Chapter 13
Quantum Information

13.1 Conceptual Framework

Assume for a moment that the Hilbert space is restricted to the pure basis states.[1] For a single qubit, the only available states would thus be the two states (12.1). For n qubits, there are 2^n orthogonal product vectors $\varphi_i^{(n)}$ in a space of 2^n dimensions. Classical computation operates in this space. Linear combinations of vectors are not allowed. Therefore, the only operations that can be performed are permutations between the basis states (unless the size of the space is changed).

Quantum mechanics allows for superpositions $\Psi^{(n)}$ of the basis vectors $\varphi_i^{(n)}$ with complex amplitudes c_i (2.6). Quantum operations are only limited by the requirement of unitarity, i.e. the norm of the state should be preserved. Therefore, classical states and classical operations constitute sets of vanishingly small size relative to those sets encompassing quantum states and quantum operations. Thus, quantum information offers a wealth of new possibilities: all kinds of interference effects may take place in the much larger space, much faster calculations can be performed if all components of the state vector work in parallel, and so on. Quite typically, the time for solving a problem may increase either exponentially or polynomially with its complexity. By taking advantage of interference and entanglement, a problem with an exponential increase in a classical computer may be transformed into a problem with polynomial increase in the quantum case.

However, this promising picture is limited by the fact that it is very difficult to extract anything from the state vector $\Psi^{(n)}$, despite the immense amount of information that it carries. In fact, the only way is to perform a measurement, which relates $\Psi^{(n)}$ to a single probability $|c_i|^2$. Therefore, the strategy consists in producing transformations that lead to a state $(\Psi')^{(n)}$, in which very few amplitudes c_i' do not vanish.

A quantum process starts with the preparation of the system in some initial state $\varphi_0^{(n)}$ (i.e. with a measurement) and ends with another measurement in the final

[1] See also Mermin's presentation [22].

D. Bes, *Quantum Mechanics*, Graduate Texts in Physics,
DOI 10.1007/978-3-642-20556-9_13, © Springer-Verlag Berlin Heidelberg 2012

state $\varphi_f^{(n)}$ (see Sects. 2.4 and 2.5). Measurements are a class of transformations that provide classical information but change the state irreversibly. Between any two measurement operations, quantum transformations are unitary operations that change the state of the system in a deterministic and reversible way. A quantum algorithm is a unitary operation that may be represented by successive unitary operations (9.7) – quantum gates (Sect. 13.5*).

A collection of n qubits is called a quantum register of size n. We assume that information is stored in the register in binary form. An n-register can store the numbers $J = 0, 1, \ldots, (2^n - 1)$. A quantum register of size 1 can store the numbers 0 and 1; of size 2, the numbers 0,1,2 and 3; etc.

We do not attempt to give a complete description of the recent developments on quantum information. Rather, we use the respectable knowledge of quantum mechanics which readers should now have to illustrate these new uses with pertinent examples: quantum cryptography (Sect. 13.2); teleportation (Sect. 13.3) and quantum computation (Sect. 13.4†).

A presentation of the most common gates used in quantum information processes is made in Sect. 13.5*.

13.2 Quantum Cryptography

Traditional strategies for keeping secrets in the distribution of cryptographic keys depend on human factors, so their safety is difficult to assess. As a consequence, they have been replaced to a large extent by cryptosystems. A cryptographic key is transmitted through a succession of numbers 0 and 1. Their present safety is due to the fact that, with classical computers, no fast algorithms can work out the decomposition of a large number in prime factors. However, this statement may no longer be true with the advent of quantum computation (see Sect. 13.4†). Hence the continuing interest in exploring safer systems for transmission of cryptographic keys. In this section, we show that the quantum key distributions are impossible to break, and that this impossibility arises from fundamental quantum laws.

