CS 70离散数学与概率论
2024年秋季课程笔记注2

1 证明

在科学中，证据是通过实验积累起来的，以证明陈述的正确性.相比之下，数学旨在获得更绝对的确定性。数学证明为确定陈述的正确性提供了手段。证明非常有力，在某些方面像计算机程序。的确，在这两个概念之间有一个深刻的历史联系，我们将在这门课程中谈到——
计算机的发明与大约一个世纪前对数学证明概念的探索密切相关。

那么，我们想要证明哪些类型的“计算机科学相关”陈述呢? 以下是两个示例：
（1）程序P是否在每个输入时都停止?（2）程序P是否正确计算函数f（x），即对于每个x,它是否对输入x输出f（x）?注意，这些语句中的每一个都涉及程序在无穷多个输入上的行为。对于这样的语句，我们可以通过测试它对x的许多值成立来尝试提供其真实性的证据。不幸的是，这并不能保证该语句适用于我们没有测试的x的无穷多个值!为了确定这句话是真的，我们必须提供严谨的证明。

那么什么是证据呢?证明是一个有限的步骤序列，称为逻辑推论，它确定所需陈述的真实性。特别地，证明的力量在于，使用有限的方法，我们可以保证无穷多情况下的陈述的真实性。

更具体地，证明通常构造如下。回想一下，有些陈述，称为公理或假设，我们无需证明就接受（我们必须从某个地方开始）。从这些公理开始，证明由一系列逻辑推论组成：应用逻辑规则的简单步骤。这导致一系列语句，其中如果先前的语句为真，则每个连续的语句必然为真。此属性由逻辑规则强制执行：每项陈述均取自先前陈述。这些逻辑规则是对被认为是人类思维基础的定律的正式提炼。它们在计算机设计中起着核心作用，从数字逻辑设计或数字电路设计的基本原理开始。在更高级的层次上，这些逻辑规则在人工智能中扮演着不可或缺的角色，人工智能的最终目标之一是在计算机上模仿人类的思维。

本说明的组织结构。我们从第2节开始，设置符号并陈述本注释中使用的基本数学事实。接下来介绍四种不同的证明技术：直接证明（第3节）、对立证明（第4节）、矛盾证明（第5节）和案例证明（第6节）。然后，我们简要讨论证明的常见陷阱和文体建议（分别为第7节和第8节）。我们在第9节结束练习。

2 符号和基本事实

在本注释中，我们使用以下符号和基本的数学事实。令Z表示整数的集合，
即Z = {..., −2, −1, 0, 1, 2, ...}，而N是自然数的集合，N = 0, 1, 2,回想一下，
两个整数的乘积是一个整数，即整数的集合在加法和乘法下是闭的。这些

自然数集在加法和乘法下也是闭的。

给定整数a和b,我们说a除b（记为ab）当且存在整数q,使得b=aq。例如，2 10,因为存在整数q = 5,使得10 = 5 2。我们说一个自然数p2是素数，如果它只能被1和它本身整除。

最后，我们使用符号：=来表示定义。例如，q：= 6 将变量 q 定义为具有值6。

3 直接校对

有了Note
0中的命题逻辑语言，我们现在可以讨论证明技术，真正的乐趣可以开始了。你准备好了吗?如果是的话，这是我们的第一个技术，称为直接证明。在本节中，请牢记我们的目标是给出清晰简明的证明。让我们从一个非常简单的例子开始。

定理2.1。*对任意a,b,c ∈Z,若a|b和a|c,则a|（b+c）.*

概念检查! 令P（x,y）表示“x | y”。使自己确信上述声明等同于

（igana, b, c ∈Z）（P（a, b）为P（a, c））=⇒ P（a, b + c））。

在高层次上，直接证明如下进行。对于每个x,我们试图证明的命题是P（x）=Q（x）的形式。对此的直接证明首先假设P（x）为x的一般值，并最终通过暗示链得出Q（x）：

直接校对

*目标：*证明P=Q。*方法*：假设P

.

