/ Proofs

/ 证明

Introduction

序言

This text explains how to use mathematical models and methods to analyze problems that arise in computer science. The notion of a proof plays a central role in this work.

这本教材解释了怎样使用数学模型和方法分析计算机科学中的问题。证明的概念是本书的核心。

Simply put, a proof is a method of establishing truth. Like beauty, "truth" sometimes depends on the eye of the beholder, and it should not be surprising that what constitutes a proof differs among fields. For example, in the judicial system, legal truth is decided by a jury based on the allowable evidence presented at trial. In the business world, authoritative truth is specified by a trusted person or organization, or maybe just your boss.In fields such as physics and biology, scientific truth[1] is confirmed by experiment. In statistics, probable truth is established by statistical analysis of sample data.

简单来说；证明是证实**真理**的方法。像美一样，要说“真理”是什么，有时也见仁见智。但不足为奇的是，不同领域对证明的定义千差万别。例如，在司法系统中，**法律真实**是由陪审团基于可在审判时呈现的证据决定的。在企业界，**权威真实**是由可信的人或组织（也可能只是你的老板）指定的。在物理、生物之类的领域，**科学事实**是由实验证实的。在统计学中，**或然性真理**是由采样数据的统计分析证实的。

Philosophical proof involves careful exposition and persuasion typically based on a series of small, plausible arguments. The best example begins with "Cogito ergo sum," a Latin sentence that translates as "I think, therefore I am." It comes from the beginning of a 17th century essay by the mathematician/philosopher, Rene´ Descartes, and it is one of the most famous quotes in the world: do a web search on the phrase and you will be flooded with hits.

Deducing your existence from the fact that you're thinking about your existence is a pretty cool and presuasive-sounding idea. However, with just a few more lines of argument in this vein, Descartes goes on to conclude that here is an infinitely beneficent God. Whether or not you believe in a beneficent God, you'll probably agree that any very short proof of God's existence is bound to be far-fetched. So even in masterful hands, this approach is not reliable.

---

[1]Actually, only scientific falsehood can be demonstrated by an experiment——when the experiment fails to behave as predicted. But no amount of experiment can confirm that the next experiment won't fail. For this reason, scientists rarely speak of truth, but rather of theories that accurately predict past, and anticipated future, experiments.

Mathematics has its own specific notion of "proof".

Definition. A mathematical proof of a proposition is a chain of logical deductions leading to the proposition from a base set of axioms.

The three key ideas in this definition are highlighted: proposition, logical deduction, and axiom. These three ideas are explained in the following chapters, beginning with propositions in Chapter 1. We will then provide lots of examples of proofs and even some examples of "false proofs" (that is, arguments that look like a proof but that contain missteps, or deductions that aren't so logical when examied closely). False proofs are often even more important as examples than correct proofs, because they are uniquely helpful with honing your skills at making sure each step of a proof follows logically from prior steps.

Creating a good proof is a lot like creating a beautiful work of art. In fact, mathematicians often refer to really good proofs as being "elegant" or "beautiful". As with any endeavor, it will probably take a little practice before your fellow students use such praise when referring to your proofs, but to get you started in the right direction, we will provide templates for the most useful proof techniques in Chapter 2 and 3. We then apply these techniques in Chapter 4 to establish some important facts about numbers; facts that form the underpinning of one of the world's most widely-used cryptosystems.

1 Propositions

1.1 Compound Propositions

1.1 复合命题

In English, we can modify, combine, and relate propositions with words such as "not", "and", "or", "implies", and "if-then". For example, we can combine three propositions into one like this:

If all humans are mortal **and** all Greeks are human, **then** all Greeks are mortal.

在英语中，我们可以用如下的词修改、组合、关联命题——“非”、“且”、“或”、“蕴涵”、“如果-那么”。例如，可以把三个命题组合成类似下面的这个：

如果所有人都终归一死**且**希腊人是人，**那么**希腊人终究会死。

For the next while, we won't be much concerned with the internals of propositions—— whether they involve mathematics or Greek mortality—— but rather with how propositions are combined and related. So we'll frequently use variables such as P and Q in place of specific propositions such as "All humans are mortal" and "2 + 3 = 5". The understanding is that these variables, like propositions, can take on only the values T(true) and F(false). Such true/false variables are sometimes called Boolean variables after their inventor, George——you guessed it ——Boole.

接下来的这段时间，我们不会太过关注命题的内在含义——无论它们涉及数学还是希腊人的必死性——相反，我们会更关注怎样组合关联命题。所以我们经常使用像P和Q一样的变量来代替像“人终有一死”和"2 + 3 = 5"一样的具体命题。我们这样做的原因是，这些变量像命题一样，可取的值只有两个：T(真)和F(假）。这种真/假变量有时叫做布尔变量——以其发明者的名字乔治·布尔（你猜对了）命名。

1.1.1 NOT, AND, and OR

1.1.1 非、与、或

We can precisely define these special words using truth tables. For example, if P denotes an arbitrary proposition, then the truth of the proposition "NOT(P)" is defined by the following truth table:

P	**NOT(P)**
T	F
F	T

可使用**真值表**精确定义这些关键词。例如，如果P代表某个任意命题，则命题“非P"的取值由以下真值表定义：

P	**非P**
T	F
F	T

The first row of the table indicates that when proposition P is true, the proposition "NOT(P)" is false. The second line indicates that when P is false, "NOT(P)" is true. This is probably what you would expect.

表格的第一行表明，命题P为真时，命题“非P”为假。第二行表明，P为假时，“非P”为真。这可能是你所期望的。

In general, a truth table indicates the true/false value of a proposition for each possible setting of the variables.

真值表通常反映了在每个可能的变量取值下，命题的真/假值。

For example, the truth table for the proposition "P AND Q" has four lines, since the two variables can be set in four different ways:

P	Q	P AND Q
T	T	T
T	F	F
F	T	F
F	F	F

例如，命题“P与Q”的真值表有四行，因为可以用四种方式来设定两个变量的值：

P	Q	P 与 Q
T	T	T
T	F	F
F	T	F
F	F	F

According to this table, the proposition "P AND Q" is true only when P and Q are both true. This is probably the way you think about the word "and".

根据这个表格，只有P和Q都为真时，命题“P与Q”才为真。也许你也是这样考虑单词“**与**”的。

There is a subtlety in the truth table for "P OR Q":

P	Q	P OR Q
T	T	T
T	F	T
F	T	T
F	F	F

"P或Q"的真值表中有个细微差别：

P	Q	P 或 Q
T	T	T
T	F	T
F	T	T
F	F	F

The second row of this table says that "P OR Q" is true even if both P and Q are true. This isn't always the intended meaning of "or" in everyday speech, but this is the standard definition in mathematical writing. So if a mathematician says, "You may have cake, or you may have ice cream," he means that you could have both.

该表格的第二行表明，即使P和Q都为真，“P或Q"也为真。这并非总是日常会话中”或“的预期含义，但却是数学著作中的标准定义。所以如果某个数学家说，”你可以吃蛋糕，**或**冰淇淋。“ 他的意思是两种都可以吃。

If you want to exclude the possibility of both having and eating, you should use "exclusive-or" (XOR):

P	**Q**	**P XOR Q**
T	T	F
T	F	T
F	T	T
F	F	F

如果你想要排除把两种都拿来吃的可能性，应使用”异或“（XOR):

P	**Q**	**P 异或 Q**
T	T	F
T	F	T
F	T	T
F	F	F

1.1.2 IMPLIES

1.1.2 蕴涵

The least intuitive connecting word is "implies". Here is its truth table, with the lines labeled so we can refer to them later.