A well-known protocol is called BB84 [89]: every actor involved is provided with a filter of the type discussed in Sect. 2.5.1. The encoder (usually named Alice) can send particles that are in an eigenstate of either $\hat{S}_z$ or $\hat{S}_x$. We label the corresponding states by φ_0, φ_1, χ_0, χ_1. The decoder (frequently called Bob) may orient his detection equipment along either the z- or the x-direction. For instance, if Alice has sent three qubits that are polarized according to $\uparrow z$, $\uparrow x$ and $\downarrow x$, and if Bob aligns his apparatus in the z-direction for the first qubit and the x-direction for the last two, he will detect intensities 1, 1 and 0 with certainty. These are the good qubits, i.e. those sent and measured with both pieces of apparatus along the same orientation. If Alice sends a qubit in the φ_0 state while Bob orients his equipment towards the x-direction, he may detect the intensities 1 or 0 with equal probability. Bad qubits are those in which the sender and receiver apparatus have different orientations.

For each qubit sent, Alice records the eigenvalue as well as the orientation of her filter. Bob selects his orientations at random and informs Alice of them. With this knowledge, Alice can tell Bob which ones are good qubits, the ones which are kept in order to codify the message. Both messages from Bob and Alice can even be made over an open phone, since they carry no information useful for a third party.

Let us assume that there is an eavesdropper, usually called Eve. Eve cannot be prevented from eavesdropping, but if she does, Alice and Bob will know: let us assume that Alice has sent a qubit in the φ_1 state, that Eve's apparatus is in orientation x, and Bob's in orientation z. Eve's measurement increases the probability that Bob will detect the particle from 0 to $1/4$ [$= |\langle\varphi_1|\chi_0\rangle\langle\chi_0|\varphi_0\rangle|^2$, see (3.21)]. Bob chooses a random subset of the good qubits that he has retained, and communicates them to Alice, also publicly. Alice may find discrepancies between her notes and Bob's message. If she does not, all good qubits constitute a perfect secret between Alice and Bob.

Quantum cryptography applies the rule that quantum states are perturbed by the act of measurement, unless the observer knows in advance what observables can be measured without being perturbed (Sect. 2.4). Eve cannot succeed without knowing the basis common to both Alice and Bob.

Commercial equipment for bank transfers by means of quantum cryptography is available, within city boundaries.

13.3 Teleportation

Alice and Bob are at a macroscopic distance from each other. Alice's particle is initially in the Ψ_c state

$$\Psi_c = c_0\varphi_0 + c_1\varphi_1 \,. \tag{13.1}$$

The objective is to put Bob's particle in the same state, but without transporting the particle or sending any classical information about it.

Alice and Bob start by each taking one of the two qubits which have been prepared, for instance in the Bell state φ_{B_0} (12.5). Alice now has two qubits, one in the state Ψ_c and the other in the Bell state (see Fig. 13.1). The three-qubit state can be written as

$$\begin{aligned}
\Psi^{(3)} &= \Psi_c\varphi_{B_0} \\
&= \frac{1}{\sqrt{2}}\left(c_0\varphi_0\varphi_0\varphi_0 + c_0\varphi_0\varphi_1\varphi_1 + c_1\varphi_1\varphi_0\varphi_0 + c_1\varphi_1\varphi_1\varphi_1\right) \qquad (13.2)\\
&= \frac{1}{2}\left[\varphi_{B_0}\begin{pmatrix} c_0 \\ c_1 \end{pmatrix} + \varphi_{B_1}\begin{pmatrix} c_0 \\ -c_1 \end{pmatrix} + \varphi_{B_2}\begin{pmatrix} c_1 \\ c_0 \end{pmatrix} + \varphi_{B_3}\begin{pmatrix} -c_1 \\ c_0 \end{pmatrix}\right],
\end{aligned}$$

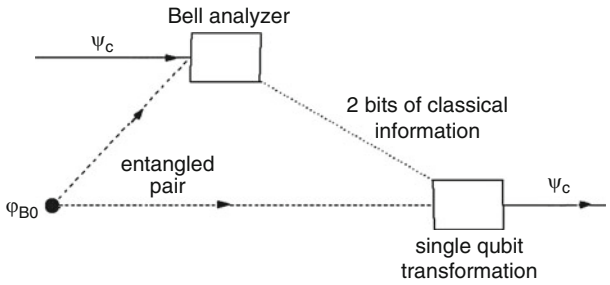

Fig. 13.1 Scheme illustrating the process of teleportation. *Dashed lines* represent entangled qubits in the state φ_{B_0}, while the *dotted line* indicates that classical information is transmitted

where the qubit taken by Bob from the Bell state has been explicitly separated and the two qubits in Alice's posesion have been expressed in terms of Bell states.