因此Q

*定理2.1的证明。*设a|b和a|c,即存在整数q1和q2,使得b=q1a,c=q2a。那么，b + c = q1a + q2a =（q1 + q2）a。由于Z在加法下是闭的，所以我们得出（q1+q2）∈Z,因此a|（b+c）是合乎需要的。

很简单，对吧? □

等等，前面我们说定理2.1等价于（a,b,cZ）（P（a,b）P（a,c））=P（a,b+c））;在上面的证明中，我们在哪里遇到了量词?关键的见解是证明没有假定a、b和c的任何特定值;确实，对于任意的a,b,c∈Z,我们的证明是成立的!因此，我们确实证明了我们所期望的主张。

---

*概念检查!*给出以下陈述的直接证据：对任意a,b,c∈Z,若a|b和a|c,则

a |（b−c）。

让我们尝试一些更具挑战性的东西。

定理2.2。*设 0 < n < 1000 为整数。如果n的数字之和可被9整除，则n可被9整除。*

请注意，此陈述等效于

（zin ∈Z+）（n < 1000）=⇒（可被 9 整除的 n 位数之和=⇒ n 可被 9 整除），

式中，Z+表示一组正整数，1,2,现在进行类似的证明——我们从
假设，对于n的一般值，n的位数之和可被9整除。然后我们进行一系列暗示，得出n本身可被9整除的结论。

*定理2.2的证明*设n（十进制）写为n=abc,即n=100a+10b+c。假定n的位数和可被9整除，即

$k \in Z$, *使得* $a+b+c=9k$。

（1）将99a + 9b加到方程（1）的两侧，我们得到

100a+10b+c=n=9k+99a+9b=9（k+11a+b）。

我们得出了n可被9整除的结论。 □

定理2.2的逆向也是正确的吗?回想一下，P=Q的逆是Q=P。定理2.2的反面说，对于任何0<n<1000的整数，如果n可被9整除，则n的位数和可被9整除。

定理2.3（与定理2.2相反）。 *设 0 < n < 1000 为整数。如果n可被9整除，则n的数字之和可被9整除。*

*证明。*假定n可被9整除。我们对n的数字使用与定理2.2的证明相同的符号。我们进行如下操作。

$$
\begin{aligned}
&n \text{ 可被 } 9 \text{ 除尽} \Rightarrow n = 9l, \text{其中 } l \in Z \\
&\Rightarrow 100a + 10b + c = 9l \\
&\Rightarrow 99a + 9b + (a + b + c) = 9l \\
&\Rightarrow a + b + c = 9l - 99a - 9b \\
&\Rightarrow a + b + c = 9(l - 11a - b) \\
&\Rightarrow a + b + c = 9k, \text{对于 } k = l - 11a - b \in Z
\end{aligned}
$$

我们得出a+b+c可被9整除的结论。 □

我们现在来谈谈这个故事的寓意。我们已经证明了定理2.2及其逆定理2.3。这意味着n的数字之和可被9整除当且仅当n可被9整除;换句话说，这两个语句在逻辑上是等价的。因此，关键的教训是：每当你希望证明一个等价PQ时，总是分别显示P=Q和Q=P（正如我们在这里做的那样）。

□⇒ ⇒ ⇒

4 对置证明

我们现在开始我们的第二种证明技术。回想一下我们关于命题逻辑的讨论，□□ P =□ Q □□□□□□Q =⇒P。然而，有时候，Q =⇒ P比P =⇒ Q更易于证明。因此，对位证明通过证明Q =⇒ P而不是P =⇒ Q来进行。

对置证明

*目标：*证明P =⇒ Q。*方法：*假设Q

.

因此，P

结论：Q =⇒ P,相当于P =⇒ Q。

现在考虑以下定理：

定理2.4. *设n为正整数，设d除以n。如果n是奇数，则d是奇数。*

通过直接证明的方法来证明这一点似乎很困难;在步骤1中，我们假设n是奇数，但是然后呢?另一方面，通过对位的方法则容易得多。

---

*概念检查!*定理2.4的反式是什么?（回答：如果d为偶数，则n为偶数。）

---

*定理2.4的证明*我们按对位法进行。假定d是偶数。然后，根据定义，对于某些k Z,d = 2k。 因为d n,那么对于某个l Z,n = dl。结合这两个陈述，我们有n=dl=（2k）l=2（kl）。我们得出了n是偶数的结论。 □

请注意，这一次，我们的证明的第一行陈述了我们的证明技术——
这是任何证明的良好实践，类似于注释代码是编程时的良好实践。像这样陈述你的证明技巧对你的读者理解你的证明下一步将何去何从是一个巨大的帮助。（让我们不要忘记，理解你证明的读者，比如助教或讲师，更有可能给你一个好的分数!）

