More information about linear algebra, in particular proofs of facts stated here, can be found in any linear algebra text, including Strang's *Linear Algebra and Its Applications* [265] and Hoffman and Kunze's *Linear Algebra* [152], or in a book on mathematics for physicists such as Bamberg and Sternberg's *A Course in Mathematics for Students of Physics* [30].

The BB84 quantum key distribution protocol was developed by Charles Bennett and Gilles Brassard [42, 43, 45] building on work of Stephen Wiesner [284]. A related protocol was shown to be unconditionally secure by Lo and Chau [198]. Their proof was later simplified by Shor and Preskill [255] and extended to BB84. Another proof was given by Mayers [206]. The BB84 protocol was first demonstrated experimentally by Bennett et al. in 1992 over 30 cm of free space [37]. Since then, several groups have demonstrated this protocol and other quantum key distribution protocols over 100 km of fiber optic cable. Bienfang et al. [51] demonstrated quantum key distribution over 23 km of free space at night, and Hughes et al. have achieved distances of 10 km through free space in daylight [156]. See the ARDA roadmap [157], the QIPC strategic report [295], and Gisin et al. [130] for detailed overviews of implementation efforts and the challenges involved. The companies id Quantique, MagiQ, and SmartQuantum currently sell quantum cryptographic systems implementing the BB84 protocol. Other quantum key distribution protocols exist. Exercise 2.11 develops the B92 protocol, and section 3.4 describes Ekert's entanglement-based quantum key distribution protocol.

While we explain all quantum mechanics needed for the topics covered in this book, the reader may be interested in books on quantum mechanics. Countless books on quantum mechanics are available. Greenstein and Zajonc [140] give a readable high-level exposition of quantum mechanics, including descriptions of many experiments. The third volume of the *Feynman Lectures on Physics* [122] is accessible to a large audience. A classical explanation of the polarization experiment is given in the first volume. Shankar's textbook [247] defines much more of the notation and mathematics required for performing calculations than do the previously mentioned books, and it is quite readable as well. Other textbooks, such as Liboff [194], may be more appropriate for readers with a physics background.

## 2.7 Exercises

**Exercise 2.1.** Let the direction $|v\rangle$ of polaroid $B$'s preferred axis be given as a function of $\theta$, $|v\rangle = \cos\theta|{\rightarrow}\rangle + \sin\theta|{\uparrow}\rangle$, and suppose that the polaroids $A$ and $C$ remain horizontally and vertically polarized as in the experiment of Section 2.1.1. What fraction of photons reach the screen? Assume that each photon generated by the laser pointer has random polarization.

**Exercise 2.2.** Which pairs of expressions for quantum states represent the same state? For those pairs that represent different states, describe a measurement for which the probabilities of the two outcomes differ for the two states and give these probabilities.

**a.** $|0\rangle$ and $-|0\rangle$

**b.** $|1\rangle$ and $\mathbf{i}|1\rangle$

c. $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $\frac{1}{\sqrt{2}}(-|0\rangle + \mathbf{i}|1\rangle)$

d. $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

e. $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ and $\frac{1}{\sqrt{2}}(|1\rangle - |0\rangle)$

f. $\frac{1}{\sqrt{2}}(|0\rangle + \mathbf{i}|1\rangle)$ and $\frac{1}{\sqrt{2}}(\mathbf{i}|1\rangle - |0\rangle)$

g. $\frac{1}{\sqrt{2}}(|+\rangle + |-\rangle)$ and $|0\rangle$

h. $\frac{1}{\sqrt{2}}(|\mathbf{i}\rangle - |-\mathbf{i}\rangle)$ and $|1\rangle$

i. $\frac{1}{\sqrt{2}}(|\mathbf{i}\rangle + |-\mathbf{i}\rangle)$ and $\frac{1}{\sqrt{2}}(|-\rangle + |+\rangle)$

j. $\frac{1}{\sqrt{2}}\left(|0\rangle + e^{\mathbf{i}\pi/4}|1\rangle\right)$ and $\frac{1}{\sqrt{2}}\left(e^{-\mathbf{i}\pi/4}|0\rangle + |1\rangle\right)$

**Exercise 2.3.** Which states are superpositions with respect to the standard basis, and which are not? For each state that is a superposition, give a basis with respect to which it is not a superposition.

