
QUANTUM COMPUTING EXPLAINED

David McMahon



WILEY-INTERSCIENCE
A John Wiley & Sons, Inc., Publication

QUANTUM COMPUTING EXPLAINED





THE WILEY BICENTENNIAL—KNOWLEDGE FOR GENERATIONS

Each generation has its unique needs and aspirations. When Charles Wiley first opened his small printing shop in lower Manhattan in 1807, it was a generation of boundless potential searching for an identity. And we were there, helping to define a new American literary tradition. Over half a century later, in the midst of the Second Industrial Revolution, it was a generation focused on building the future. Once again, we were there, supplying the critical scientific, technical, and engineering knowledge that helped frame the world. Throughout the 20th Century, and into the new millennium, nations began to reach out beyond their own borders and a new international community was born. Wiley was there, expanding its operations around the world to enable a global exchange of ideas, opinions, and know-how.

For 200 years, Wiley has been an integral part of each generation's journey, enabling the flow of information and understanding necessary to meet their needs and fulfill their aspirations. Today, bold new technologies are changing the way we live and learn. Wiley will be there, providing you the must-have knowledge you need to imagine new worlds, new possibilities, and new opportunities.

Generations come and go, but you can always count on Wiley to provide you the knowledge you need, when and where you need it!

A handwritten signature in black ink that reads "William J. Pesce".

WILLIAM J. PESCE
PRESIDENT AND CHIEF EXECUTIVE OFFICER

A handwritten signature in black ink that reads "Peter Booth Wiley".

PETER BOOTH WILEY
CHAIRMAN OF THE BOARD

QUANTUM COMPUTING EXPLAINED

David McMahon



WILEY-INTERSCIENCE
A John Wiley & Sons, Inc., Publication

Copyright © 2008 by John Wiley & Sons, Inc. All rights reserved.

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise, except as permitted under Section 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 750-4470, or on the web at www.copyright.com. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at <http://www.wiley.com/go/permission>.

Limit of Liability/Disclaimer of Warranty: While the publisher and author have used their best efforts in preparing this book, they make no representations or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Neither the publisher nor author shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

For general information on our other products and services or for technical support, please contact our Customer Care Department within the United States at (800) 762-2974, outside the United States at (317) 572-3993 or fax (317) 572-4002.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic formats. For more information about Wiley products, visit our web site at www.wiley.com.

Wiley Bicentennial Logo: Richard J. Pacifico

Library of Congress Cataloging-in-Publication Data:

McMahon, David (David M.)

Quantum computing explained / David McMahon.

p. cm.

Includes index.

ISBN 978-0-470-09699-4 (cloth)

1. Quantum computers. I. Title.

QA76.889.M42 2007

004.1—dc22

2007013725

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

CONTENTS

Preface

xvii

1	A BRIEF INTRODUCTION TO INFORMATION THEORY	1
	Classical Information	1
	Information Content in a Signal	2
	Entropy and Shannon's Information Theory	3
	Probability Basics	7
	Example 1.1	8
	Solution	8
	Exercises	8
2	QUBITS AND QUANTUM STATES	11
	The Qubit	11
	Example 2.1	13
	Solution	13
	Vector Spaces	14
	Example 2.2	16
	Solution	17
	Linear Combinations of Vectors	17
	Example 2.3	18
	Solution	18
	Uniqueness of a Spanning Set	19
	Basis and Dimension	20
	Inner Products	21
	Example 2.4	22
	Solution	23
	Example 2.5	24
	Solution	24
	Orthonormality	24
	Gram-Schmidt Orthogonalization	26
	Example 2.6	26
	Solution	26

Bra-Ket Formalism	28
Example 2.7	29
Solution	29
The Cauchy-Schwartz and Triangle Inequalities	31
Example 2.8	32
Solution	32
Example 2.9	33
Solution	34
Summary	35
Exercises	36
3 MATRICES AND OPERATORS	39
Observables	40
The Pauli Operators	40
Outer Products	41
Example 3.1	41
Solution	41
You Try It	42
The Closure Relation	42
Representations of Operators Using Matrices	42
Outer Products and Matrix Representations	43
You Try It	44
Matrix Representation of Operators in Two-Dimensional Spaces	44
Example 3.2	44
Solution	44
You Try It	45
Definition: The Pauli Matrices	45
Example 3.3	45
Solution	45
Hermitian, Unitary, and Normal Operators	46
Example 3.4	47
Solution	47
You Try It	47
Definition: Hermitian Operator	47
Definition: Unitary Operator	48
Definition: Normal Operator	48
Eigenvalues and Eigenvectors	48
The Characteristic Equation	49
Example 3.5	49
Solution	49
You Try It	50
Example 3.6	50
Solution	50
Spectral Decomposition	53
Example 3.7	53