Alice now filters her two qubits into a well-defined Bell state (Problem 10). Simultaneously, Bob's qubit is also projected into a well-defined state, but Bob ignores the relation between this state and the initial state Ψ_c. Bob needs to know in which Bell state the system has collapsed to reconstruct the original qubit. This information must be provided by Alice by conventional means, i.e. at a speed less than or equal to the velocity of light.

Suppose, for instance, that instead of going through the previous procedure, Alice constructs the state Ψ_c by filtering the spin, and sends the information about the alignment axis to Bob, who can thus filter the particle in the same direction. Are there still advantages in teleportation? The answer is affirmative, for the following reasons:

- The teleported state Ψ_c might not be known by Alice. If she attempts to measure it, the state of the qubit could be changed.
- Bob receives complete information about Alice's qubit at the expense of that qubit: in quantum teleportation the original qubit is destroyed. This is a manifestation of the no-cloning theorem (Sect. 2.6.2).
- The qubit Ψ_c is determined by the amplitudes c_0, c_1, for which the transmission time increases with the required precision. Now the results of the quantum experiments are discrete numbers. In quantum teleportation, discrete information about the Bell state is transformed into continuous information about the state of the qubit.

Quantum teleportation was discovered in 1993 [90]. It was observed for the first time in 1997 with entangled photons [91].

13.4† Quantum Computation

We describe the factorization procedure as one of the few "best typical" examples of the still unharnessed power of quantum computers.[2] Note that the security of widely used encryption codes rests on the present practical impossibility of breaking a large number N in its prime factors, using classical computers.

13.4.1† Factorization

Factorization of a number in its prime components makes use of the following property: Let a be coprime with N (no common factors) and define the function

$$f_{aN}(J) \equiv a^J, \bmod N. \tag{13.3}$$

This function has at least two important properties:

- It is periodic. For instance, if $a = 2$, $N = 15$, the successive values of the function f are $1, 2, 4, 8, 1, 2$ and so on. Thus, the period $P = 4$.
- Provided that P is even, the greatest common divisors of the pairs $(a^{P/2} + 1, \bmod N)$ and $(a^{P/2} - 1, \bmod N)$ are factors of N. In the present example, they are 5 and 3, respectively.

The level of complexity in the calculation of the period using a classical computer is as large as any other factorization algorithm. By contrast, there exists the following quantum algorithm due to Schor [93]:

1. The operation makes use of a control register (left) and a target register (right). Start the operation with both registers in the state with $J = 0$ [all qubits in the φ_0 state (13.25)]
$$\Psi_1^{(n)} = \varphi_0^{(n)} \varphi_0^{(n)}. \tag{13.4}$$
2. Load the control register with the integer series (13.26)
$$\Psi_2^{(n)} = 2^{-n/2} \sum_{J=0}^{J=2^n-1} \varphi_J^{(n)} \varphi_0^{(n)}. \tag{13.5}$$
3. Select a value for a (coprime to N) and place the remainder $f_{aN}(J)$ in the target register, as in (13.27)
$$\Psi_3^{(n)} = 2^{-n/2} \sum_{J=0}^{J=2^n-1} \varphi_J^{(n)} \varphi_{f_{aN}(J)}^{(n)}. \tag{13.6}$$

[2]The contents of this section have been mainly extracted from [92].

For $n = 4$ and the previous example, $\Psi_3^{(n)}$ takes the value

$$\frac{1}{4}\left(\varphi_0^{(4)} + \varphi_4^{(4)} + \varphi_8^{(4)} + \varphi_{12}^{(4)}\right)\varphi_1^{(4)} + \frac{1}{4}\left(\varphi_1^{(4)} + \varphi_5^{(4)} + \varphi_9^{(4)} + \varphi_{13}^{(4)}\right)\varphi_2^{(4)} + \frac{1}{4}\left(\varphi_2^{(4)} + \varphi_6^{(4)} + \varphi_{10}^{(4)} + \varphi_{14}^{(4)}\right)\varphi_4^{(4)} + \frac{1}{4}\left(\varphi_3^{(4)} + \varphi_7^{(4)} + \varphi_{11}^{(4)} + \varphi_{15}^{(4)}\right)\varphi_8^{(4)}. \tag{13.7}$$

Thus, the period $P = 4$ is encoded in each of the superposition states representing the control register.

