the two qubit state $\frac{1}{2}|00\rangle + \frac{\mathbf{i}}{2}|01\rangle + \frac{1}{\sqrt{2}}|11\rangle$

will have matrix representation

$$\begin{pmatrix} \frac{1}{2} \\ \frac{\mathbf{i}}{2} \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix}.$$

Chapter 3 – Multiple-Qubit Systems
3.1 Quantum State Spaces



Bell basis for a two-qubit system,

$$|\Phi^+\rangle = 1/\sqrt{2}(|00\rangle + |11\rangle$$

$$|\Phi^-\rangle = 1/\sqrt{2}(|00\rangle - |11\rangle$$

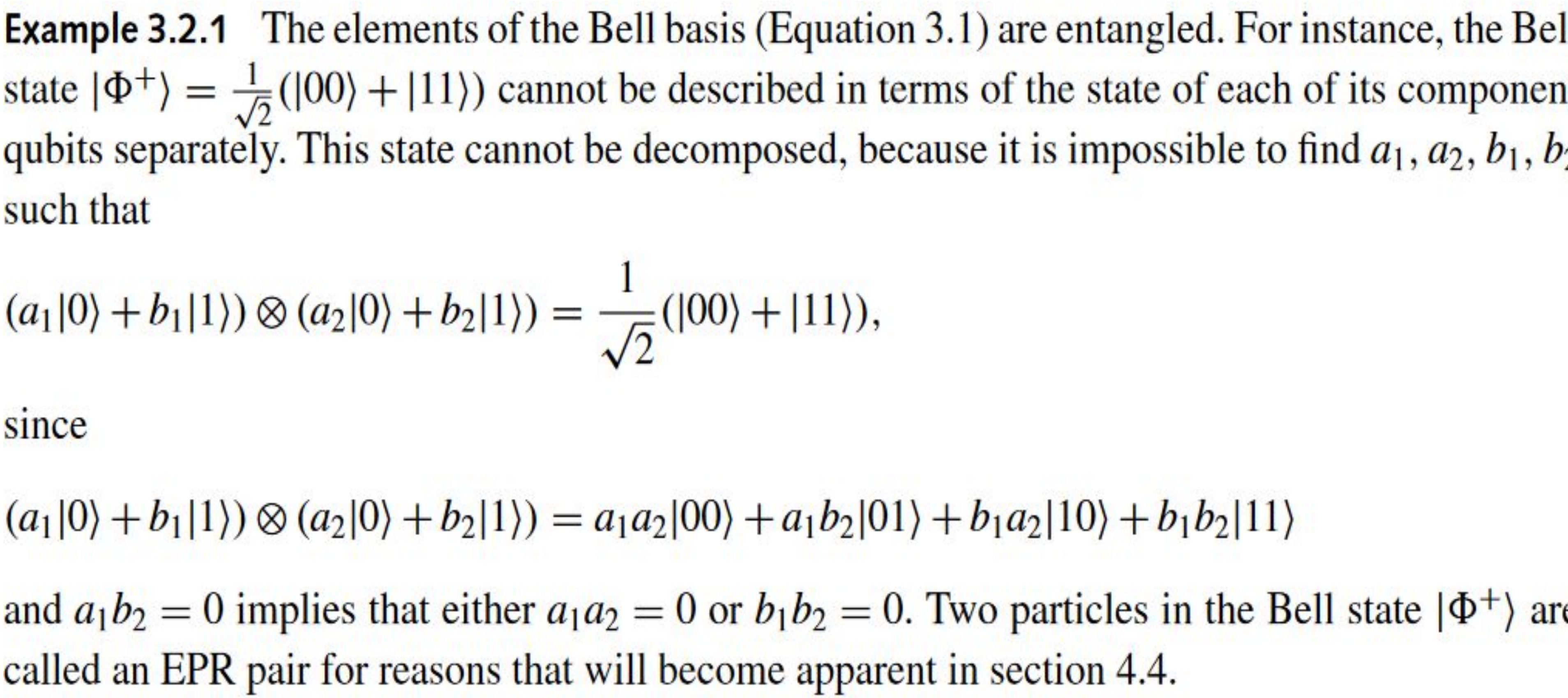
$$|\Psi^+\rangle = 1/\sqrt{2}(|01\rangle + |10\rangle$$

$$|\Psi^-\rangle = 1/\sqrt{2}(|01\rangle - |10\rangle$$

Chapter 3 – Multiple-Qubit Systems
3.2 Entangled States

- States that cannot be written as the tensor product of n single-qubit states are called entangled states
- The vast majority of quantum states are entangled
  - The definition of entanglement has no reference to a basis
- Most n-qubit states are superpositions
  - Nontrivial linear combinations of basis vectors
  - Helpful to think of superpositions as being in multiple states at once

