

# 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 whole 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 Euclid, 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

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

### 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  $P \text{ IMPLIES } Q$ . There is only one case where  $P$  and  $P \text{ IMPLIES } Q$  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

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

### 规则 2.1.2

$$\frac{P \text{ 蕴涵 } Q, Q \text{ 蕴涵 } R}{P \text{ 蕴涵 } R}$$

### Rule 2.1.3

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

### 规则 2.1.3

$$\frac{P \text{ 蕴涵 } Q, \text{ 非 } Q}{\text{ 非 } P}$$

### Rule 2.1.4

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

### 规则 2.1.4

$$\frac{\text{ 非 } P \text{ 蕴涵 } \text{ 非 } Q}{Q \text{ 蕴涵 } P}$$

On the other hand,

### Non-Rule.

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

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 its 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  $P \text{ IMPLIES } Q$  is equivalent to its contrapositive  $\text{NOT}(Q) \text{ IMPLIES } \text{NOT}(P)$  by considering all 4 possible assignments of T or F to P and Q. In each of the four cases, we showed that  $P \text{ IMPLIES } Q$  is true if and only if  $\text{NOT}(Q) \text{ IMPLIES } \text{NOT}(P)$  is true. For example, if  $P = \text{True}$  and  $Q = \text{False}$ , then both  $P \text{ IMPLIES } Q$  and  $\text{NOT}(Q) \text{ IMPLIES } \text{NOT}(P)$  are false, thereby establishing that  $(P \text{ IMPLIES } Q) \text{ IFF } (\text{NOT}(Q) \text{ IMPLIES } \text{NOT}(P))$  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“ $P \rightarrow Q$ ”等价于其对换命题“ $(\neg Q) \rightarrow (\neg P)$ ”。在四种情形中，我们都证明了“ $P \rightarrow Q$ ”为真当且仅当“ $(\neg Q) \rightarrow (\neg P)$ ”为真。例如，如果 $P=T, Q=F$ ，那么“ $P \rightarrow Q$ ”和“ $(\neg Q) \rightarrow (\neg P)$ ”都为假，由此证实在这种情形下，“ $P \rightarrow Q$ ”当且仅当“ $(\neg Q) \rightarrow (\neg P)$ ”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 " $P \rightarrow Q$ ".

有着“如果P, 那么Q”形式的命题称为蕴含。该蕴含常重新表述为“P 蕴含 Q”或“ $P \rightarrow Q$ ”。

Here are some examples of implications:

下面是一些蕴含示例：

- (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  $P \text{ IMPLIES } Q$ , there are two cases to consider:  $P$  is true and  $P$  is false. The case when  $P$  is false is easy since, by definition,  $F \text{ IMPLIES } Q$  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  $P \text{ IMPLIES } Q$ :

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 $P$ ”。
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 scratchwork 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  $\square$  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  $P \text{ IMPLIES } Q$ , 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 " $P \text{ IMPLIES } Q$ " is logically equivalent to its contrapositive

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

我们已经知道蕴涵“ $P$ 蕴涵 $Q$ ”在逻辑上等价于其对换命题

$$\text{“非}Q\text{蕴涵非}P\text{”}$$

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”，所以常把它简称为“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.

## 2.4.2 Method #2: Construct a Chain of IFFs

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.

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.

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

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

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

where  $\mu$  is the mean of the values:

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

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.)

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

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

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

$$(x_1 - \mu)^2 + (x_2 - \mu)^2 + \dots + (x_n - \mu)^2 = 0 \quad (2.3)$$

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

$$\text{Every term on the left hand side of (2.3) is zero.} \quad (2.4)$$

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.