Solution	54
The Trace of an Operator	54
Example 3.8	54
Solution	54
Example 3.9	55
Solution	55
Important Properties of the Trace	56
Example 3.10	56
Solution	56
Example 3.11	57
Solution	57
The Expectation Value of an Operator	57
Example 3.12	57
Solution	58
Example 3.13	58
Solution	59
Functions of Operators	59
Unitary Transformations	60
Example 3.14	61
Solution	61
Projection Operators	62
Example 3.15	63
Solution	63
You Try It	63
Example 3.16	65
Solution	65
Positive Operators	66
Commutator Algebra	66
Example 3.17	67
Solution	67
The Heisenberg Uncertainty Principle	68
Polar Decomposition and Singular Values	69
Example 3.18	69
Solution	70
The Postulates of Quantum Mechanics	70
Postulate 1: The State of a System	70
Postulate 2: Observable Quantities Represented by Operators	70
Postulate 3: Measurements	70
Postulate 4: Time Evolution of the System	71
Exercises	71
4 TENSOR PRODUCTS	73
Representing Composite States in Quantum Mechanics	74
Example 4.1	74
Solution	74

Example 4.2	75
Solution	75
Computing Inner Products	76
Example 4.3	76
Solution	76
You Try It	76
Example 4.4	77
Solution	77
You Try It	77
Example 4.5	77
Solution	77
You Try It	77
Tensor Products of Column Vectors	78
Example 4.6	78
Solution	78
You Try It	78
Operators and Tensor Products	79
Example 4.7	79
Solution	79
You Try It	79
Example 4.8	80
Solution	80
Example 4.9	80
Solution	81
Example 4.10	81
Solution	81
You Try It	82
Example 4.11	82
Solution	82
You Try It	82
Tensor Products of Matrices	83
Example 4.12	83
Solution	83
You Try It	84
Exercises	84

5 THE DENSITY OPERATOR **85**

The Density Operator for a Pure State	86
Definition: Density Operator for a Pure State	87
Definition: Using the Density Operator to Find the Expectation Value	88
Example 5.1	88
Solution	89
You Try It	89
Time Evolution of the Density Operator	90
Definition: Time Evolution of the Density Operator	91

The Density Operator for a Mixed State	91
Key Properties of a Density Operator	92
Example 5.2	93
Solution	93
Expectation Values	95
Probability of Obtaining a Given Measurement Result	95
Example 5.3	96
Solution	96
You Try It	96
Example 5.4	96
Solution	97
You Try It	98
You Try It	99
You Try It	99
Characterizing Mixed States	99
Example 5.5	100
Solution	100
Example 5.6	102
Solution	103
You Try It	103
Example 5.7	103
Solution	104
Example 5.8	105
Solution	105
Example 5.9	106
Solution	106
You Try It	108
Probability of Finding an Element of the Ensemble in a Given State	108
Example 5.10	109
Solution	109
Completely Mixed States	111
The Partial Trace and the Reduced Density Operator	111
You Try It	113
Example 5.11	114
Solution	114
The Density Operator and the Bloch Vector	115
Example 5.12	116
Solution	116
Exercises	117
6 QUANTUM MEASUREMENT THEORY	121
Distinguishing Quantum States and Measurement	121
Projective Measurements	123
Example 6.1	125
Solution	126