P	**Q**	**P IMPLIES Q**
T	T	T (tt)
T	F	F (tf)
F	T	T (ft)
F	F	T (ff)

最不直观的连接词是“蕴涵”。下面是它的真值表，每行都加了标记，以便在之后提及。

P	Q	P 蕴涵 Q
T	T	T (tt)
T	F	F (tf)
F	T	T (ft)
F	F	T (ff)

Let's experiment with this definition. For example, is the following proposition true or false?

"If the Riemann Hypothesis is true, then $x^2 \geq 0$ for every real number x."

让我们试用下该定义。例如，以下命题是真还是假?

"如果黎曼假设为真，那么对于每个实数x,有$x^2 \geq 0$"。

The Riemann Hypothesis is a famous unresolved conjecture in mathematics —no one knows if it is true or false. But that doesn't prevent you from answering the question! This proposition has the form P IMPLIES Q where the *hypothesis*, P , is “the Riemann Hypothesis is true” and the *conclusion*, Q, is “$x^2 \geq 0$ for every real number x”. Since the conclusion is definitely true, we're on either line (tt) or line (ft) of the truth table. Either way, the proposition as a while is *true*!

黎曼假设是数学中一个尚未证实的著名猜想——没人知道它的真假。但这并不妨碍你回答该问题！这个命题有着“P蕴涵Q"的形式——假设P是”黎曼假设是真的“，而结论Q是”对于每个实数x, $x^2 \geq 0$ “。因为结论肯定为真，所以该命题要么落在真值表的tt行，要么落在真值表的ft行。不管是哪种情况，该命题总是为真！

One of our original examples demonstrates an even stranger side of implications.

"If pigs can fly, then you can understand the Chebyshev bound."

我们最初的一个示例明显显露了**蕴涵**更为奇怪的一面。

”如果猪会飞，那么你就能理解契比雪夫不等式。“

Don't take this as an insult; we just need to figure out whether this proposition is true or false. Curiously, the answer has nothing to do with whether or not you can understand the Chebyshev bound. Pigs cannot fly, so we're on either line(ft) or line(ff) of the truth table. In both cases, the proposition is true!

别把它当侮辱；我们只需要搞清楚这一命题是真还是假。奇怪的是，答案和你是否能够理解契比雪夫不等式没有一点关系。猪不会飞，所以该命题落在真值表的ft行或ff行。在两种情形下，该命题都为真！

In contrast, here's an example of a false implication:

"If the moon shines white, then the moon is made of white cheddar."

相反，下面的示例是一个值为假的蕴涵：

"如果月亮发白光，那么它是用白色切达干酪做成的。"

Yes, the moon shines white. But, no, the moon is not made of white cheddar cheese. So we're on line(tf) of the truth table, and the proposition is false.

是的，月亮发白光。但是，月亮却不是用白色切达干酪做成的。所以该命题落在真值表的tf行，它的值为假。

The truth table for implications can be summarized in words as follows:

An implication is true exactly when the if-part is false or the then-part is true.

可以用如下的话来总结蕴涵的真值表：

当某蕴涵"**如果部分**"的值为**假**或"**那么部分**"的值为**真**时，该蕴涵的值正好为**真**。

This sentence is worth remembering; a large fraction of all mathematical statements are of the if-then form!

这句话值得牢记; 一大部分数学公式有着**如果-那么**的格式！

1.1.3 IFF

1.1.3 当且仅当

Mathematicians commonly join propositions in one additional way that doesn't arise in ordinary speech. The proposition "P if and only if Q" asserts that P and Q are logically equivalent; that is, either both are true or both are false.

数学家常用普通谈话中所没有的罕见方式来连接命题。命题"**P当且仅当Q**"断言P和Q逻辑上等价；即，**要么两者全为真；要么两者全为假**。

P	Q	P IFF Q
T	T	T
T	F	F
F	T	F
F	F	T

For example, the following if-and-only-if statement is true for every real number x:

例如，对于每个实数x, 以下的**"当且仅当"陈述**都为真：

$$x^2 - 4 \geq 0 \text{ iff } |x| \geq 2$$

For some values of x, both inequalities are true. For other values of x, neither inequality is true. In every case, however, the proposition as a whole is true.

对于x的某些值，两个不等式都为真。对于x的其他值，两个等式都不为真。但是不管怎样，**整个命题**都为真。

1.1.4 Notation

1.1.4 记法

Mathematicians have devised symbols to represent words like "AND" and "NOT". The most commonly-used symbols are summarized in the table below.

English	Symbolic Notation
NOT(P)	$\neg P$ (alternatively, $\overline{P}$)
P AND Q	P $\wedge$ Q
P OR Q	P $\vee$ Q
P IMPLIES Q	P $\rightarrow$ Q
if P then Q	P $\rightarrow$ Q
P IFF Q	P $\leftrightarrow$ Q

数学家设计了符号来代表“与”和“非”之类的词。下表总结了最常用的符号。

English	符号记法
非P	$\neg P$ (或, $\overline{P}$)
P与Q	P $\wedge$ Q
P或Q	P $\vee$ Q
P蕴涵Q	P $\rightarrow$ Q
如果P，那么Q	P $\rightarrow$ Q
P当且仅当Q	P $\leftrightarrow$ Q

For example, using this notation, "If P AND NOT(Q), then R" would be written:

例如，使用这种记法，“如果P与(非Q), 那么R”将记作：

$$(P \wedge \overline{Q}) \rightarrow R$$

This symbolic language is helpful for writing complicated logical expressions compactly. But words such as "OR" and "IMPLIES" generally serve just as well as the symbols $\vee$ and $\rightarrow$, and their meaning is easy to remember. We will use the prior notation for the most part in this text, but you can feel free to use whichever convention is easiest for you.

这种符号语言能够简洁地标记复杂的逻辑表达式。不过，像“或”和“蕴涵”之类的词，作用通常和符号$\vee$ 和 $\rightarrow$一样，符号的含义还容易记。本书中的大部分内容都将使用前面的记法，但你可以不受限制地使用对你来讲最简单的任何记法。

1.1.5 Logically Equivalent Implications

1.1.5 逻辑等价蕴涵

Do these two sentences say the same thing?

If I am hungry, then I am grumpy.
If I am not grumpy, then I am not hungry.

这两句话说的是同一件事吗?

"**如果**我饿了，**那么**我会颓丧易怒。“

"**如果**我愉快平和，**那么**我不饿。“

We can settle the issue by recasting both sentences in terms of propositional logic. Let P be the proposition “I am hungry”, and let Q be “I am grumpy”. The first sentence says “P IMPLIES Q” and the second says “NOT(Q) IMPLIES NOT(P) ”.

用命题逻辑的术语重新组织这两个句子，可以解决该问题。设P为命题“我饿了”，Q为命题“我颓丧易怒”。第一个句子表示为“P蕴涵Q”，第二个句子表示为“非(Q)蕴涵非(P)”。

We can compare these two statements in a truth table:

P	Q	P IMPLIES Q	NOT(Q) IMPLIES NOT(P)
T	T	T	T
T	F	F	F
F	T	T	T
F	F	T	T

我们可以在真值表中比较这两种陈述：

P	Q	P 蕴涵 Q	非Q 蕴涵 非P
T	T	T	T
T	F	F	F
F	T	T	T
F	F	T	T

Sure enough, the columns of truth values under these two statements are the same, which precisely means they are equivalent. In general, "NOT(Q) IMPLIES NOT(P)" is called the **contrapositive** of the implication "P IMPLIES Q". And, as we've just shown, the two are just different ways of saying the same thing.

果不其然，这两个陈述的**真假值**列相同，这正好表明它们等价。“非Q蕴涵非P"通常称为”P蕴涵Q"的对换命题。正如我们刚刚展示的那样，这两种陈述只是同一件事的不同描述方式。

In contrast, the converse of "P IMPLIES Q" is the statement "Q IMPLIES P". In terms of our example, the converse is:

If I am grumpy, then I am hungry.