a. $|+\rangle$

b. $\frac{1}{\sqrt{2}}(|+\rangle + |-\rangle)$

c. $\frac{1}{\sqrt{2}}(|+\rangle - |-\rangle)$

d. $\frac{\sqrt{3}}{2}|+\rangle - \frac{1}{2}|-\rangle)$

e. $\frac{1}{\sqrt{2}}(|\mathbf{i}\rangle - |-\mathbf{i}\rangle)$

f. $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

**Exercise 2.4.** Which of the states in 2.3 are superpositions with respect to the Hadamard basis, and which are not?

**Exercise 2.5.** Give the set of all values of $\theta$ for which the following pairs of states are equivalent.

a. $|1\rangle$ and $\frac{1}{\sqrt{2}}\left(|+\rangle + e^{\mathbf{i}\theta}|-\rangle\right)$

b. $\frac{1}{\sqrt{2}}\left(|\mathbf{i}\rangle + e^{\mathbf{i}\theta}|-\mathbf{i}\rangle\right)$ and $\frac{1}{\sqrt{2}}\left(|-\mathbf{i}\rangle + e^{-\mathbf{i}\theta}|\mathbf{i}\rangle\right)$

c. $\frac{1}{2}|0\rangle - \frac{\sqrt{3}}{2}|1\rangle$ and $e^{\mathbf{i}\theta}\left(\frac{1}{2}|0\rangle - \frac{\sqrt{3}}{2}|1\rangle\right)$

**Exercise 2.6.** For each pair consisting of a state and a measurement basis, describe the possible measurement outcomes and give the probability for each outcome.

a. $\frac{\sqrt{3}}{2}|0\rangle - \frac{1}{2}|1\rangle$, $\{|0\rangle, |1\rangle\}$

**b.** $\frac{\sqrt{3}}{2}|1\rangle - \frac{1}{2}|0\rangle, \{|0\rangle, |1\rangle\}$

**c.** $|-\mathbf{i}\rangle, \{|0\rangle, |1\rangle\}$

**d.** $|0\rangle, \{|+\rangle, |-\rangle\}$

**e.** $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \{|\mathbf{i}\rangle, |-\mathbf{i}\rangle\}$

**f.** $|1\rangle, \{|\mathbf{i}\rangle, |-\mathbf{i}\rangle\}$

**g.** $|+\rangle, \{\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle, \frac{\sqrt{3}}{2}|0\rangle - \frac{1}{2}|1\rangle\}$

**Exercise 2.7.** For each of the following states, describe all orthonormal bases that include that state.

**a.** $\frac{1}{\sqrt{2}}(|0\rangle + \mathbf{i}|1\rangle)$

**b.** $\frac{1+\mathbf{i}}{2}|0\rangle - \frac{1-\mathbf{i}}{2}|1\rangle$

**c.** $\frac{1}{\sqrt{2}}\left(|0\rangle + e^{\mathbf{i}\pi/6}|1\rangle\right)$

**d.** $\frac{1}{2}|+\rangle - \frac{\mathbf{i}\sqrt{3}}{2}|-\rangle$

**Exercise 2.8.** Alice is confused. She understands that $|1\rangle$ and $-|1\rangle$ represent the same state. But she does not understand why that does not imply that $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ would be the same state. Can you help her out?

**Exercise 2.9.** In the BB84 protocol, how many bits do Alice and Bob need to compare to have a 90 percent chance of detecting Eve's presence?

**Exercise 2.10.** Analyze Eve's success in eavesdropping on the BB84 protocol if she does not even know which two bases to choose from and so chooses a basis at random at each step.

**a.** On average, what percentage of bit values of the final key will Eve know for sure after listening to Alice and Bob's conversation on the public channel?

**b.** On average, what percentage of bits in her string are correct?

**c.** How many bits do Alice and Bob need to compare to have a 90 percent chance of detecting Eve's presence?

**Exercise 2.11.** *B92 quantum key distribution protocol.* In 1992 Bennett proposed the following quantum key distribution protocol. Instead of encoding each bit in either the standard basis or the Hadamard basis as is done in the BB84 protocol, Alice encodes her random string $x$ as follows

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

and sends them to Bob. Bob generates a random bit string $y$. If $y_i = 0$ he measures the $i$ th qubit in the Hadamard basis $\{|+\rangle, |-\rangle\}$, if $y_i = 1$ he measures in the standard basis $\{|0\rangle, |1\rangle\}$. In this protocol, instead of telling Alice over the public classical channel which basis he used to measure