Example 6.2	128
Solution	129
You Try It	130
Example 6.3	130
Solution	130
Measurements on Composite Systems	132
Example 6.4	132
Solution	132
Example 6.5	133
Solution	134
Example 6.6	135
Solution	135
You Try It	136
Example 6.7	136
Solution	137
You Try It	138
Example 6.8	138
Solution	138
Generalized Measurements	139
Example 6.9	140
Solution	140
Example 6.10	140
Solution	140
Positive Operator-Valued Measures	141
Example 6.11	141
Solution	142
Example 6.12	142
Solution	143
Example 6.13	143
Solution	144
Exercises	145
7 ENTANGLEMENT	147
Bell's Theorem	151
Bipartite Systems and the Bell Basis	155
Example 7.1	157
Solution	157
When Is a State Entangled?	157
Example 7.2	158
Solution	158
Example 7.3	158
Solution	158
Example 7.4	159
Solution	159
You Try It	162

You Try It	162
The Pauli Representation	162
Example 7.5	162
Solution	162
Example 7.6	163
Solution	163
Entanglement Fidelity	166
Using Bell States For Density Operator Representation	166
Example 7.7	167
Solution	167
Schmidt Decomposition	168
Example 7.8	168
Solution	168
Example 7.9	169
Solution	169
Purification	169
Exercises	170

8 QUANTUM GATES AND CIRCUITS **173**

Classical Logic Gates	173
You Try It	175
Single-Qubit Gates	176
Example 8.1	178
Solution	178
You Try It	179
Example 8.2	179
Solution	180
More Single-Qubit Gates	180
You Try It	181
Example 8.3	181
Solution	181
Example 8.4	182
Solution	182
You Try It	183
Exponentiation	183
Example 8.5	183
Solution	183
You Try It	184
The Z–Y Decomposition	185
Basic Quantum Circuit Diagrams	185
Controlled Gates	186
Example 8.6	187
Solution	188
Example 8.7	188
Solution	188

Example 8.8	190
Solution	190
Example 8.9	191
Solution	192
Gate Decomposition	192
Exercises	195
9 QUANTUM ALGORITHMS	197
Hadamard Gates	198
Example 9.1	200
Solution	201
The Phase Gate	201
Matrix Representation of Serial and Parallel Operations	201
Quantum Interference	202
Quantum Parallelism and Function Evaluation	203
Deutsch-Jozsa Algorithm	207
Example 9.2	208
Solution	208
Example 9.3	209
Solution	209
Quantum Fourier Transform	211
Phase Estimation	213
Shor's Algorithm	216
Quantum Searching and Grover's Algorithm	218
Exercises	221
10 APPLICATIONS OF ENTANGLEMENT: TELEPORTATION AND SUPERDENSE CODING	225
Teleportation	226
Teleportation Step 1: Alice and Bob Share an Entangled Pair of Particles	226
Teleportation Step 2: Alice Applies a CNOT Gate	226
Teleportation Step 3: Alice Applies a Hadamard Gate	227
Teleportation Step 4: Alice Measures Her Pair	227
Teleportation Step 5: Alice Contacts Bob on a Classical Communications Channel and Tells Him Her Measurement Result	228
The Peres Partial Transposition Condition	229
Example 10.1	229
Solution	230
Example 10.2	230
Solution	231
Example 10.3	232
Solution	232
Entanglement Swapping	234
Superdense Coding	236

Example 10.4	237
Solution	237
Exercises	238
11 QUANTUM CRYPTOGRAPHY	239
A Brief Overview of RSA Encryption	241
Example 11.1	242
Solution	242
Basic Quantum Cryptography	243
Example 11.2	245
Solution	245
An Example Attack: The Controlled NOT Attack	246
The B92 Protocol	247
The E91 Protocol (Ekert)	248
Exercises	249
12 QUANTUM NOISE AND ERROR CORRECTION	251
Single-Qubit Errors	252
Quantum Operations and Krauss Operators	254
Example 12.1	255
Solution	255
Example 12.2	257
Solution	257
Example 12.3	259
Solution	259
The Depolarization Channel	260
The Bit Flip and Phase Flip Channels	261
Amplitude Damping	262
Example 12.4	265
Solution	265
Phase Damping	270
Example 12.5	271
Solution	271
Quantum Error Correction	272
Exercises	277
13 TOOLS OF QUANTUM INFORMATION THEORY	279
The No-Cloning Theorem	279
Trace Distance	281
Example 13.1	282
Solution	282
You Try It	283
Example 13.2	283