相反，“P蕴涵Q”的逆命题是陈述“Q蕴涵P”。就我们的示例而言，逆命题是：

"**如果**我颓丧易怒，**那么**我会感觉饿。“

This sounds like a rather different contention, and a truth table confirms this suspicion:

P	Q	P IMPLIES Q	Q IMPLIES P
T	T	T	T
T	F	F	T
F	T	T	F
F	F	T	T

这听起来像是个相当不同的观点，而真值表证实了该推想：

P	Q	P 蕴涵 Q	Q 蕴涵 P
T	T	T	T
T	F	F	T
F	T	T	F
F	F	T	T

Thus, an implication is logically equivalent to its contrapositive but is not equivalent to its converse.

因此，蕴涵在逻辑上等价于它的对换命题，但却不等价于其逆命题。

One final relationship: an implication and its converse together are equivalent to an **iff statement**. For example,

If I am grumpy, then I am hungry, AND

if I am hungry, then I am grumpy.

are equivalent to the single statement:

I am grumpy IFF I am hungry.

最后一个关系：**蕴涵**“与上”其**逆命题**等价于**“当且仅当”陈述**。例如，

"**如果**我颓丧易怒，**那么**我会感觉饿。“ **与上**

"**如果**我饿了，**那么**我会颓丧易怒。“

等价于单个陈述：

“我颓丧易怒**当且仅当**我饿了。”

Once again, we can verify this with a truth table:

P	Q	P IMPLIES Q	Q IMPLIES P	(P IMPLIES Q) AND (Q IMPLIES P)	P IFF Q
T	T	T	T	T	T
T	F	F	T	F	F
F	T	T	F	F	F
F	F	T	T	T	T

我们可以再次使用真值表来验证它：

P	Q	P 蕴涵 Q	Q 蕴涵 P	(P 蕴涵 Q) 与 (Q 蕴涵 P)	P 当且仅当 Q
T	T	T	T	T	T
T	F	F	T	F	F
F	T	T	F	F	F
F	F	T	T	T	T

2 Patterns of Proof

证明的方法

2.1 The Axiomatic Method

2.1 公理化方法

The standard procedure for establishing truth in mathematics was invented by Eu- clid, a mathematician working in Alexandria, Egypt around 300 BC. His idea was to begin with five assumptions about geometry, which seemed undeniable based on direct experience.For example, one of the assumptions was "There is a straight line segment between every pair of points." Propositions like these that are simply accepted true are called axioms.

数学家欧几里得，生活于公元前300年左右的埃及亚历山大港，他发明了在数学中证实命题正确性的标准步骤。他的思想发端于几何学上的五个假设，它们基于直接经验，似乎毋庸置疑。例如，其中一个假设是“两点之间只有一个直线段。”像这样不证自明的命题称为公理。

Starting from these axioms, Euclid established the truth of many additional propositions by providing "proofs".A proof is a sequence of logical deductions **from** axioms and previously-proved statements that concludes with the proposition in question.

从这些公理开始，通过提供“证明”，欧几里得证实了许多附加命题的正确性。证明是一系列逻辑推论——从公理和之前证实过的陈述开始，以所讨论的命题作为结束。

There are several common terms for a proposition that has been proved.The different terms hint at the role of the proposition within a larger body of work.

- Important propositions are called *theorems*.
- A *lemma* is a preliminary proposition useful for proving later propositions.
- A *corollary* is a proposition that follows in just a few logical steps from a lemma or a theorem.

可用多个常见术语来指代已证明的命题。不同的术语暗示着该命题在更大工作体系中的作用。

- 重要的命题称作**定理**。
- **引理**是个可用于证明后续命题的初级命题。
- 从某个引理或定理开始，仅推导几步，就可得到叫做**推论**的命题。

Euclid's axiom-and-proof approach, now called the axiomatic method, is the foundation for mathematics today. In fact, just a handful of axioms, collectively called Zermelo-Frankel Set Theory with Choice(ZFC), together with a few logical deduction rules, appear to be sufficient to derive essentially all of mathematics.

欧几里德的公理&证明方法，现在称为公理化方法，是现代数学的基石。事实上，只需几个公理——它们统称为包括选择公理的策梅洛-弗兰克尔集合论——加上一些逻辑推论规则，似乎就足以推导出大体上所有的数学理论。

2.1.1 Our Axioms

2.1.1 我们的公理

The ZFC axioms are important in studying and justifying the foundations of mathematics, but for practical purposes, they are much too primitive.Proving theorems in ZFC is a little like writing programs in byte code instead of a full-fledged programming language——by one reckoning, a formal proof in ZFC that 2 + 2 = 4 requires more than 20,000 steps! So instead of starting with ZFC, we're going to take a huge set of axioms as our foundation: we'll accept all familiar facts from high school math!

在研究及证明数学基础的合理性方面，ZFC公理价值很大，但对实际应用来讲，它们却太过简陋。用ZFC证明定理有点象用字节码而非完备的编程语言来编写程序——据估计，用规范的ZFC来证明2 + 2 = 4需要超过20,000 个步骤！所以与其从ZFC开始，倒不如把超大的公理集当作我们的基础：我们将把高中数学中的常见事实都默认为公理！

This will give us a quick launch, but you may find this imprecise specification of the axioms troubling at times.For example, in the midst of a proof, you may find yourself wondering, "Must I prove this little fact or can I take it as an axiom?"Feel free to ask for guidance, but really there is no absolute answer. Just be up front about what you're assuming, and don't try to evade homework and exam problems by declaring everything an axiom!

这让我们得以快速开始，但有时你也会认为公理的这种不精确的规范会让人苦恼。例如，你可能在证明时陷入疑惑，“我是否必须证明这一小处事实，还是可以把它当公理？”不要羞于寻求指导，但的确不存在绝对正确的答案。只需直面你的职责，不要把一切都声明为公理来逃避作业和考试中的问题！

2.1.2 Logical Deductions

2.1.2 逻辑推论

Logical deductions or **inference rules** are used to prove new propositions using previously proved ones.

使用之前证实的命题来证明一个新命题时，会用到**逻辑推论**或**推理规则**。

A fundamental inference rule is *modus ponens*. This rule says that a proof of P together with a proof that P *IMPLIES* Q is a proof of Q.

假言推理是一个基本的**推理规则**。该规则称，**P**为真且**P蕴涵Q**为真，即可证明**Q**为真。

Inference rules are sometimes written in a funny notation. For example, *modus ponens* is written:

推理规则有时用古怪的符号标记。例如，假言推理标记如下：

Rule 2.1.1

$$\frac{P,\ P\ \ IMPLIES\ \ Q}{Q}$$

规则2.1.1

$$\frac{P,\ P\ \ \text{蕴 涵}\ \ Q}{Q}$$

When the statements above the line, called the antecedents, are proved, then we can consider the statement below the line, called the conclusion or **consequent**, to also be proved.

直线上面的陈述叫做**前件**，下面的陈述叫做**结论**或**后件**。证明了前件，就可以认为也证明了后件。

A key requirement of an **inference rule** is that it must be *sound*: any assignment of truth values that makes all the antecedents true must also make the consequent true. So if we start off with true axioms and apply sound inference rules, everything we prove will also be true.

一定得合理是推理规则的必要条件：指定任何值使所有前件为真，必然使后件也为真。所以如果我们从正确的公理着手，应用合理的推理规则，那么我们所证明的一切也都将为真。

You can see why modus ponens is a sound inference rule by checking the truth table of P *IMPLIES* Q. There is only one case where P and P IMPLIES Q are both true, and in that case Q is also true.