4. Measure the target register. This information yields one value $\chi = f_{aN}(J)$ and destroys the information about the others. According to (2.18) we retain only the terms $\varphi_J^{(n)}$ in the control register that are multiplied by $\varphi_\chi^{(n)}$

$$\Psi_4^{(n)} = \frac{1}{\sqrt{2^n/P}}\left(\sum_{r=0}^{r=2^n/P-1} \varphi_{J=rP+q}^{(n)}\right)\varphi_\chi^{(n)}, \tag{13.8}$$

where we have assumed that $2^n/P$ is an integer,[3] as in (13.7).

5. The residue q must be eliminated in order to find the period. To do so we perform a Fourier transform on the control register

$$\begin{aligned}\Psi_5^{(n)} &= \mathcal{U}_{\mathrm{FT}}^{(\mathrm{ctrl})}\,\Psi_4^{(n)} \\ &= \frac{\sqrt{P}}{2^n}\left(\sum_{K=0}^{K=2^n-1}\sum_{r=0}^{r<2^n/P} \exp[\mathrm{i}K(rP+q)\pi/2^{(n-1)}]\varphi_K^{(n)}\right)\varphi_\chi^{(n)} \\ &= \left(\sum_{r=0}^{r<2^n/P} c_{\chi,rP}\,\varphi_{rP}^{(n)}\right)\varphi_\chi^{(n)}.\end{aligned} \tag{13.9}$$

The last step relies on the vanishing of the factor

$$\sum_{r=0}^{r<2^n/P} \exp[\mathrm{i}K(rP)\pi/2^{(n-1)}], \tag{13.10}$$

unless K is zero or an integer multiple of $2^n/P$, if P is an integer divisor of 2^n. Accordingly, the Fourier transform of (13.7) yields

$$\left(c_{i0}\varphi_0^{(4)} + c_{i4}\varphi_4^{(4)} + c_{i8}\varphi_8^{(4)} + c_{i12}\varphi_{12}^{(4)}\right)\varphi_\chi^{(4)}, \tag{13.11}$$

where all subindexes in the control register are multiples of the period.

[3] The procedure can be extended if this is not the case.

6. Measure the control system.
7. Repeat the operation until the period becomes established.

The number ν of bit operations required to factor the number N with a classical computer is expected to increase with N no less rapidly than

$$\nu(N) = \exp\left[1.32\, L^{1/3}\ (\log_2 L)^{2/3}\right], \tag{13.12}$$

where $L = \log_2 N$ is essentially the number of bits required to represent N. The number ν_q of universal quantum gates needed to implement Schor's algorithm has been estimated to be

$$\nu_q(N) = L^2\ (\log_2 L)\ (\log_2 \log_2 L)\,. \tag{13.13}$$

Thus, the factorization is transformed from a problem in which time increases exponentially, to a problem in which it increases only polynomially. It has been estimated that the factorization time of a 400-digit number can be reduced from the age of the universe to a few years [77].

A variety of two-level quantum systems has been considered. Modern experimental techniques allow us to orient their spins (or equivalent observables) and to implement the gates. However, the situation becomes drastically more complicated when operating a large scale computer, combining many gates. The greatest problems lie in alteration of states due to decoherence, i.e. the unavoidable coupling with a surrounding medium (Sect. 14.2†). Up to now, the successes of quantum computation have been limited to the decomposition of small numbers into their prime factors [94]. The number of operational qubits can still be expressed with one digit, while many thousand qubits would be neeeded for the envisaged applications.