Solution	284
Example 13.3	285
Solution	285
Fidelity	286
Example 13.4	287
Solution	288
Example 13.5	289
Solution	289
Example 13.6	289
Solution	289
Example 13.7	290
Solution	290
Entanglement of Formation and Concurrence	291
Example 13.8	291
Solution	292
Example 13.9	293
Solution	293
Example 13.10	294
Solution	294
Example 13.11	295
Solution	295
You Try It	296
Information Content and Entropy	296
Example 13.12	298
Solution	298
Example 13.13	299
Solution	299
Example 13.14	299
Solution	299
Example 13.15	300
Solution	300
Example 13.16	301
Solution	301
Example 13.17	302
Solution	302
Exercises	303
14 ADIABATIC QUANTUM COMPUTATION	305
Example 14.1	307
Solution	307
Adiabatic Processes	308
Example 14.2	308
Solution	309
Adiabatic Quantum Computing	310
Example 14.3	310

Solution	310
Exercises	313
15 CLUSTER STATE QUANTUM COMPUTING	315
Cluster States	316
Cluster State Preparation	316
Example 15.1	317
Solution	317
Adjacency Matrices	319
Stabilizer States	320
Aside: Entanglement Witness	322
Cluster State Processing	324
Example 15.2	326
Exercises	326
References	329
Index	331

PREFACE

“In the twenty-first” century it is reasonable to expect that some of the most important developments in science and engineering will come about through interdisciplinary research. Already in the making is surely one of the most interesting and exciting development we are sure to see for a long time, *quantum computation*. A merger of computer science and physics, quantum computation came into being from two lines of thought. The first was the recognition that *information is physical*, which is an observation that simply states the obvious fact that information can’t exist or be processed without a physical medium.

At the present time quantum computers are mostly theoretical constructs. However, it has been proved that in at least some cases quantum computation is much faster in principle than any done by classical computer. The most famous algorithm developed is Shor’s factoring algorithm, which shows that a quantum computer, if one could be constructed, could quickly crack the codes currently used to secure the world’s data. Quantum information processing systems can also do remarkable things not possible otherwise, such as teleporting the state of a particle from one place to another and providing unbreakable cryptography systems.

Our treatment is not rigorous nor is it complete for the following reason: this book is aimed primarily at two audiences, the first group being undergraduate physics, math, and computer science majors. In most cases these undergraduate students will find the standard presentations on quantum computation and information science a little hard to digest. This book aims to fill in the gap by providing undergraduate students with an easy to follow format that will help them grasp many of the fundamental concepts of quantum information science.

This book is also aimed at readers who are technically trained in other fields. This includes students and professionals who may be engineers, chemists, or biologists. These readers may not have the background in quantum physics or math that most people in the field of quantum computation have. This book aims to fill the gap here as well by offering a more “hand-holding” approach to the topic so that readers can learn the basics and a little bit on how to do calculations in quantum computation.

Finally, the book will be useful for graduate students in physics and computer science taking a quantum computation course who are looking for a computationally oriented supplement to their main textbook and lecture notes.

The goal of this book is to open up and introduce quantum computation to these nonstandard audiences. As a result the level of the book is a bit lower than that found in the standard quantum computation books currently available. The presentation is informal, with the goal of introducing the concepts used in the field and then showing through explicit examples how to work with them. Some topics are left out entirely and many are not covered at the deep level that would be expected in a graduate level quantum computation textbook. An in-depth treatment of adiabatic quantum computation or cluster state computation is beyond this scope of this book. So this book could not be considered complete in any sense. However, it will give readers who are new to the field a substantial foundation that can be built upon to master quantum computation.

While an attempt was made to provide a broad overview of the field, the presentation is weighted more in the physics direction.

A BRIEF INTRODUCTION TO INFORMATION THEORY

In this chapter we will give some basic background that is useful in the study of quantum information theory. Our primary focus will be on learning how to quantify information. This will be done using a concept known as *entropy*, a quantity that can be said to be a measure of disorder in physics. Information is certainly the opposite of disorder, so we will see how entropy can be used to characterize the information content in a signal and how to determine how many bits we need to reliably transmit a signal. Later these ideas will be tied in with quantum information processing. In this chapter we will also briefly look at problems in computer science and see why we might find quantum computers useful. This chapter won't turn you into a computer engineer, we are simply going to give you the basic fundamentals.