通过核查"P蕴涵Q"的真值表，你就会明白为什么要说假言推理是合理的推理规则。只在一种情形下**P**与**P蕴涵Q**都为真，同时**Q**也为真。

P	Q	$P \rightarrow Q$
F	F	T
F	T	T
T	F	F
T	T	T

There are many other natural, sound inference rules, for example:

也有很多自然合理的推理规则，如：

Rule 2.1.2

$$\frac{P\ IMPLIES\ Q,\ \ Q\ \ IMPLIES\ \ R}{P\ IMPLIES\ R}$$

规则 2.1.2

$$\frac{P\ 蕴\ 涵\ \ Q, Q\ 蕴\ 涵\ \ R}{P\ 蕴\ 涵\ \ R}$$

Rule 2.1.3

$$\frac{P\ IMPLIES\ Q,\ \ NOT(Q)}{NOT(P)}$$

规则 2.1.3

$$\frac{P\ 蕴\ 涵\ \ Q, 非\ Q}{非\ P}$$

Rule 2.1.4

$$\frac{NOT(P)\ IMPLIES\ NOT(Q)}{Q\ \ IMPLIES\ \ P}$$

规则 2.1.4

$$\frac{非\ P\ 蕴\ 涵\ \ 非\ Q}{Q\ 蕴\ 涵\ \ P}$$

On the other hand,

Non-Rule.

$$\frac{NOT(P)\ IMPLIES\ NOT(Q)}{P\ \ IMPLIES\ \ Q}$$

is not sound: if P is assigned **T** and Q is assigned **F**, then the antecedent is true and the consequent is not.

另一方面，

非规则

$$\frac{\text{非}\ P\ \text{蕴 涵}\ \text{非}\ Q}{P\ \text{蕴 涵}\ Q}$$

并不合理：如果指定P为**真**，Q为**假**，那么前件为真，但后件却不为真。

Note that a propositional inference rule is sound precisely when the conjunction(AND) of all its antecedents implies its consequent.

请注意，**命题推理规则**所有前件的合取(AND)表明它的后件为真时，才可以说**该规则**真正合理。

As with axioms, we will not be too formal about the set of legal inference rules. Each step in a proof should be clear and "logical"; in particular, you should state what previously proved facts are used to derive each new conclusion.

就像对待公理那样，我们不要求太过规范的**合法推理规则集**。证明中的每一步都应清楚、“合乎逻辑”；你尤其应该声明使用了之前证实过的哪些事实来推导每个新结论。

2.1.3 Proof Templates

2.1.3 证明模板

In principle, a proof can be any sequence of logical deductions from axioms and previously proved statements that concludes with the proposition in question. This freedom in constructing a proof can seem overwhelming at first. How do you even start a proof?

从理论上讲，证明可以是任意的逻辑推论序列——从公理与之前证实过的陈述开始，以所讨论的命题作为结束。**证明构造**中的这种自由乍看似乎让人无所适从。究竟怎样开始一段证明?

Here’s the good news: many proofs follow one of a handful of standard templates. Each proof has it own details, of course, but these templates at least provide you with an outline to fill in. In the remainder of this chapter, we’ll go through several of these standard patterns, pointing out the basic idea and common pitfalls and giving some examples. Many of these templates fit together; one may give you a top-level outline while others help you at the next level of detail. And we’ll show you other, more sophisticated proof techniques in Chapter 3.

好消息是，许多证明都遵循少数几个标准模板中的某一个。当然，每个证明都有它自己的细节，但这些模板至少为你提供了一个可以增补的框架。本章的剩余部分，我们将通读几个这类标准方法，指出基本思想、常见陷阱，并提供一些示例。许多这类模板可以组合使用；某个模板可能为你提供顶层框架，而其他模板会在另一个细节层次上帮到你。在第3章中，我们还将向你介绍其他更高超的证明技巧。

The recipes that follow are very specific at times, telling you exactly which words to write down on your piece of paper. You’re certainly free to say things your own way instead; we’re just giving you something you *could* say so that you’re never at a complete loss.

下面列出的方法有时非常具体，精确地告诉你在纸上写下哪个字。与之相反，你当然可不受限制地用自己的方式来完成证明；我们只是给你一些建议，以免你全然不知所措。

2.2 Proof by Cases

2.2 分情况证明

Breaking a complicated proof into cases and proving each case separately is a useful and common proof strategy. In fact, we have already implicitly used this strategy when we used truth tables to show that certain propositions were true or valid. For example, in section 1.1.5, we showed that an implication P IMPLIES Q is equivalent to its contrapositive NOT(Q) IMPLIES NOT(P) by considering all 4 possible assignments of T or F to P and Q. In each of the four cases, we showed that P IMPLIES Q is true if and only if NOT (Q) IMPLIES NOT (P) is true. For example, if P = T and Q = F, then both P IMPLIES Q and NOT (Q) IMPLIES NOT (P) are false, thereby establishing that (P IMPLIES Q) IFF (NOT (Q) IMPLIES NOT (P)) is true for this case. If a proposition is true in every possible case, then it is true.

把复杂的证明分解为若干情况，并分别证明各个情况，这是一种又有效又常见的证明策略。事实上，我们使用真值表证明某些命题为真（或合理）时，就隐式地用过该策略。例如，在1.1.5小节中，通过把T或F赋给P及Q的4种可能情形，我们证明了蕴涵**“P蕴涵Q”**等价于其对换命题**“(非Q)蕴涵(非P)"**。在四种情形中, 我们都证明了**“P蕴涵Q”**为真当且仅当**“非Q蕴涵非P”**为真。例如，如果P=T,Q=F, 那么**“P蕴涵Q ”**和**”(非Q)蕴涵(非P)“** 都为假，由此证实在这种情形下，**“P 蕴涵Q” 当且仅当“(非Q)蕴涵(非P)”**为真。如果某个命题在所有可能情形下都为真，那么该命题为真。

Proof by cases works in much more general environments than propositions involving Boolean variables. In what follows, we will use this approach to prove a simple fact about acquaintances. As background, we will assume that for any pair of people, either they have met or not. If every pair of people in a group has met, we'll call the group a *club*. If every pair of people in a group has not met, we'll call it a group of *strangers*.

与涉及布尔变量的命题相比，**分情况证明**在更一般的环境下有效。接下来，我们将用这一方法证明熟人关系的简单事实。作为背景，我们假定对于任何一对人，他们要么见过面，要么没见过。如果某组里每对人都见过面，我们称该组为**俱乐部**。如果某组里的每对人都没见过面，我们称它为**由陌生人构成的组**。

Theorem. *Every collection of 6 people includes a club of 3 people or a group of 3 strangers.*

定理：**每个6人组**都包括**一个3人俱乐部**或一个**由3个陌生人构成的组**。

Proof. The proof is by **case analysis**. Let x denote one of the six people. There are two cases:

1. Among the other 5 people besides x, at least 3 have met x.
2. Among the other 5 people, at least 3 have not met x.

证明：通过**情况分解**来证明。用x代表6个人中的某一个。有两种情况：

1. 除x以外的其他5个人中，至少有3个人见过x。
2. 其他5个人中，至少有3个人没见过x。

Now we have to be sure that at least one of these two cases must hold, but that's easy: we've split the 5 people into two groups, those who have shaken hands with x and those who have not, so one of the groups must have at least half the people.

现在我们必须确定，这两种情况中至少有一种肯定成立，这并不难：我们已经把这5个人分成了两组，一组和x握过手，一组没握过，所以其中一组必定至少有一半人。

- **Case 1:** Suppose that at least 3 people have met x.

  This case splits into two subcases:

  - **Case 1.1:** Among the people who have met x, none have met each other. Then the people who have met x are a group of at least 3 strangers. So the Theorem holds in this subcase.
  - **Case 1.2**: Among the people who have met x, some pair have met each other. Then that pair, together with x, form a club of 3 people. So the Theorem holds in this subcase.

This implies that the Theorem holds in Case 1.