It is true that we cannot ignore the example of the path traveled "from the Pascal machine to the Pentium processor." There exist new strategies for partially controlling the effects of decoherence. For instance, by redundancy. The fact that this problem is linked to defence and financial activities has undoubtedly contributed to intense endeavors on the subject. But we should bear in mind that the interest in quantum computing is not limited to those applications: the physics involved in experiments with entangled particles is helping us to obtain a better understanding of the most fundamental aspects of quantum mechanics.

13.5* Quantum Gates

A quantum gate is a device that performs a unitary transformation on selected qubits at a certain time. A quantum network is a device consisting of quantum gates that are synchronized in time.

It can be proved that any unitary operation in a system of qubits may be reproduced by a sequence of one- and two-qubit operations, which constitutes a practical advantage from the engineering point of view. Manipulations of a single qubit may be performed by controlling a magnetic field at its site (Sect. 9.2). Simultaneous manipulations of two qubits require an interaction between them. Therefore we use a controlling Hamiltonian

$$\hat{H}_{\text{ctr}} = -\mu_s \sum_{i}^{N} \boldsymbol{B}^{(i)}(t)\cdot\hat{\boldsymbol{S}}^{(i)} + \sum_{\substack{a,b \\ i\neq j}} J_{ab}^{(i,j)}(t)\hat{S}_a^{(i)}\hat{S}_b^{(j)} \ , \tag{13.14}$$

where summation over space indices $a, b = x, y, z$ is understood (see Problem 9 in Chap. 6 and Problem 7 in Chap. 9). This Hamiltonian satisfies the requirements for controlling a quantum computer. In fact, it even exceeds them. The Hadamard gate, all the phase gates and the controlled-NOT gate constitute a universal set of gates, although this set is not unique. Any transformation between the n-states of a register may be constructed from them.

Interactions with the measurement device and with the environment should also be taken into account.

13.5.1 One-Qubit Systems*

The Hadamard gate $\mathcal{U}_{\text{H}}$ and the phase gate $\mathcal{U}_{\phi}(\beta)$ transform the one-qubit states through the operations[4]

$$\mathcal{U}_{\text{H}}\,\varphi_J = \frac{1}{\sqrt{2}}\sum_{K=0}^{K=1}\exp(\mathrm{i}JK\pi)\varphi_K \ , \qquad J = 0, 1,$$

$$\mathcal{U}_{\text{H}}\,\varphi_0 = \frac{1}{\sqrt{2}}(\varphi_0 + \varphi_1) \ , \qquad \mathcal{U}_{\text{H}}\,\varphi_1 = \frac{1}{\sqrt{2}}(\varphi_0 - \varphi_1) \ . \tag{13.15}$$

The phase gate adds a phase to the state φ_1.

$$\mathcal{U}_{\phi}(\beta)\,\varphi_J = \exp(\mathrm{i}J\beta)\varphi_J \ . \tag{13.16}$$

These two operations are sufficient to construct any unitary operation on a single qubit, since

[4] We keep the quantum mechanical notation previously used in this text. In computation texts, the Hadamard gate is denoted by H, successive transformations are read from left to right, and so on. Overall phases are frequently disregarded.

$$\mathcal{U}_\phi(\eta+\pi/2)\,\mathcal{U}_{\rm H}\,\mathcal{U}_\phi(\beta)\,\mathcal{U}_{\rm H}\varphi_0 = \varphi_0\cos\frac{\beta}{2} + \varphi_1\exp(\mathrm{i}\eta)\sin\frac{\beta}{2}\,, \tag{13.17}$$

up to a phase. This expression is the most general form for a qubit.

A qubit is manipulated by acting with the first term in (13.14). Switching on the z- or x-component of the magnetic field during a time τ introduces the transformations $\mathcal{U}_z(\beta/2)$ and $\mathcal{U}_x(\beta/2)$. They are given by (9.14) and (9.17), respectively, with $\beta = \omega_{\rm L}\tau$.

The Hadamard gate and the phase gate can be constructed by means of the following operations:

$$\mathcal{U}_{\rm H} = \mathcal{U}_z(\pi/2)\,\mathcal{U}_x(\pi/2)\,\mathcal{U}_z(\pi/2) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \tag{13.18}$$

$$\mathcal{U}_\phi(\beta) = \mathcal{U}_z(-\beta) = \begin{pmatrix} 1 & 0 \\ 0 & \exp(\mathrm{i}\beta) \end{pmatrix}. \tag{13.19}$$

We obtain expressions (13.15) upon application of matrices (13.18) and (13.19) to column states (12.1).