CLASSICAL INFORMATION

Quantum computation is an entirely new way of information processing. For this reason traditional methods of computing and information processing you are familiar with are referred to as *classical information*. For those new to the subject, we begin with a simple and brief review of how information is stored and used in computers. The most basic piece of information is called a *bit*, and this basically represents a

yes—no answer to a question. To represent this mathematically, we use the fact that we're dealing with a two-state system and choose to represent information using base 2 or *binary* numbers. A binary number can be 0 or 1, and a bit can assume one or the other of these values. Physically we can implement a bit with an electrical circuit that is either at ground or zero volts (binary 0), or at say +5 volts (binary 1). The physical implementation of a computing system is not our concern in this book; we are only worried about the mathematics and logic of the system. As a first step in getting acquainted with the binary world we might want to learn how to count using base 2.

Before we do that, we need to know that the number of bits required to represent something can be determined in the following way: Suppose that some quantity can assume one of m different states. Then

$$2^n \geq m \tag{1.1}$$

for some n . The smallest n for which this holds tells us the number of bits we need to represent or encode that quantity.

To see how this works, suppose that we want to represent the numbers 0, 1, 2, 3 in binary. We have four items, and $2^2 = 4$. Therefore we need at least two bits to represent these numbers. The representation is shown in Table 1.1.

To represent the numbers 0 through 7, we have $2^3 = 8$, so we need three bits. The binary representation of the numbers 0 through 7 is shown in Table 1.2.

INFORMATION CONTENT IN A SIGNAL

Now that we know how to encode information, we can start thinking about how to quantify it. That is, given a message m , how much information is actually contained in that message?

A clue about how this quantification might be done can be found by looking at (1.1). Considering the case where we take the equal sign, let's take the base two logarithm of both sides. That is, we start with

$$m = 2^n$$

TABLE 1.1 Binary representation of the numbers 0–3

Decimal	Binary
0	00
1	01
2	10
3	11

TABLE 1.2 Binary representation of the numbers 0–7

Decimal	Binary
0	000
1	001
2	010
3	011
4	100
5	101
6	110
7	111

Taking the base 2 log of both sides, we find that

$$\log_2 m = n \tag{1.2}$$

Equation (1.2) was proposed by Ralph Hartley in 1927. It was the first attempt at quantifying the amount of information in a message. What (1.2) tells us is that n bits can store m different messages. To make this more concrete, notice that

$$\log_2 8 = 3$$

That tells us that 3 bits can store 8 different messages. In Table 1.2 the eight messages we encoded were the numbers 0 through 7. However, the code could represent anything that had eight different possibilities.

You're probably familiar with different measurements of information storage capacity from your computer. The most basic word or unit of information is called a *byte*. A byte is a string of eight bits linked together. Now

$$\log_2 256 = 8$$

Therefore a byte can store 256 different messages. Measuring information in terms of logarithms also allows us to exploit the fact that logarithms are additive.

ENTROPY AND SHANNON'S INFORMATION THEORY

The Hartley method gives us a basic characterization of information content in a signal. But another scientist named Claude Shannon showed that we can take things a step further and get a more accurate estimation of the information content in a signal by thinking more carefully. The key step taken by Shannon was that he asked how *likely* is it that we are going to see a given piece of information? This is an

important insight because it allows us to characterize how much information we actually *gain* from a signal.

If a message has a very high probability of occurrence, then we don't gain all that much new information when we come across it. On the other hand, if a message has a low probability of occurrence, when we are made aware of it, we gain a significant amount of information. We can make this concrete with an example. A major earthquake occurred in the St. Louis area way back in 1812. Generally speaking, earthquakes in that area are relatively rare—after all, when you think of earthquakes, you think of California, not Missouri.

So most days people in Missouri aren't waiting around for an earthquake. Under typical conditions the probability of an earthquake occurring in Missouri is low, and the probability of an earthquake *not* occurring is high. If our message is that tomorrow there will *not* be an earthquake in Missouri, our message is a high probability message, and it conveys very little new information—for the last two hundred years day after day there hasn't been an earthquake. On the other hand, if the message is that tomorrow there will be an earthquake, this is dramatic news for Missouri residents. They gain *a lot* of information in this case.