Chapter 3 – Multiple-Qubit Systems
3.2 Entangled States



Example 3.2.1 The elements of the Bell basis (Equation 3.1) are entangled. For instance, the Bel state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ cannot be described in terms of the state of each of its componen qubits separately. This state cannot be decomposed, because it is impossible to find a_1, a_2, b_1, b such that

$$(a_1|0\rangle + b_1|1\rangle) \otimes (a_2|0\rangle + b_2|1\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle),$$

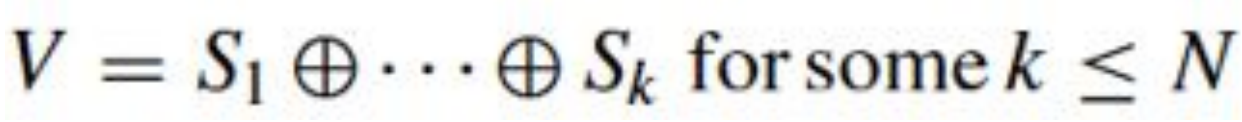
since

$$(a_1|0\rangle + b_1|1\rangle) \otimes (a_2|0\rangle + b_2|1\rangle) = a_1a_2|00\rangle + a_1b_2|01\rangle + b_1a_2|10\rangle + b_1b_2|11\rangle$$

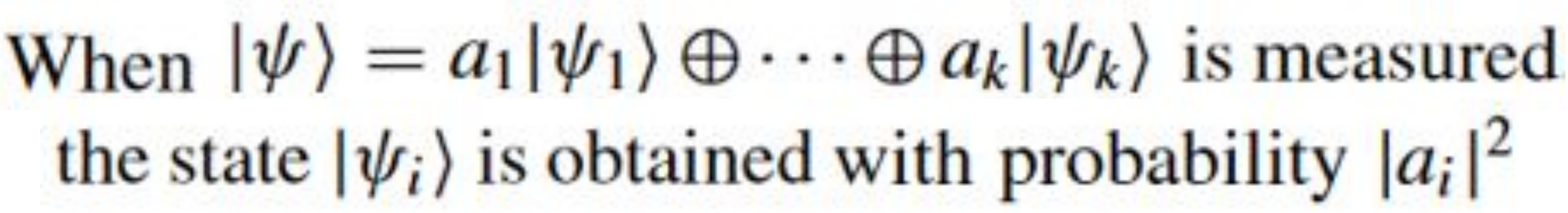
and $a_1b_2 = 0$ implies that either $a_1a_2 = 0$ or $b_1b_2 = 0$. Two particles in the Bell state $|\Phi^+\rangle$ ar called an EPR pair for reasons that will become apparent in section 4.4.

Chapter 3 – Multiple-Qubit Systems
3.3 Basics of Multi-Qubit Measurement

- Measurements of multi-qubit systems is similar to that of single qubit systems, except that the set of possible measurements and outcomes is significantly richer
- Let *V* be the *N=2*^{n} dim vector space of n-qubit system



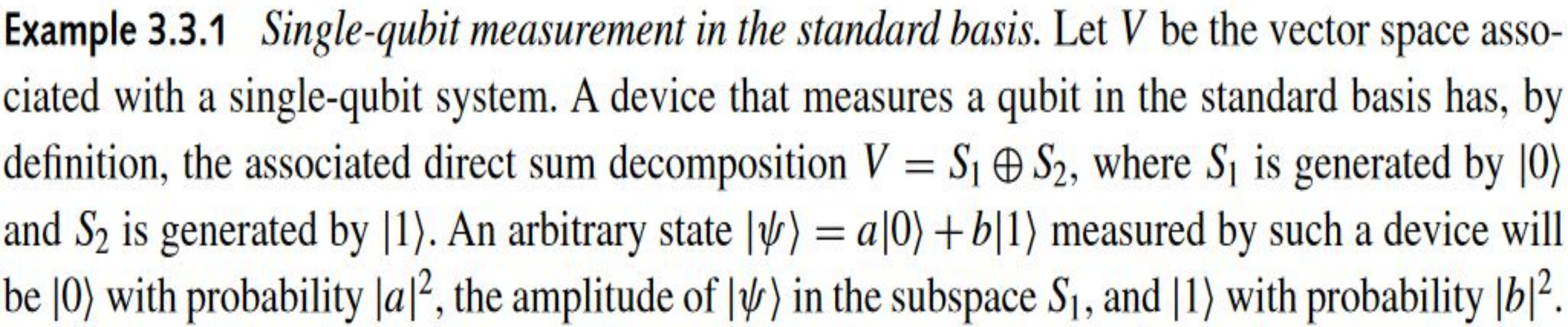
$V = S_1 \oplus \cdots \oplus S_k$ for some $k \leq N$



When $|\psi\rangle = a_1|\psi_1\rangle \oplus \cdots \oplus a_k|\psi_k\rangle$ is measured the state $|\psi_i\rangle$ is obtained with probability $|a_i|^2$