13.5.2 Two-Qubit Systems*

The two-qubit states can be represented as products of single qubits $\varphi_J(1)\varphi_K(2)$ or in the computational basis $\varphi_J^{(2)}$, with $J = 0, 1, 2, 3$. Any effect upon them of the Pauli principle is ignored, since they are separated in space and thus distinguishable.

Successive application of the Hadamard gate on the state $\varphi_0^{(2)}$ yields

$$\mathcal{U}_{\rm H}(2)\,\mathcal{U}_{\rm H}(1)\,\varphi_0^{(2)} = \mathcal{U}_{\rm H}(2)\frac{1}{\sqrt{2}}\left(\varphi_0^{(2)} + \varphi_1^{(2)}\right) = \frac{1}{2}\sum_{J=0}^{J=3}\varphi_J^{(2)}. \tag{13.20}$$

Useful gates acting on two-qubit systems are the controlled-NOT gate $\mathcal{U}_{\rm CNOT}$ and the controlled-phase gate $\mathcal{U}_{\rm CB}(\phi)$

$$\begin{aligned} \mathcal{U}_{\rm CNOT}\,\varphi_J\,\varphi_K &= \varphi_J\,\varphi_{J\oplus K}, \\ \mathcal{U}_{\rm CB}(\phi)\,\varphi_J\,\varphi_K &= \exp[\mathrm{i}JK\phi]\,\varphi_J\,\varphi_K\,, \end{aligned} \tag{13.21}$$

where the symbol $\oplus$ denotes the summation $(J + K)$ modulo 2. These two gates apply a single-qubit transformation to the target qubit if the control qubit is in the state φ_1, and do nothing if the control qubit is in the state φ_0. The control bit remains unchanged, but its states determine the evolution of the target.

The controlled-NOT and the controlled-phase gates are expressed, in matrix form

$$\mathcal{U}_{\text{CNOT}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}; \quad \mathcal{U}_{\text{CB}}(\phi) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \exp(\mathrm{i}\phi) \end{pmatrix}. \tag{13.22}$$

The construction of the controlled-NOT and controlled-phase gates starting from the Hamiltonian (13.14) has been omitted from this presentation.

Combining these operations yields the discrete Fourier transformation

$$\begin{aligned} \mathcal{U}_{\text{FT}}\, \varphi_J^{(2)} &= \frac{1}{2} \sum_{K=0}^{K=3} \exp[\mathrm{i} JK\pi/2]\, \varphi_K^{(2)}, \\ \mathcal{U}_{\text{FT}} &= \mathcal{U}_{\text{SWAP}} \left(\frac{\pi}{2}\right) \mathcal{U}_{\text{H}}^{(\text{targ})}\, \mathcal{U}_{\text{CB}} \left(\frac{\pi}{2}\right) \mathcal{U}_{\text{H}}^{(\text{ctrl})} \\ &= \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & \mathrm{i} & -1 & -\mathrm{i} \\ 1 & -1 & 1 & -1 \\ 1 & -\mathrm{i} & -1 & I \end{pmatrix}, \end{aligned} \tag{13.23}$$

where the SWAP transformation interchanges the values of the control and target bits

$$\begin{aligned} \mathcal{U}_{\text{SWAP}}\, \varphi_J(1)\, \varphi_K(2) &= \varphi_K(1)\, \varphi_J(2) \\ \mathcal{U}_{\text{SWAP}} &= \mathcal{U}_{\text{CNOT}} \mathcal{U}_{\text{H}}^{\text{ctr}} \mathcal{U}_{\text{H}}^{\text{tag}} \sqcap_{\text{CNOT}} \mathcal{U}_{\text{H}}^{\text{tag}} \mathcal{U}_{\text{H}}^{\text{ctr}} \mathcal{U}_{\text{CNOT}} \\ &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \end{aligned} \tag{13.24}$$