Shannon quantified this by taking the base 2 logarithm of the probability of a given message occurring. That is, if we denote the information content of a message by I , and the probability of its occurrence by p , then

$$I = -\log_2 p \quad (1.3)$$

The negative sign ensures that the information content of a message is positive, and that the less probable a message, the higher is the information content. Let's suppose that the probability of an earthquake not happening tomorrow in St. Louis is 0.995. The information content of this fact is

$$I = -\log_2 0.995 = 0.0072$$

Now the probability that an earthquake does happen tomorrow is 0.005. The information content of this piece of information is

$$I' = -\log_2 0.005 = 7.6439$$

So let's summarize the use of logarithms to characterize the information content in a signal by saying:

- A message that is unlikely to occur has a low probability and therefore has a large information content.
- A message that is very likely to occur has a high probability and therefore has a small information content.

Next let's develop a more formal definition. Let X be a random variable characterized by a probability distribution \vec{p} , and suppose that it can assume one of

the values x_1, x_2, \dots, x_n with probabilities p_1, p_2, \dots, p_n . Probabilities satisfy $0 \leq p_i \leq 1$ and $\sum_i p_i = 1$.

The Shannon entropy of X is defined as

$$H(X) = - \sum_i p_i \log_2 p_i \tag{1.4}$$

If the probability of a given x_j is zero, we use $0 \log 0 = 0$. Notice that if we are saying that the logarithm of the probability of x gives the information content, we can also view the Shannon entropy function as a measure of the amount of uncertainty or randomness in a signal.

We can look at this more concretely in terms of transmitted message signals as follows: Suppose that we have a signal that always transmits a “2,” so that the signal is the string 2222222222... What is the entropy in this case? The probability of obtaining a 2 is 1, so the entropy or disorder is

$$H = -\log_2 1 = 0$$

The Shannon entropy works as we expect—a signal that has all the same characters with no changes has no disorder and hence no entropy.

Now let's make a signal that's a bit more random. Suppose that the probability of obtaining a “1” is 0.5 and the probability of obtaining a “2” is 0.5, so the signal looks something like 11212221212122212121112... with approximately half the characters 1's and half 2's. What is the entropy in this case? It's

$$H = -\frac{1}{2} \log_2 \frac{1}{2} - \frac{1}{2} \log_2 \frac{1}{2} = \frac{1}{2} + \frac{1}{2} = 1$$

Suppose further that there are three equally likely possibilities. In that case we would have

$$H = -\frac{1}{3} \log_2 \frac{1}{3} - \frac{1}{3} \log_2 \frac{1}{3} - \frac{1}{3} \log_2 \frac{1}{3} = 0.528 + 0.528 + 0.528 = 1.585$$

In each case that we have examined here, the uncertainty in regard to what character we will see next in the message has increased each time—so the entropy also increases each time. In this view we can see that Shannon entropy measures the amount of uncertainty or randomness in the signal. That is:

- If we are certain what the message is, the Shannon entropy is zero.
- The more uncertain we are as to what comes next, the higher the Shannon entropy.

We can summarize Shannon entropy as

Decrease uncertainty \Rightarrow Increase information

Increase uncertainty \Rightarrow Increase entropy

Now suppose that we require l_i bits to represent each x_i in X . Then the *average bit rate* required to encode X is

$$R_X = \sum_{i=1}^n l_i p_i \quad (1.5)$$

The Shannon entropy is the lower bound of the average bit rate

$$H(X) \leq R_X \quad (1.6)$$

The worst-case scenario in which we have the least information is a distribution where the probability of each item is the same—meaning a uniform distribution. Again, suppose that it has n elements. The probability of finding each x_i if the distribution is uniform is $1/n$. So sequence X with n elements occurring with uniform probabilities $1/n$ has entropy $-\sum \frac{1}{n} \log_2 \frac{1}{n} = \sum \frac{1}{n} \log n = \log n$. This tells us that the Shannon entropy has the bounds

$$0 \leq H(X) \leq \log_2 n \quad (1.7)$$

The *relative entropy* of two variables X and Y characterized by probability distributions p and q is