- **情况1**：假设至少有3个人**见过**x。

  该情况分为两种子情况：

  - **情况1.1**：**见过x的人**互相都未见过面。那么**见过x的人**就构成了一个**至少包含3个陌生人的组**。所以该定理在这一子情况中成立。
  - **情况1.2**：见过x的人中，有一对彼此见过面。那么这一对和x一起，就构成 了**3人俱乐部**。所以该定理在这一子情况中成立。

这表明该定理在情况1中成立。

- **Case 2**: Suppose that at least 3 people have not met x.

  This case also splits into two subcases:

  - **Case 2.1**: Among the people who have not met x, every pair has met each other. Then the people who have not met x are a club of at least 3 people. So the Theorem holds in this subcase.
  - **Case 2.2**: Among the people who have not met x, some pair have not met each other. Then that pair, together with x, form a group of at least 3 strangers. So the Theorem holds in this subcase.

This implies that the Theorem also holds in Case 2, and therefore holds in all cases.■

- **情况2**：假设至少有3个人**没见过**x。

  这一情况也分为两种子情况：

  - **情况2.1**：**没见过x的人**，每对都互相见过面。则那些没见过x的人，构成了一个至少包含3个人的俱乐部。 所以该定理在这一子情况中成立。
  - **情况2.2**：**没见过x的人**中，有一对彼此未见过面。那么这一对和x一起，就构成了一组至少包含3个陌生人的组。所以该定理在这一子情况中成立。

这表明该定理在情况2中也成立，因此该定理在所有情况中都成立。■

2.3 Proving an Implication

2.3 证明蕴含

Propositions of the form "If P, then Q" are called implications. This implication is often rephrased as "P IMPLIES Q" or "$P \to Q$".

有着**“如果P, 那么Q”**形式的命题称为蕴涵。该蕴涵常重新表述为"P 蕴涵 Q" 或 "$P \to Q$"。

Here are some examples of implications:

下面是一些蕴涵示例：

- (Quadratic Formula) If $ax^2 + bx + c = 0$ and $a \neq 0$, then
$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$
- (二次公式）如果$ax^2 + bx + c = 0$ 且 $a \neq 0$, 那么
$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$
- (Goldbach's Conjecture) If n is an even integer greater than 2, then n is a sum of two primes.
- (哥德巴赫猜想）如果n是一个大于2的偶数，那么n是两个素数的和。
- If $0 \leq x \leq 2$, then $-x^3 + 4x + 1 > 0$.
- 如果 $0 \leq x \leq 2$, 那么 $-x^3 + 4x + 1 > 0$.

There are a couple of standard methods for proving an implication.

有几个标准方法可以证明蕴涵。

2.3.1 Method #1: Assume P is true

2.3.1 方法1：假设P为真

When proving P IMPLIES Q, there are two cases to consider: P is true and P is false. The case when P is false is easy since, by definition, **F** IMPLIES Q is true no matter what Q is. This case is so easy that we usually just forget about it and start right off by assuming that P is true when proving an implication, since this is the only case that is interesting.

证明**“P蕴涵Q”**时要考虑两种情况：P为真及P为假。**“P为假”**的情况容易证明，因为根据定义，无论Q是什么，“**F**蕴涵Q"总为真。这种情况太容易了，证明蕴涵时，常常只用忽略它，通过假定"P为真"（因为它是值得关注的唯一情形），立刻开始证明。

Hence, in order to prove that P IMPLIES Q:

1. Write, "Assume P".
2. Show that Q logically follows.

因此，为证明“P蕴涵Q”，得这样做：

1. 写下“假设P为真”。
2. 证明在逻辑上可推断出Q。

For example, we will use this method to prove

例如，我们将使用该方法证明

Theorem 2.3.1. If $0 \leq x \leq 2$, then $-x^3 + 4x + 1 > 0$.

定理2.3.1. 如果 $0 \leq x \leq 2$, 那么 $-x^3 + 4x + 1 > 0$.

Before we write a proof of this theorem, we have to do some scratchwork to figure out why it is true.

在写下该定理的证明前，不得不做一些草拟的工作来弄清它为真的原因。

The inequality certainly holds for x=0; then the left side is equal to 1 and $1 > 0$. As x grows, the 4x term (which is positive) initially seems to have greater magnitude than $-x^3$ (which is negative). For example, when x = 1, we have $4x = 4$, but $-x^3 = -1$. In fact, it looks like $-x^3$ doesn't begin to dominate $4x$ until $x > 2$. So it seems the $-x^3 + 4x$ part should be nonnegative for all x between 0 and 2, which would imply that $-x^3 + 4x + 1$ is positive.

x=0时该不等式肯定成立；此时左侧等于1，而$1 > 0$。当x增大时，起初项4x(值为正）的绝对值**似乎**要大过 $-x^3$(值为负)。例如，当x=1时，有 $4x = 4$, 但 $-x^3 = -1$. 事实上，很可能直到$x > 2$，$-x^3$ 才开始超过4x。所以对于0到2之间的所有x, **好像** $-x^3 + 4x$ 这部分应该是非负值，这意味着 $-x^3 + 4x + 1$是正值。

So far, so good. But we still have to replace all those "seems like" phrases with solid, logical arguments. We can get a better handle on the critical $-x^3 + 4x$ part by factoring it, which is not too hard:

$$-x^3 + 4x = x(2 - x)(2 + x)$$

到目前为止还不错。但我们还需要把所有这些“似乎”词组替换为逻辑上的确切论据。通过把关键部分$-x^3 + 4x$分解成因子（这并不太难），我们可以更好地理解它：

$$-x^3 + 4x = x(2 - x)(2 + x)$$

Aha! For x between 0 and 2, all of the terms on the right side are nonnegative. And a product of nonnegative terms is also nonnegative. Let's organize this blizzard of observations into a clean proof.

啊哈！对于0到2之间的x，右侧的所有项都是非负的。而非负项的乘积也是非负的。让我们把这一大堆观察所得整理成清晰准确的证明。

Proof. Assume $0 \leq x \leq 2$. Then x, 2-x, and 2+x are all nonnegative. Therefore, the product of these terms is also nonnegative. Adding 1 to this product gives a positive number, so:

$$x(2 - x)(2 + x) + 1 > 0$$

Multiplying out on the left side proves that

$$-x^3 + 4x + 1 > 0$$

as claimed. ■

证明：假设 $0 \leq x \leq 2$，那么x, 2-x, 2+x都是非负的。因此，这些项的乘积也是非负的。把1加到该乘积上得到一个正数，所以：

$$x(2 - x)(2 + x) + 1 > 0$$

把左侧的乘积展开，就证明了前面声称的

$$-x^3 + 4x + 1 > 0$$

There are a couple points here that apply to all proofs:

有两个细节适用于所有证明：

- You'll often need to do some scratchwork while you're trying to figure out the logical steps of a proof. Your sratchwork can be as disorganized as you like——full of dead-ends, strange diagrams, obscene words, whatever.But keep your scratchwork separate from your final proof, which should be clear and concise.
- 在你尝试着搞清楚证明的逻辑步骤时，常常需要做一些草拟的工作。你的草拟工作可以随心所欲——充斥着毫无进展可能的工作、奇怪的图表、令人憎恶的词等等。但要把你的草稿和最终的证明分开，后者应该清楚简明。
- Proofs typically begin with the word "Proof" and end with some sort of doohickey like □ or ■ or "q.e.d.". The only purpose for these conventions is to clarify where proofs begin and end.
- 证明通常用“证明”这个词开始，用某些像□ 、 ■ 或 "q.e.d."一样的小玩意结束。这些约定的唯一目的是阐明证明从哪开始，到哪结束。

Potential Pitfall

潜在的陷阱

For the purpose of proving an implication P IMPLIES Q, it's OK, and typical, to begin by assuming P. But when the proof is over, it's no longer OK to assume that P holds! For example, Theorem 2.3.1 has the form "if P, then Q" with P being "$0 \leq x \leq 2$ " and Q being "$-x^3 + 4x + 1 > 0$", and its proof began by assuming that $0 \leq x \leq 2$. But of course this assumption does not always hold. Indeed, if you were going to prove another result using the variable x, it could be disastrous to have a step where you assume that $0 \leq x \leq 2$ just because you assumed it as part of the proof of Theorem 2.3.1.