13.5.3 n-Qubit Systems*

As for the one- and two-qubit cases, we may use either the product or the column representation. In most applications the initial state is

$$\varphi_0^{(n)} = \prod_{k=1}^{k=n} \varphi_0(k). \tag{13.25}$$

The transformations (13.20), (13.21) and (13.24) may be generalized to the case of n-qubits

$$\Pi_{k=1}^{k=n}\mathcal{U}_H(k)\,\varphi_0^{(n)} = \frac{1}{\sqrt{2^n}}\sum_{J=0}^{J=2^n-1}\varphi_J^{(n)}. \tag{13.26}$$

If the control and target are n-registers, operation (13.21) becomes

$$\mathcal{U}\varphi_J^{(n)}\varphi_K^{(n)} = \varphi_J^{(n)}\varphi_{K\oplus J}^{(n)}\,, \qquad \mathcal{U}_f\,\varphi_J^{(n)}\varphi_K^{(n)} = \varphi_J^{(n)}\varphi_{K\oplus f(J)}^{(n)}\,, \tag{13.27}$$

where the symbol $\oplus$ in the first equation (13.21) denotes summation modulo 2^n and a function $f(J)$ is defined mapping the number J into another number that may be stored by an n-register.

The discrete Fourier transformation (13.23) is generalized as

$$\mathcal{U}_{\mathrm{FT}}\varphi_J^{(n)} = 2^{-n/2}\sum_{K=0}^{K=2^n-1}\exp[\mathrm{i}JK\pi/2^{(n-1)}]\varphi_K^{(n)}\,. \tag{13.28}$$

All components of the state vector work in parallel using the gates described above.

Problems

Problem 1. Find the eigenvalues of the product operators $\hat{S}_z(1)\,\hat{S}_z(2)$ and $\hat{S}_x(1)\,\hat{S}_x(2)$ for each Bell state.

Problem 2. Alice and Bob share a good qubit (Sect. 13.2). Assume that Alice sends the qubit in the state φ_0. Determine the probability that Bob detects the intensity 1 if:

1. There is no eavesdropper and Bob's detector is aligned with the z-axis.
2. There is no eavesdropper and Bob's detector is antialigned with the z-axis.
3. There is no eavesdropper and Bob's detector is oriented at random.
4. Eve is active and Bob's detector is aligned with the z-axis.
5. Eve is active and Bob's detector is antialigned with the z-axis.
6. Eve is active and Bob's detector is oriented at random.

Problem 3. Find the generators of rotations that Bob has to perform in order to obtain the original qubit for each Bell state that Alice may have detected (Sect. 13.3).

Problem 4. Express the Fourier transform of a single qubit in terms of universal gates.

Problem 5. Show that $\mathcal{U}_x(\pi)\,\mathcal{U}_z(\beta)\,\mathcal{U}_x(-\pi) = \mathcal{U}_z(-\beta)$.

Problem 6. Show that $\dfrac{\hbar}{2}\mathcal{U}_{\text{CNOT}}\,\hat{S}_x^{(\text{ctrl})}\,\mathcal{U}_{\text{CNOT}} = \hat{S}_x^{(\text{ctrl})}\hat{S}_x^{(\text{targ})}$.

Problem 7. Verify (13.26) for the case $n = 3$.

Problem 8. Alice and Bob share two particles in a given Bell state. Alice performs a unitary transformation on her qubit using either the unit matrix $\mathcal{I}$ or one of the Pauli matrices. Subsequently, she sends her qubit to Bob.

1. Can Bob find which transformation Alice has performed?
2. Can Eve find which transformation Alice has performed?

The information that Bob receives (one of the four numbers) can be encoded in two bits of classical information, in spite of the fact that he receives a single qubit (from which a single bit is expected to be extracted). This quantum result is called superdense coding.

Problem 9. Find the value of the amplitudes c_{ir} in the Fourier transform (13.11).

Problem 10. Construct the algorithm for a Bell analyzer

1. Apply the controlled-NOT gate to each Bell state
2. Apply the Hadamard gate to the control qubit
3. Show that the resultant states are products of classical bits (12.1).