Chapter 3 – Multiple-Qubit Systems

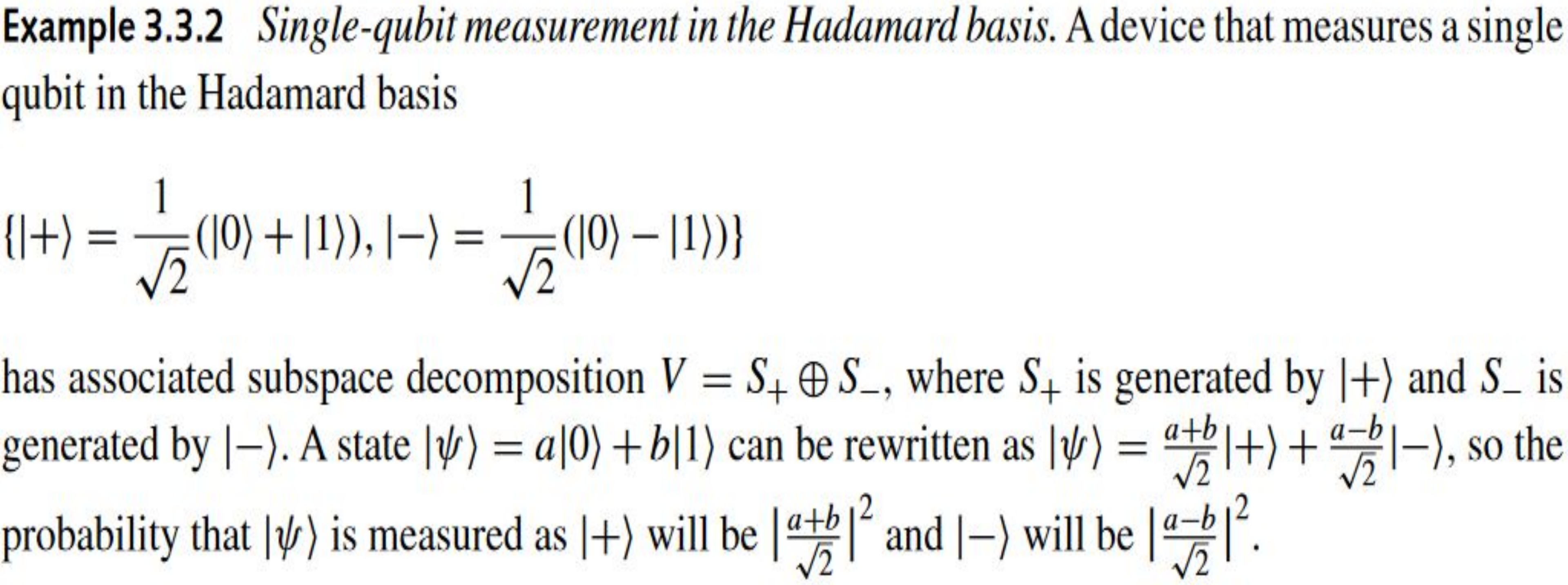
3.3 Basics of Multi-Qubit Measurement



Example 3.3.1 *Single-qubit measurement in the standard basis.* Let V be the vector space associated with a single-qubit system. A device that measures a qubit in the standard basis has, by definition, the associated direct sum decomposition $V = S_1 \oplus S_2$, where S_1 is generated by $|0\rangle$ and S_2 is generated by $|1\rangle$. An arbitrary state $|\psi\rangle = a|0\rangle + b|1\rangle$ measured by such a device will be $|0\rangle$ with probability $|a|^2$, the amplitude of $|\psi\rangle$ in the subspace S_1, and $|1\rangle$ with probability $|b|^2$.

Chapter 3 – Multiple-Qubit Systems

3.3 Basics of Multi-Qubit Measurement



Example 3.3.2 *Single-qubit measurement in the Hadamard basis.* A device that measures a single qubit in the Hadamard basis

$$\{|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$$

has associated subspace decomposition $V = S_+ \oplus S_-$, where S_+ is generated by $|+\rangle$ and S_- is generated by $|-\rangle$. A state $|\psi\rangle = a|0\rangle + b|1\rangle$ can be rewritten as $|\psi\rangle = \frac{a+b}{\sqrt{2}}|+\rangle + \frac{a-b}{\sqrt{2}}|-\rangle$, so the probability that $|\psi\rangle$ is measured as $|+\rangle$ will be $|\frac{a+b}{\sqrt{2}}|^2$ and $|-\rangle$ will be $|\frac{a-b}{\sqrt{2}}|^2$.

Chapter 3 – Multiple-Qubit Systems

3.4 Quantum Key Distribution with Entangled States

- It is easy to prove the security of protocols based on quantum entangled states
- The BB84 protocol described earlier begins with the creation of a sequence of pairs of qubits all in the entangled state

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$