为了证明蕴涵“P蕴涵Q”这一目的，用“假设P为真”开始通常没问题。但证明结束后，再假设P成立就不行了。例如，定理2.3.1有着”若P,则Q“的格式，P是"$0 \leq x \leq 2$ ",Q是"$-x^3 + 4x + 1 > 0$"，证明从假设$0 \leq x \leq 2$开始。但显而易见，这一假设并非一直成立。确切来说，如果你要用变量x证明其他结果，有这样一个步骤——只是因为你把它看作定理2.3.1的一部分，就假设 $0 \leq x \leq 2$——可能会很糟糕。

2.3.2 Method #2: Prove the Contrapositive

2.3.2 方法2：证明对换命题

We have already seen that an implication "P IMPLIES Q" is logically equivalent to its contrapositive

NOT(Q) IMPLIES NOT(P)

我们已经知道蕴涵”P蕴涵Q“在逻辑上等价于其对换命题

”非Q蕴涵非P“

Proving one is as good as proving the other, and proving the contrapositive is sometimes easier than proving the original statement.

证明一个就相当于证明了另一个，而证明对换命题有时要比证明最初的陈述更为容易。

Hence, you can proceed as follows:

1. Write, "We prove the contrapositive:" and then state the contrapositive.
2. Proceed as in Method #1.

因此，你可以按照如下方式证明：

1.写下，”证明对换命题：“，然后陈述对换命题。

2.像方法1一样继续证明。

For example, we can use this approach to prove

Theorem 2.3.2. If r is irrational, then $\sqrt{r}$ is also irrational.

例如，我们可以用该方法来证明

定理2.3.2. 如果r是无理数，那么$\sqrt{r}$也是无理数。

Recall that rational numbers are equal to a ratio of integers and irrational numbers are not. So we must show that if r is *not* a ratio of integers, then $\sqrt{r}$ is also *not* a ratio of integers. That's pretty convoluted! We can eliminate both *not*'s and make the proof straightforward by considering the contrapositive instead.

回想一下，有理数等于整数之比，而无理数却不是这样。所以我们必须证明，如果r**不是**整数之比，那么$\sqrt{r}$也**不是**整数之比。这太让人费解了！相反，通过考虑对换命题，我们可以把两个“**不是**”都给剔除掉，使该证明更为简洁。

Proof. We prove the contrapositive:if $\sqrt{r}$ is rational, then r is rational.

Assume that $\sqrt{r}$ is rational. Then there exist integers a and b such that:

$$\sqrt{r} = \frac{a}{b}$$

Squaring both sides gives:

$$r = \frac{a^2}{b^2}$$

Since a^2 and b^2 are integers, r is also rational. ■

证明：证明对换命题：如果$\sqrt{r}$是有理数，那么r是有理数。

假设$\sqrt{r}$是有理数。则存在整数a、b,使得：

$$\sqrt{r} = \frac{a}{b}$$

将两边都平方，可得：

$$r = \frac{a^2}{b^2}$$

因为 a^2 和 b^2 是整数，所以r也是有理数。 ■

2.4 Proving an “If and Only If”

2.4 证明“当且仅当”

Many mathematical theorems assert that two statements are logically equivalent; that is, one holds if and only if the other does.

许多数学定理断言两个陈述逻辑上等价；即，一个陈述成立**当且仅当**另一个陈述也成立。

Here is an example that has been known for several thousand years:

Two triangles have the same side lengths if and only if two side lengths and the angle between those sides are the same in each triangle.

下面是一个数千年来公认的例子：

当且仅当两个三角形的两边及它们之间的夹角相等时，这两个三角形才全等。

The phrase "if and only if" comes up so often that it is often abbreviated "iff".

我们会非常频繁地提到词组“当且仅当”，所以常把它简写为**“iff"**。

2.4.1 Method #1: Prove Each Statement Implies the Other

2.4.1 方法1：证明每个陈述蕴涵另一个陈述

The statement "P IFF Q" is equivalent to the two statements "P IMPLIES Q" and "Q IMPLIES P". So you can prove an "iff" by proving two implications:

1.Write, "We prove P implies Q and vice-versa".

2.Write, "First, we show P implies Q". Do this by one of the methods in Section 2.3.

3.Write,"Now, we show Q implies P". Again, do this by one of the methods in Section 2.3.

陈述“P**当且仅当**Q"等价于两个陈述”P蕴涵Q“和”Q蕴涵P”。所以你可以通过证明两个蕴涵来证明”当且仅当“：

1.写下，”证明P蕴涵Q,反之亦然”。

2.写下，“首先证明P蕴涵Q”。用2.3节中的一种方法来证明。

3.写下，“现在证明Q蕴涵P”。再次使用2.3节里的一种方法证明。

2.4.2 Method #2: Construct a Chain of IFFs

2.4.2 方法2：构造“当且仅当”链

In order to prove that P is true iff Q is true:

1. Write, "We construct a chain of if-and-only-if implications".
2. Prove P is equivalent to a second statement which is equivalent to a third statement and so forth until you reach Q.

为证明当且仅当Q为真时，P才为真，得这样做：

1.写下，“构造一个当且仅当蕴涵链”。

2.证明P等价于第二个陈述，第二个陈述等价于第三个陈述，依此类推，直到到达Q为止。

This method sometimes requires more ingenuity than the first, but the result can be a short, elegant proof, as we see in the following example.

与第一种方法相比，该方法有时需要更多技巧，但正如我们在下面的示例中所看到的那样，结果却可能是个简洁优雅的证明。

Theorem 2.4.1. The standard deviation of a sequence of values $x_1,...,x_n$ is zero iff all the values are equal to the mean.

定理2.4.1. 当且仅当序列 $x_1,...,x_n$的所有值都等于均值时，该序列的标准差才为零。

Definition. The standard deviation of a sequence of values $x_1,x_2,...,x_n$ is defined to be:

$$\sqrt{\frac{(x_1-\mu)^2+(x_2-\mu)^2+...+(x_n-\mu)^2}{n}} \qquad (2.1)$$

where μ is the mean of the values:

$$\mu ::= \frac{x_1+x_2+...+x_n}{n}$$

定义 定义序列 $x_1,...,x_n$标准差为：

$$\sqrt{\frac{(x_1-\mu)^2+(x_2-\mu)^2+...+(x_n-\mu)^2}{n}} \qquad (2.1)$$

这里的μ是所有值的均值：

$$\mu ::= \frac{x_1+x_2+...+x_n}{n}$$

As an example, Theorem 2.4.1 says that the standard deviation of test scores is zero if and only if everyone scored exactly the class average. (We will talk a lot more about means and standard deviations in Part IV of the book.)