作为对置证明的又一例证，我们将证明一个著名的定理“鸽子洞原理”。虽然这个定理的陈述可能看起来很简单，但它有令人吃惊的结果。

定理2.5（Pigeonhole原理）。 *设n和k为正整数。将 n 个对象放入 k 个框。如果 n > k,则至少一个框必须包含多个对象。*

这个定理的名字来源于假设n个物体是鸽子，我们试图把它们放在鸽子洞里。

*定理2.5的证明。*我们按对位法进行。如果所有框最多包含一个对象，则对象的数量最多为框的数量，即n ≤ k。 □

这个定理的效用源于这样一个事实，即无论盒子中物体的配置如何，它都成立。在对象以复杂的方式放置在盒子中的情况下，该定理的结论可以是非平凡的。

下面是一个示例。在互联网上快速搜索发现，人类头上的毛发数量平均大约是100000。因此，我们可以合理地确信，没有一个人头上的毛发超过50万根。另一方面，旧金山的人口（截至2016年）超过80万人。如果我们把旧金山的居民看作是“鸽子”，把住户头上的头发数看作是他或她掉进去的“盒子”，那么鸽子洞原理让我们得出一个有趣的事实：旧金山有两个人头上头发的数量完全一样!

5 矛盾证明

在这篇笔记中我们讨论的所有证明技巧中，或许最难抗拒这一技巧的吸引力;毕竟，谁不想使用一种叫做还原荒谬的方法，即还原到荒谬呢?矛盾证明的思想是假设你想要证明的声明是错误的（是的，这似乎是倒退的，但请忍受我们）。然后，你证明这导致了完全无稽之谈的结论：矛盾因此，你方得出结论，你的主张实际上一定是真实的。

---

*概念检查!*矛盾证明的关键在于，如果一个命题不是假的，那么它一定是真的。上一堂课的哪条定律体现了黑白对陈述的解释?

矛盾证明目标：为了证明
P.*方法：*假设P

.
R
.
^*R*

*结论：−P =⇒ −R,是一个矛盾。*因此，P.

□□□ ´P =□ ´R ≤ R ≡ False（假）。反义词
因此，该声明为真=⇒ P。
现在让我们来试用这种证明技术。请注意，在这样做时，我们延续了悠久的遗产——[1]
下面定理的证明可以追溯到古希腊数学家亚历山大（Alexandria）的欧几里德（Euclid of Alexandria）的2000多年前。

定理2.6.*有无穷多个素数。*

为了理解矛盾的力量，让我们停下来思考一下，我们如何通过不同的证明技术，例如直接证明，来证明定理2.6。看起来很困难，对吧?如何构造无穷多个素数?然而，关于矛盾的显著之处在于，如果我们假设这个陈述是错误的，也就是说，只有有限的许多质数，那么坏的事情就会发生。

为了继续，我们现在陈述一个简单引理，它对于证明定理2.6是方便的。它的证明将推迟到以后的讲座，我们将在其中学习归纳法。

1或许值得在此停下来欣赏一下这一声明的真实规模——毕竟，在数千年之后，我们人类遗产中有多少方面仍然相关?音乐?时尚?所有这些都随着时间的推移而很快过时。但在某种意义上，数学是永恒的。

引理2.1. *每个大于1的自然数要么是素数，要么有一个素因子。*

*定理2.6的证明*我们以矛盾的方式前进。假设定理2.6是错误的，即只有有限多个素数，比方说k个素数。然后，我们可以列举它们：p1,p2,p3,...，pk.

现在，定义数字 q：= p1 p2 p3。..pk+1,它是所有素数加一的乘积。我们认为q不能是素数。为什么?因为根据定义，它比所有的素数p1到pk都大!通过引理2.1,我们因此得出结论，q有一个素因子p。这将是我们的声明R。

接下来，因为p1、p2、p3、...，pk是所有的素数，p必须等于其中之一;因此，p除以r：= *p1 p2 p3 ...;*结因此，p | q 和p | r 表示 p | (q−r)。但q−r = 1,意味着p ≤ 1,因此p不是素数;这是声明R。因此，正如我们所期望的，我们有一个矛盾的R、R。 □

现在我们已经热身了，让我们来讨论另一个涉及矛盾的经典证明。回想一下，有理数是可以用两个整数之比表示的数。例如，2、3和9为有理数 3 5 16 编号。 另一方面，不能用分数表示的N√数称为无理数。 现在，两个怎么样?你认为这是合理的还是非理性的?答案如下。