$$H(X\|Y) = \sum p \log_2 \frac{p}{q} = -H(X) - \sum p \log_2 q \quad (1.8)$$

Suppose that we take a fixed value y_i from Y . From this we can get a conditional probability distribution $p(X|y_i)$ which are the probabilities of X given that we have y_i with certainty. Then

$$H(X|Y) = - \sum_j p(x_j|y_i) \log_2(p(x_j|y_i)) \quad (1.9)$$

This is known as the *conditional entropy*. The conditional entropy satisfies

$$H(X|Y) \leq H(X) \quad (1.10)$$

To obtain equality in (1.10), the variables X and Y must be independent. So

$$H(X, Y) = H(Y) + H(X|Y) \quad (1.11)$$

We are now in a position to define *mutual information* of the variables X and Y . In words, this is the difference between the entropy of X and the entropy of X

given knowledge of what value Y has assumed, that is,

$$I(X|Y) = H(X) - H(X|Y) \quad (1.12)$$

This can also be written as

$$I(X|Y) = H(X) + H(Y) - H(X, Y) \quad (1.13)$$

PROBABILITY BASICS

Before turning to quantum mechanics in the next chapter, it's a good idea to quickly mention the basics of probability. Probability is heavily used in quantum theory to predict the possible results of measurement.

We can start by saying that the probability p_i of an event x_i falls in the range

$$0 \leq p_i \leq 1 \quad (1.14)$$

The two extremes of this range are characterized as follows: The probability of an event that is *impossible* is 0. The probability of an event that is *certain to happen* is 1. All other probabilities fall within this range.

The probability of an event is simply the relative frequency of its occurrence. Suppose that there are n total events, the j th event occurs n_j times, and we have $\sum_{j=1}^{\infty} n_j = n$. Then the probability that the j th event occurs is

$$p_j = \frac{n_j}{n} \quad (1.15)$$

The sum of all the probabilities is 1, since

$$\sum_{j=1}^{\infty} p_j = \sum_{j=1}^{\infty} \frac{n_j}{n} = \frac{1}{n} \sum_{j=1}^{\infty} n_j = \frac{n}{n} = 1 \quad (1.16)$$

The average value of a distribution is referred to as the *expectation value* in quantum mechanics. This is given by

$$\langle j \rangle = \sum_{j=1}^{\infty} \frac{j n_j}{n} = \sum_{j=1}^{\infty} j p_j \quad (1.17)$$

The *variance* of a distribution is

$$\langle (\Delta j)^2 \rangle = \langle j^2 \rangle - \langle j \rangle^2 \quad (1.18)$$

Example 1.1

A group of students takes an exam. The number of students associated with each score is

Score	Students
95	1
85	3
77	7
71	10
56	3

What is the most probable test score? What is the expectation value or average score?

Solution

First we write down the total number of students

$$n = \sum n_j = 1 + 3 + 7 + 10 + 3 = 24$$

The probability of scoring 95 is

$$p_1 = \frac{n_1}{n} = \frac{1}{24} = 0.04$$

and the other probabilities are calculated similarly. The most probable score is 71 with probability

$$p_4 = \frac{n_4}{n} = \frac{10}{24} = 0.42$$

The expectation value is found using (1.17):

$$\langle j \rangle = \sum j p_j = 95(0.04) + 85(0.13) + 77(0.29) + 71(0.42) + 56(0.13) = 74.3$$

In the next chapter we will see how to quantum mechanics uses probability.

EXERCISES

1.1. *How many bits are necessary to represent the alphabet using a binary code if we only allow uppercase characters? How about if we allow both uppercase and lowercase characters?*

- 1.2.** Describe how you can create an OR gate using NOT gates and AND gates.
- 1.3.** A kilobyte is 1024 bytes. How many messages can it store?
- 1.4.** What is the entropy associated with the tossing of a fair coin?
- 1.5.** Suppose that X consists of the characters A, B, C, D that occur in a signal with respective probabilities 0.1, 0.4, 0.25, and 0.25. What is the Shannon entropy?
- 1.6.** A room full of people has incomes distributed in the following way:

$$n(25.5) = 3$$

$$n(30) = 5$$

$$n(42) = 7$$

$$n(50) = 3$$

$$n(63) = 1$$

$$n(75) = 2$$

$$n(90) = 1$$

What is the most probable income? What is the average income? What is the variance of this distribution?