举个例子，按照定理2.4.1的理论，当且仅当每个人的得分都刚好等于班级平均分时，测验得分的标准差才为零。（在本书的第四部分，我们会更多地谈到均值与标准差）。

Proof. We construct a chain of "iff" implications, starting with the statement that the standard deviation (2.1) is zero:

$$\sqrt{\frac{(x_1-\mu)^2+(x_2-\mu)^2+...+(x_n-\mu)^2}{n}} = 0 \qquad (2.2)$$

Since zero is the only number whose square root is zero, equation(2.2) holds iff

$$(x_1-\mu)^2+(x_2-\mu)^2+\ldots+(x_n-\mu)^2=0 \qquad (2.3)$$

Squares of real numbers are always nonnegative, and so every term on the left hand side of equation (2.3) is nonnegative. This means that (2.3) holds iff

Every term on the left hand side of (2.3) is zero. (2.4)

But a term $(x_i - \mu)^2$ is zero iff $x_i = \mu$, so (2.4) is true iff

Every x_i equals the mean. ■

证明：我们构造了一个"当且仅当"蕴涵链，它从标准差（2.1）为零这个陈述开始：

$$\sqrt{\frac{(x_1-\mu)^2+(x_2-\mu)^2+...+(x_n-\mu)^2}{n}} = 0 \qquad (2.2)$$

因为零是唯一一个平方根为零的数，所以**当且仅当**

$$(x_1 - \mu)^2 + (x_2 - \mu)^2 + \ldots + (x_n - \mu)^2 = 0 \qquad (2.3)$$

等式（2.2）才成立。

实数的平方总是非负的，所以等式（2.3）左手侧的每一项都是非负的。这意味着**当且仅当**

等式（2.3）左手侧的每一项都为零时 （2.4）

等式（2.3）成立。

但**当且仅当**$x_i = \mu$时，某一项 $(x_i - \mu)^2$ 才为零，所以**当且仅当**

每个 x_i 都等于均值时，

等式（2.4）才为真。 ■

2.5 Proof by Contradiction

2.5 反证法

In a proof by contradiction or indirect proof, you show that if a proposition were false, then some false fact would be true. Since a false fact can't be true, the proposition had better not be false. That is, the proposition really must be true.

在反证法或间接证明中，证明了如果命题为假，那么某个错误的事实就会为真。因为错误的事实不能为真，所以该命题最好不要为假。也就是说，该命题必定为真。

Proof by contradiction is always a viable approach. However, as the name suggests, indirect proofs can be a little convoluted. So direct proofs are generally preferable as a matter of clarity.

反证法始终是个可行的方法。然而正如名字所示，间接证明可能会有些令人费解。所以要让证明清晰易懂，直接证明通常更合适些。

Method: In order to prove a proposition P by contradiction:

1. Write, "We use proof by contradiction."
2. Write, "Suppose P is false."
3. Deduce something known to be false (a logical contradiction).
4. Write, "This is a contradiction. Therefore, P must be true."

方法：为了用反证法证明命题P, 得这么做：

1. 写下"使用反证法证明"。
2. 写下"假设P为假"。

3. 推断出已知事实为假（逻辑矛盾）。
4. 写下“导出矛盾，因此，P肯定为真。”

As an example, we will use proof by contradiction to prove that $\sqrt{2}$ is irrational. Recall that a number is rational if it is equal to a ratio of integers. For example, $3.5 = 7/2$ and $0.1111... = 1/9$ are rational numbers.

举个例子，我们将使用反证法来证明 $\sqrt{2}$是无理数。回想一下，如果某个数等于整数之比，那么该数为有理数。如，$3.5 = 7/2$ 和 $0.1111... = 1/9$是有理数。

Theorem 2.5.1. $\sqrt{2}$ is irrational.

Proof. We use proof by contradiction. Suppose the claim is false; that is, $\sqrt{2}$ is rational. Then we can write $\sqrt{2}$ as a fraction n/d where n and d are positive integers. Furthermore, let's take n and d so that n/d is in lowest terms (that is, so that there is no number greater than 1 that divides both n and d).

Squaring both sides gives $2 = n^2/d^2$ and so $2d^2 = n^2$. This implies that n is a multiple of 2. Therefore n^2 must be a multiple of 4. But since $2d^2 = n^2$, we know $2d^2$ is a multiple of 4 and so d^2 is a multiple of 2. This implies that d is a multiple of 2.

So the numerator and denominator have 2 as a common factor, which contradicts the fact that n/d is in lowest terms. So $\sqrt{2}$ must be irrational. ■

定理2.5.1. $\sqrt{2}$是无理数。

证明：使用反证法证明 。假设这个待证明的论点为假；也就是说，$\sqrt{2}$ 是有理数。那么就可以把 $\sqrt{2}$ 写作分数 n/d，这里的n和d都是正整数。更进一步，取n和d,使得 n/d是最简分式（即，使得n和d没有大于1的公因子）。

把两边都平方可得$2 = n^2/d^2$，所以$2d^2 = n^2$。这间接说明n是2的倍数。因此n^2一定是4的倍数。又因为 $2d^2 = n^2$，可知 $2d^2$ 是4的倍数，所以d^2是2的倍数。这间接说明d是2的倍数。

所以分子和分母有个公因子2，这与n/d 是最简分式的事实相矛盾。所以$\sqrt{2}$ 必定是无理数。■

Potential Pitfall

潜在的陷阱

A proof of a proposition P by contradiction is really the same as proving the implication **T** IMPLIES P by contrapositive. Indeed, the contrapositive of **T** IMPLIES P is NOT(P) IMPLIES **F**. As we saw in Section 2.3.2, such a proof would be begin by assuming NOT(P) in an effort to derive a falsehood, just as you do in a proof by contradiction.

用反证法证明命题P实际上和用对换命题证明蕴涵”**T**蕴涵P“是一样的。其实，”**T**蕴涵P“的对换命题是“非P蕴涵**F**"。正如我们在2.3.2小节所学到的，这种证明可能会以假设”非P“为真开始，试图导出错误，正好和用反证法证明时的做法相同。

No matter how you think about it, it is important to remember that when you start by assuming NOT(P), you will derive conclusions along the way that are not necessarily true. (Indeed, the whole point of the method is to derive a falsehood.) This means that you cannot rely on intermediate results after a proof by contradiction is completed (for example, that n is even after the proof of Theorem 2.5.1). There was not much risk of that happening in the proof of Theorem

2.5.1, but when you are doing more complicated proofs that build up from several lemmas, some of which utilize a proof by contradiction, it will be important to keep track of which propositions only follow from a (false) assumption in a proof by contradiction.

无论你怎样理解，重要的是要记住，从假设"非P"为真开始，将沿着未必正确的道路，推导出结论。(确切说来，该方法的目标是导出错误。）这意味着用反证法证明完毕后，你不能依靠它的中间结果。（如，在证明完定理2.5.1.后，不能使用n是偶数这个中间结果）在证明定理2.5.1.时，不太可能发生这种情况。但有时你会进行更为复杂的证明，它们从几个引理系统地发展而来，其中有些引理使用了反证法。这时，记录哪些命题只是从反证法中的错误假设推断出来的，就变得重要起来。

2.6 Proofs about Sets

Sets are simple, flexible, and everywhere. You will find some set mentioned in nearly every section of this text. In fact, we have already talked about a lot of sets: the set of integers, the set of real numbers, and the set of positive even numbers, to name a few.

In this section, we'll see how to prove basic facts about sets. We'll start with some definitions just to make sure that you know the terminology and that you are comfortable working with sets.

2.6.1 Definitions

Informally, a set is a bunch of objects, which are called the elements of the set. The elements of a set can be just about anything: numbers, points in space, or even other sets. The conventional way to write down a set is to list the elements inside curly-braces. For example, here are some sets:

$A = \{Alex, Tippy, Shells, Shadow\}$ dead pets

$B = \{red, blue, yellow\}$ primary colors

$C = \{\{a, b\}, \{a, c\}, \{b, c\}\}$ a set of sets

This works fine for small finite sets. Other sets might be defined by indicating how to generate a list of them:

$D = \{1, 2, 4, 8, 16, \dots\}$ the powers of 2

The order of elements is not significant, so $\{x, y\}$ and $\{y, x\}$ are the same set written two different ways. Also, any object is, or is not, an element of a given set——there is no notion of an element appearing more than once in a set. So writing $\{x, x\}$ is just indicating the same thing twice, namely, that x is in the set. In particular, $\{x, x\}$=$\{x\}$.

The expression $e \in S$ asserts that e is an element of set S. For example, $32 \in D$ and blue $\in B$, but Tailspin $\notin A$ ——yet.