定理2.7. *√2是不合理的。*

在提供证据之前，让我们问一个关键问题：为什么矛盾应该是一个好的候选证明技巧来尝试这里?那么，请考虑一下：定理2.6和定理2.7有共同的共同点——在这两种情况下，我们希望证明某些东西是不存在的。例如，对于定理2.6,我们希望证明最大素数不存在，对于定理2.7,我们希望证明整数a和*b满足2=a/b不存在*。一般来说，证明某事不存在似乎很困难。但是这个实际上是证明矛盾的背景。

为了证明定理2.7,我们使用下面的简单引理。在第九节中，我们要求你证明引理2.2。

引理2.2。 *如果a2为偶数，则a为偶数。*

定理2.7的证明 我们以矛盾的方式前进。假设√2是有理的。通过比率的√定义-nal数，存在除1外没有公因子的整数a和b,使得2 = a/b。 让我们的断言R声明a和b不共享公共因素。

现在，对于任意数x和y,我们知道x=y=x2=y2。因此2 = a2/b2。两边都乘以b2,我们得到a2 = 2b2。由于b是整数，因此b2是整数，因此a2是偶数（根据均匀度的定义）。在引理2.2中，我们得到a是偶数。换句话说，存在整数c,使得a=2c。

综合到目前为止的所有事实，我们得到2b2=4c2或b2=2c2。由于c是整数，因此c2是整数，因此b2是偶数。因此，再次应用引理2.2,我们得出b是偶数的结论。

但我们已经证明a和b都是偶数。特别地，这意味着它们共享公因子2。这意味着R。我们得出了R、R成立的结论;因此，正如我们所期望的，我们有一个矛盾。 □

6 案例证明

这里有一个可以逗你兴致勃勃的证据;它依赖于另一种称为案例证明的证明技术，我们将在本节非正式地谈到这种技术。具体而言，案例证明背后的理念如下：有时，当我们希望证明一项主张时，我们不知道一组可能的案例中哪一个是正确的，但我们

知道其中至少有一个是真实的。我们能做的是证明这两种情况的结果;那么，总的声明显然必须成立。

定理2.8. *存在无理数x和y,使得xy是有理的。*

*证明。*我们按个案处理。注意，该定理的陈述是由存在量词量化的：因此，为了证明你的主张，只要证明一个x和y就足够了，因为x是有理的。为此，让我们x^y *x=2且y=2*。让我们把我们的证明分成两个例子，其中必须有一个是正确的：

(a) $\sqrt{2}^{\sqrt{2}}$是合理的，或

(b) $\sqrt{2}^{\sqrt{2}}$是不合理的。

（情况（a））首先假设$\sqrt{2}^{\sqrt{2}}$是合理的。但这立即产生了我们的主张，因为x和y是无理数，所以xy是有理的。

（情况（b））现在假设$\sqrt{2}^{\sqrt{2}}$是不合理的。我们对x和y的第一次猜测并不完全正确，但现在我们有一个新的无理数来玩，$\sqrt{2}^{\sqrt{2}}$.那么，让我们尝试设置$x = \sqrt{2}^{\sqrt{2}}$且$y = \sqrt{2}$.然后，

$$xy = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\sqrt{2}} = \sqrt{2}^{2} = 2,$$

其中第二等式来自公理（xy）z=xyz。但现在我们再次从两个无理数x和y开始，得到有理数xy。

由于情形（a）或情形（b）之一必须成立，因此我们得出结论，定理2.8的陈述是正确的。 □

在结束之前，让我们指出上述证明的一个特点。 x和y的实际数字是多少满足定理2.8的要求。是否为$x = \sqrt{2}$和$y = \sqrt{2}$?或者$x = \sqrt{2}^{\sqrt{2}}$且$y = \sqrt{2}$?嗯，因为我们做了一个案例分析，我们不清楚这两个选择中哪一个实际上是正确的。换句话说，我们刚刚演示了一个非构造性证明：我们已经证明了某些对象X的存在，但是没有显式地揭示X本身是什么!

7 编写校样时的常见错误

写出简明扼要的证明是件了不起的事，而且可以说是人们所能达到的智力启蒙的最高形式之一。它要求你的头脑批判性地反思它自己的内部运作（即你的思维过程），并将它们重新组织成连贯的、逻辑的思维序列。换句话说，你的心智正在一个非常基本的层次上自我改进，远远超越了计算机科学或任何特定研究领域的界限。这个训练的好处将触及你生活的方方面面，正如你所知道的;的确，它会塑造你对待生活本身的方式。

与任何这样的基本成就一样，发展写出严格的证明的能力可能是你在大学将面临的最困难的学习挑战之一，所以如果它给你带来麻烦，不要绝望;你并不孤单。在这里，千方百计地实践是无可替代的。为了帮助您开始，我们现在提出了一些关于在撰写校样中的常见陷阱的红旗。让我们从一个简单但常见的错误开始。

声明： $-2 = 2$。

证明?假设−2 = 2。将两侧平方，则（−2）2 = 22或4 = 4,即为真。我们得出结论：−2 = 2（根据需要）。**加上**

这个定理显然是错误的，那么我们做错了什么呢?我们的算术是正确的，每一步都严格遵循上一步。因此，错误必定在证明的开头，在那里我们做出一个厚颜无耻的假设：那2=2。但是，等等，这不是我们试图证明的陈述吗?完全正确。换句话说，为了证明P “ 2 = 2”，我们只是证明了P = True,这与证明P不同。第 1 课：撰写证明时，不要假定你想要证明的声明!

第2课是关于数字0：特别是，不要忘记考虑变量取值为0的情况。否则，可能会发生这种情况：

声明：1 = 2。

证明?设对于整数x,y∈Z,x=y。然后，

$$x2 - xy = x2 - y2 \text{（因为} x = y \text{）} x(x - y) = (x + y)(x - y)$$

$$x = x + y \text{（两侧除以} x - y \text{）}$$

$$x = 2 \text{倍}$$

设置 x = y = 1 得出声明。**加上**

但是，很明显1=2,除非你的小学老师对你撒谎。我们哪里搞错了?在推导第三个等式时，我们除以（x y）。在我们的环境中（x y）值是多少?零。除以零的定义不明确;因此，第三个等式不成立。

第3课说在混合负数和不等式时要小心。例如：

声明：4≤1。

证明?我们知道 −2 ≤ 1;对该不等式的两侧进行平方，得到4 ≤ 1。**加上**

概念检查! 要了解此证明失败的原因，请问自己： 如果a b,那么a b一定是真的吗?你能举个反例吗?

另外，不要忘记不等式乘以负数会颠倒不等式的方向!例如，将 −2 < 5 的两侧乘以 −1 得到 2 > −5,正如您所期望的。

8 证据的风格和实质

最后，我们提出一些一般性的建议。首先，养成在写下证据的下一句之前仔细思考的习惯。如果你不能清楚地解释为什么这个步骤是合理的，那么你就是在飞跃，你需要回头再想想。理论上，证明中的每一步都必须通过引用定义或一般公理来证明其合理性。在实践中，一个人必须这么做的深度是品味的问题。例如，我们可以将步骤“因为a是整数，（2a2+2a）是整数”分解为多个步骤。[练习：它们是什么?]只有当你绝对确信（1）它是正确的，（2）读者会自动同意它是正确的，才可以在没有证据的情况下陈述理由。

注意，在√2是无理的证明中，我们使用了这样的结果：“对于任何整数n,如果n2是偶数，那么*n为偶数，"两次*。这表明在许多证据中它可能是一个有用的事实。在更复杂的证明中有用的辅助结果叫做引理。把一个很长的证明分解成

几个引理。这与将大型编程任务划分成较小的子例程的方式类似。此外，使每个引理（像每个子程序一样）尽可能通用，以便可以在其他地方重用。

引理和定理之间的分界线并不明确。通常，当写论文时，定理是那些你想要从论文中“导出”到世界其他地方的命题，而引理是局部用于证明你的定理的命题。然而，有一些引理（例如，抽运引理和提升引理）可能比它们用来证明的定理更著名和更重要。

最后，你应该记住，这次讲座的重点不是我们证明的具体陈述，而是不同的证明策略，以及它们的逻辑结构。确保您清楚地理解;当你自己写作业和考试的证明时，你会用到它们。

9 练习

1. 推广定理2.2的证明，使其适用于任何正整数n。（提示：假设n具有

   k个数字，并为n的数字写入a_i，使得$n = \sum_{i=0}^{k-1} a_i 10^i$。）
2. 证明引理2.2。（提示：首先尝试直接证明。然后，尝试对位。哪种证明方法更适合证明这个引理?）