Some Popular Sets

Mathematicians have devised special symbols to represent some common sets.

symbol	set	elements
$\emptyset$	the empty set	none
$\mathbb{N}$	nonnegative integers	$\{0, 1, 2, 3, \dots\}$
$\mathbb{Z}$	integers	$\{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$
$\mathbb{Q}$	rational numbers	$\frac{1}{2}$, $-\frac{5}{3}$, 16, etc.
$\mathbb{R}$	real numbers	π, e, -9, $\sqrt{2}$, etc.
$\mathbb{C}$	complex numbers	i, $\frac{19}{2}$, $\sqrt{2} - 2i$, etc.

A superscript "$+$" restricts a set to its positive elements; for example, $\mathbb{R}^+$ denotes the set of positive real numbers. Similarly, $\mathbb{R}^-$ denotes the set of negative reals.

Comparing and Combining Sets

The expression $S \subseteq T$ indicates that set S is a subset of set T, which means that every element of S is also an element of T (it could be that $S = T$). For example, $\mathbb{N} \subseteq \mathbb{Z}$ and $\mathbb{Q} \subseteq \mathbb{R}$ (every rational number is a real number), but $\mathbb{C} \nsubseteq \mathbb{Z}$ (not every complex number is an integer).

As a memory trick, notice that the $\subseteq$ points to the smaller set, just lik a $\leq$ sign points to the smaller number. Actually, this connection goes a little further: there is a symbol $\subset$ analogous to $<$. Thus, $S \subset T$ means that S is a subset of T, but the two are not equal. So $A \subseteq A$, but $A \not\subset A$ for every set A.

There are several ways to combine sets. Let's define a couple of sets for use in examples:

$$X ::= \{1, 2, 3\}$$

$$Y ::= \{2, 3, 4\}$$

- The union of sets X and Y (denoted $X \cup Y$) contains all elements appearing in X or Y or both. Thus, $X \cup Y = \{1, 2, 3, 4\}$.
- The intersection of X and Y (denoted $X \cap Y$) consists of all elements that appear in both X and Y. So $X \cap Y = \{2, 3\}$.
- The set difference of X and Y (denoted $X - Y$) consists of all elements that are in X, but not in Y. Therefore, $X - Y = \{1\}$ and $Y - X = \{4\}$.

The Complement of a Set

Sometimes we are focused on a particular domain, D. Then for any subset, A, of D, we define $\overline{A}$ to be the set of all elements of D not in A. That is, $\overline{A} ::= D - A$. The set

$\overline{A}$ is called the complement of A.

For example, when the domain we're working with is the real numbers, the complement of the positive real numbers is the set of negative real numbers together with zero. That is,

$$\overline{\mathbb{R}^+} = \mathbb{R}^- \cup \{0\}.$$

It can be helpful to rephrase properties of sets using complements. For example, two sets, A and B, are said to be *disjoint* iff they have no elements in common, that is, $A \cap B = \emptyset$. This is the same as saying that A is a subset of the complement of B, that is, $A \subseteq \overline{B}$.

Cardinality

The *cardinality* of a set A is the number of elements in A and is denoted by $|A|$. For example,

$|\emptyset| = 0$,

$|\{1, 2, 4\}| = 3$, and

$|\mathbb{N}|$ is infinite.

The Power Set

The set of all the subsets of a set, A, is called the *power set*, $\wp(A)$, of A. So $B \in \wp(A)$ iff $B \subseteq A$. For example, the elements of $\wp(\{1, 2\})$ are $\emptyset$, $\{1\}$, $\{2\}$ and $\{1, 2\}$.

More generally, if A has n elements, then there are 2^n sets in $\wp(A)$. In other words, if A is finite, then $|\wp(A)| = 2^{|A|}$. For this reason, some authors use the notation 2^A instead of $\wp(A)$ to denote the power set of A.

Sequence

Sets provide one way to group a collection of objects. Another way is in a sequence, which is a list of objects called terms or components. Short sequences are commonly described by listing the elements between parentheses; for example, (a,b,c) is a sequence with three terms.

While both sets and sequences perform a gathering role, there are several differences.

- The elements of a set are required to be distinct, but terms in a sequence can be the same. Thus, (a,b,a) is a valid sequence of length three, but $\{a, b, a\}$ is a set with two elements——not three.
- The terms in a sequence have a specified order, but the elements of a set do not. For example, (a, b, c) and (a, c, b) are different sequences, but $\{a, b, c\}$ and $\{a, c, b\}$ are the same set.
- Texts differ on notation for the *empty sequence*; we use λ for the empty sequence and $\emptyset$ for the empty set.

Cross Products

The product operation is one link between sets and sequences. A product of sets, $S_1 \times S_2 \times \ldots \times S_n$, is a new set consisting of all sequences where the first component is drawn from S_1, the second from S_2, and so forth. For example, $\mathbb{N} \times \{a, b\}$ is the set of all pairs whose first element is a nonnegative integer and whose second element is an a or a b:

$$\mathbb{N} \times \{a, b\} = \{(0, a), (0, b), (1, a), (1, b), (2, a), (2, b), \ldots\}$$

A product of n copies of a set S is denoted S^n. For example, $\{0, 1\}^3$ is the set of all 3-bit sequences:

$$\{0, 1\}^3 = \{(0, 0, 0), (0, 0, 1), (0, 1, 0), (0, 1, 1), (1, 0, 0), (1, 0, 1), (1, 1, 0), (1, 1, 1)\}$$

2.6.2 Set Builder Notation

An important use of predicates is in set builder notation. We'll often want to talk about sets that cannot be described very well by listing the elements explicitly or by taking unions, intersections, etc., of easily-described sets. Set builder notation often comes to the rescue. The idea is to define a set using a predicate; in particular, the set consists of all values that make the predicate true. Here are some examples of set builder notation:

$$A ::= \{n \in \mathbb{N} | n \; is \; a \; prime \; and \; n = 4k + 1 \; for \; some \; integer \; k\}$$

$$B ::= \{x \in \mathbb{R} | x^3 - 3x + 1 > 0\}$$

$$C ::= \{a + bi \in \mathbb{C} | a^2 + 2b^2 \leq 1\}$$

The set A consists of all nonnegative integers n for which the predicate

"n is a prime and n=4k+1 for some integer k"

is true. Thus, the smallest elements of A are:

5,13,17,29,37,41,53,57,61,73,...

Trying to indicate the set A by listing these first few elements wouldn't work very well, even after ten terms, the pattern is not obvious! Similarly, the set B consists of all real numbers x for which the predicate

$$x^3 - 3x + 1 > 0$$

is ture.In this case, an explicit description of the set B in terms of intervals would require solving a cubic equation. Finally, set C consists of all complex numbers $a + bi$ such that:

$$a^2 + 2b^2 \leq 1$$

This is an oval-shaped region around the origin in the complex plane.

2.6.3 Proving Set Equalities

Two sets are defined to be equal if they contain the same elements. That is ,$X = Y$ means that $z \in X$ if and only if $z \in Y$, for all elements, z. (This is actually the first of the ZFC axioms.) So set equalities can often be formulated and proved as "iff" theorems. For example:

Theorem 2.6.1 (*Distributive Law* for Sets). Let A, B, and C be sets. Then:

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \qquad (2.5)$$

Proof. The equality (2.5) is equivalent to the assertion that

$$z \in A \cap (B \cup C) \quad \text{iff } z \in (A \cap B) \cup (A \cap C) \qquad (2.6)$$

for all z. This assertion looks very similar to the Distributive Law for AND and OR that we proved in Section 1.4(equation 1.6). Namely, if P, Q, and R are propositions, then

[P AND (Q OR R)] IFF [(P AND Q) OR (P AND R)] (2.7)

Using this fact, we can now prove (2.6) by a chain of iff's: