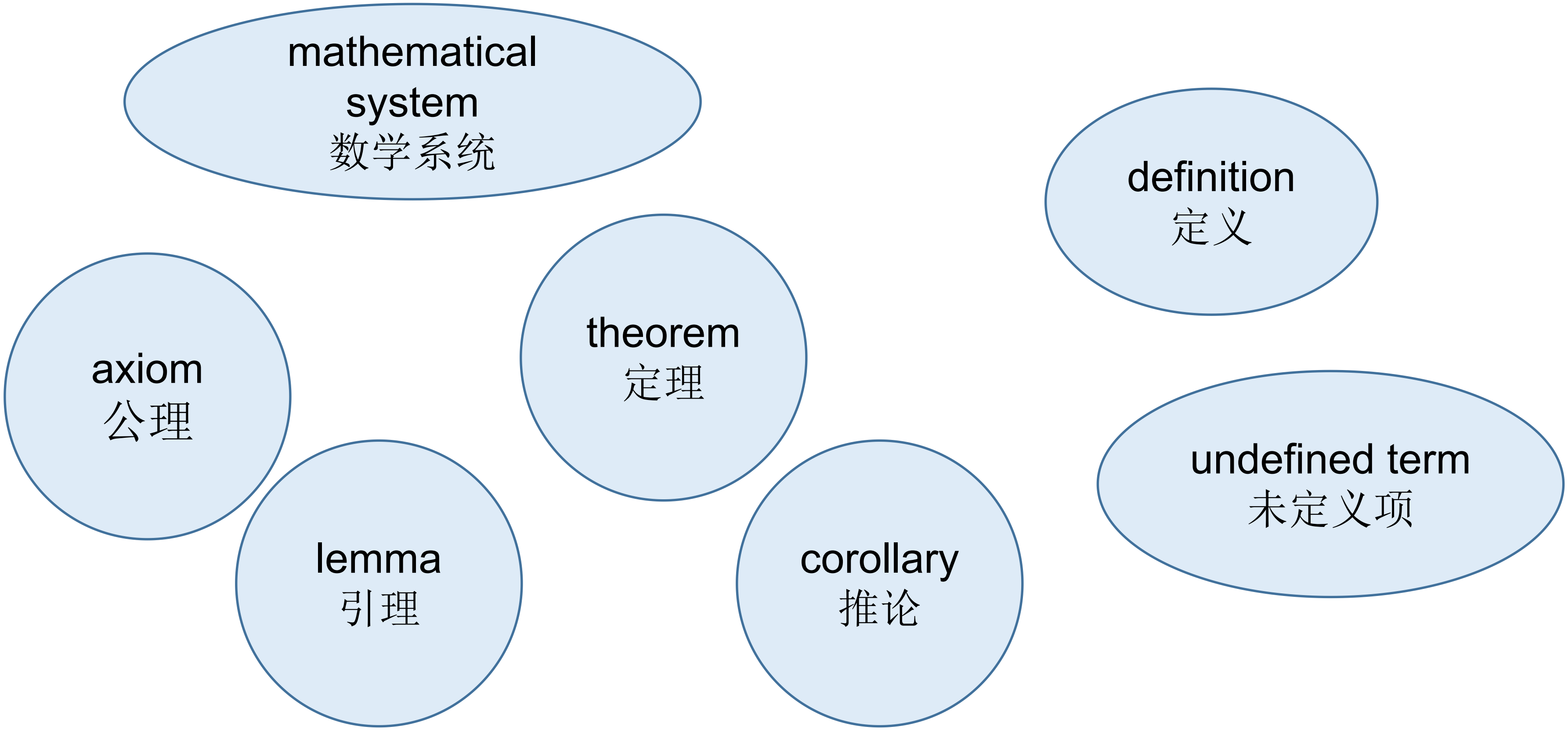
Chapter 2 Proofs 证明

Lu Han

hl@bupt.edu.cn

2.1 Mathematical Systems (数学系统), Direct Proofs (直接证明), and Counterexamples (反例)



mathematical system
数学系统

definition
定义

axiom
公理

theorem
定理

lemma
引理

corollary
推论

undefined term
未定义项

Direct Proof 直接证明

Theorem are often of the **form**

For all $x_1, x_2,\ldots, x_n$, if $p(x_1, x_2, \ldots, x_n)$ then $q(x_1, x_2, \ldots, x_n)$.

A direct proof assumes that $p(x_1, x_2, \ldots, x_n)$ is true and then using $p(x_1, x_2, \ldots, x_n)$ as well as other axioms, definitions, previously derived theorems, and rules of inference, shows directly that $q(x_1, x_2, \ldots, x_n)$ is true.

Definition 2.1.7 An integer n is even if there exists an integer k such that $n=2k$. An integer n is odd if there exists an integer k such that $n=2k+1$.

Example 2.1.10 Given a direct proof of the following statement: For all integers m and n, if m is odd and n is even, then $m+n$ is odd.

m is odd and n is even (Hypotheses)
…
$m+n$ is odd (Conclusion)

Definition 2.1.7 An integer n is even if there exists an integer k such that $n=2k$. An integer n is odd if there exists an integer k such that $n=2k+1$.

Example 2.1.10 Given a direct proof of the following statement: For all integers m and n, if m is odd and n is even, then $m+n$ is odd.

Proof Let m and n be arbitrary integers, and suppose that m is odd and n is even. We prove that $m + n$ is odd. By definition, since m is odd, there exists an integer k_1 suchthat $m = 2k_1+1$. Also, by definition, since n is even, there exists an integer k_2 such that $n = 2k_2$. Now the sum is

$m + n = (2k_1+1) + (2k_2) = 2(k_1 + k_2) + 1.$

Thus, there exists an integer k (namely $k = k_1 + k_2$) such that $m + n = 2k+1$.

Therefore, $m + n$ is odd.

Example 2.1.11 Give a direct proof of the following statement.

For all sets X, Y, and Z, $X \cap (Y - Z) = (X \cap Y) - (X \cap Z)$.

X, Y, and Z are sets (Hypotheses)

…

$X \cap (Y - Z) = (X \cap Y) - (X \cap Z)$ (Conclusion)

For every x,

if $x \in X \cap (Y - Z)$, then $x \in (X \cap Y) - (X \cap Z)$,

and

if $x \in (X \cap Y) - (X \cap Z)$, then $x \in X \cap (Y - Z)$.

How to prove two sets are equal ?

Two sets A and B are equal and we write $A = B$ if A and B have the same elements. To put it another way, $A = B$ if the following two conditions hold:

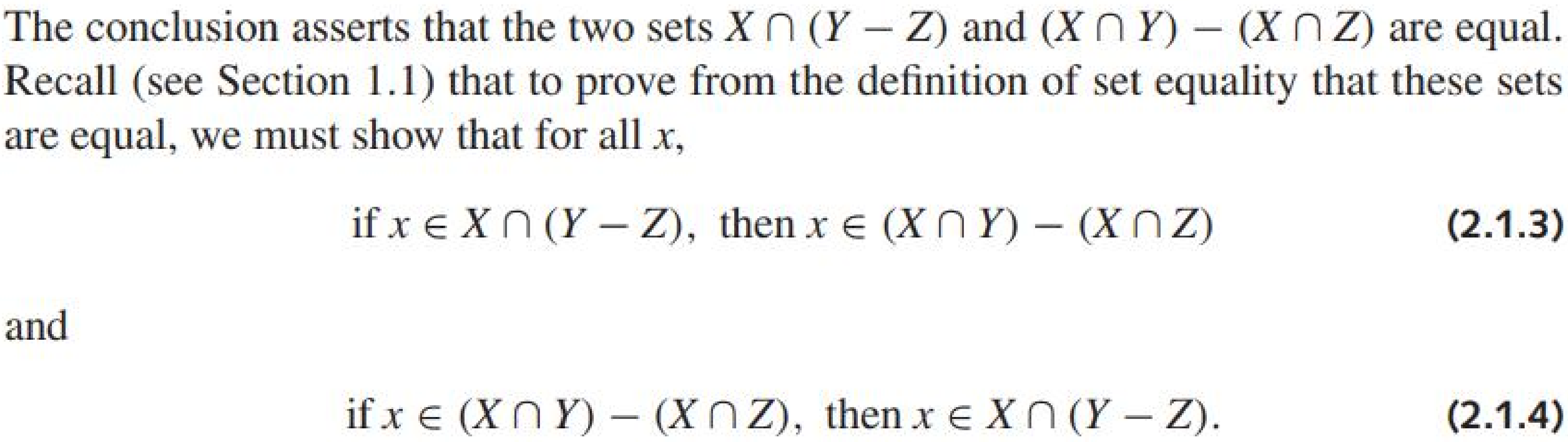
- For every x, if $x \in A$, then $x \in B$,

and

- For every x, if $x \in B$, then $x \in A$.

Example 2.1.11 Give a direct proof of the following statement.

For all sets X, Y, and Z, $X \cap (Y - Z) = (X \cap Y) - (X \cap Z)$.



The conclusion asserts that the two sets $X \cap (Y - Z)$ and $(X \cap Y) - (X \cap Z)$ are equal. Recall (see Section 1.1) that to prove from the definition of set equality that these sets are equal, we must show that for all x,

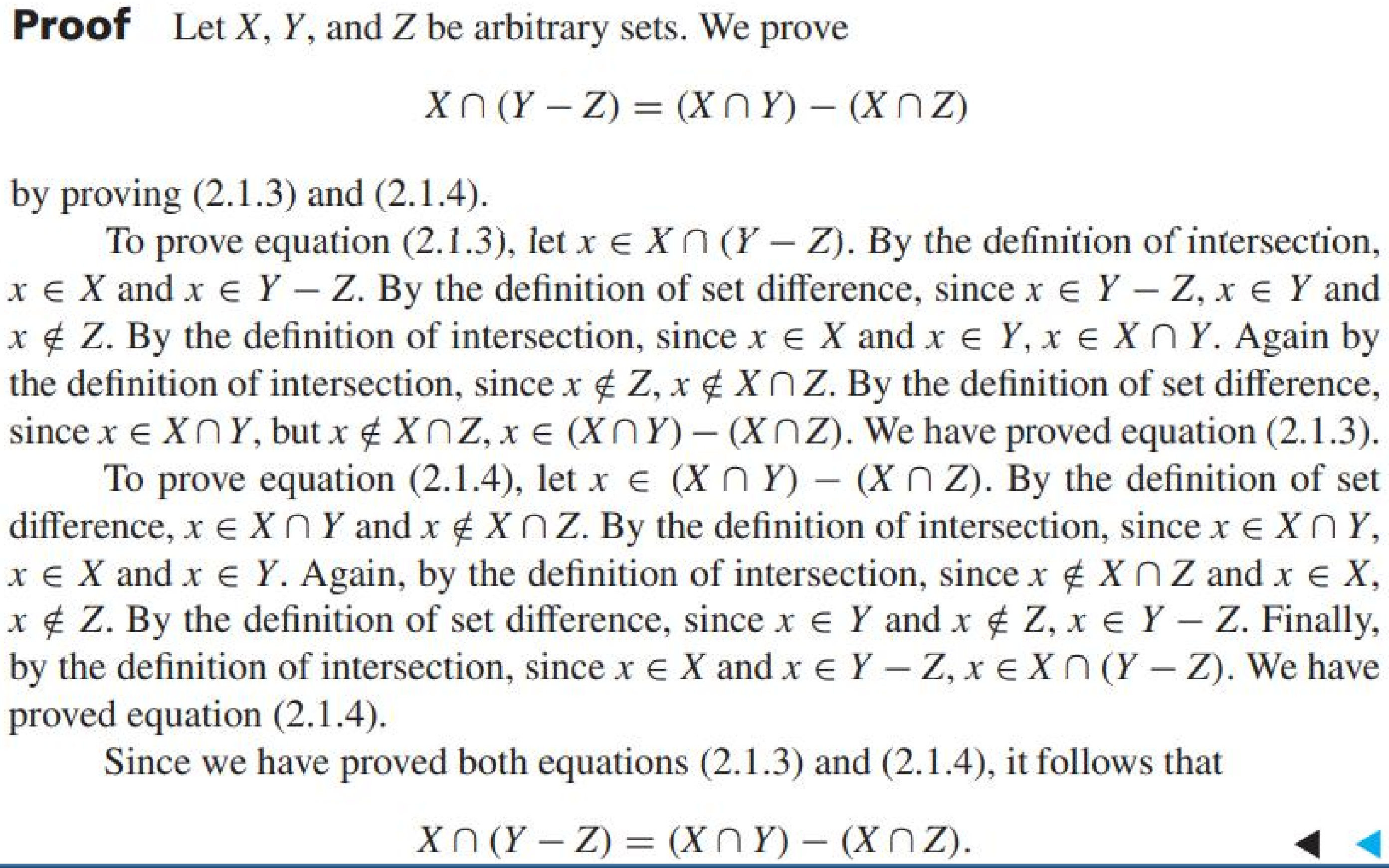
$$\text{if } x \in X \cap (Y - Z), \text{ then } x \in (X \cap Y) - (X \cap Z) \qquad \textbf{(2.1.3)}$$

and

$$\text{if } x \in (X \cap Y) - (X \cap Z), \text{ then } x \in X \cap (Y - Z). \qquad \textbf{(2.1.4)}$$

Example 2.1.11 Give a direct proof of the following statement.

For all sets X, Y, and Z, $X \cap (Y - Z) = (X \cap Y) - (X \cap Z)$.



Proof Let X, Y, and Z be arbitrary sets. We prove

$$X \cap (Y - Z) = (X \cap Y) - (X \cap Z)$$

by proving (2.1.3) and (2.1.4).

To prove equation (2.1.3), let $x \in X \cap (Y - Z)$. By the definition of intersection, $x \in X$ and $x \in Y - Z$. By the definition of set difference, since $x \in Y - Z$, $x \in Y$ and $x \notin Z$. By the definition of intersection, since $x \in X$ and $x \in Y$, $x \in X \cap Y$. Again by the definition of intersection, since $x \notin Z$, $x \notin X \cap Z$. By the definition of set difference, since $x \in X \cap Y$, but $x \notin X \cap Z$, $x \in (X \cap Y) - (X \cap Z)$. We have proved equation (2.1.3).

To prove equation (2.1.4), let $x \in (X \cap Y) - (X \cap Z)$. By the definition of set difference, $x \in X \cap Y$ and $x \notin X \cap Z$. By the definition of intersection, since $x \in X \cap Y$, $x \in X$ and $x \in Y$. Again, by the definition of intersection, since $x \notin X \cap Z$ and $x \in X$, $x \notin Z$. By the definition of set difference, since $x \in Y$ and $x \notin Z$, $x \in Y - Z$. Finally, by the definition of intersection, since $x \in X$ and $x \in Y - Z$, $x \in X \cap (Y - Z)$. We have proved equation (2.1.4).

Since we have proved both equations (2.1.3) and (2.1.4), it follows that

$$X \cap (Y - Z) = (X \cap Y) - (X \cap Z).$$

Disproving a Universally Quantified Statement
证明全称量词语句为假

To disprove $\forall x\ P(x)$ we simply need to find one member x in the domain of discourse that makes $P(x)$ false.

Such that a value for x is called a **counterexample (反例)**.

Disproving a Universally Quantified Statement
证明全称量词语句为假

To disprove $\forall x\ P(x)$ we simply need to find one member x in the domain of discourse that makes $P(x)$ false.

Such that a value for x is called a **counterexample (反例)**.

Example 1.5.6 Determine whether the universally quantified statement $\forall x\ (x^2 - 1 > 0)$ is true or false. The domain of discourse is **R**.

Disproving a Universally Quantified Statement 证明全称量词语句为假

To disprove $\forall x\ P(x)$ we simply need to find one member x in the domain of discourse that makes $P(x)$ false.

Such that a value for x is called a **counterexample (反例)**.

Example 1.5.6 Determine whether the universally quantified statement $\forall x\ (x^2 - 1 > 0)$ is true or false. The domain of discourse is **R**.

Value 1 is a counterexample to the statement $\forall x\ (x^2 - 1 > 0)$.

Disproving a Universally Quantified Statement 证明全称量词语句为假

To disprove $\forall x\ P(x)$ we simply need to find one member x in the domain of discourse that makes $P(x)$ false.

Such that a value for x is called a **counterexample (反例)**.

Example 2.1.4 Determine whether the universally quantified statement $\forall n \in \boldsymbol{Z}^{+}$ $(2^{n} + 1$ is prime) is true or false. If false, give a counterexample.

Disproving a Universally Quantified Statement
证明全称量词语句为假

To disprove $\forall x\ P(x)$ we simply need to find one member x in the domain of discourse that makes $P(x)$ false.

Such that a value for x is called a **counterexample (反例)**.

Example 2.1.4 Determine whether the universally quantified statement $\forall n \in \boldsymbol{Z}^{+}$ $(2^{n}$ + 1 is prime) is true or false. If false, give a counterexample.

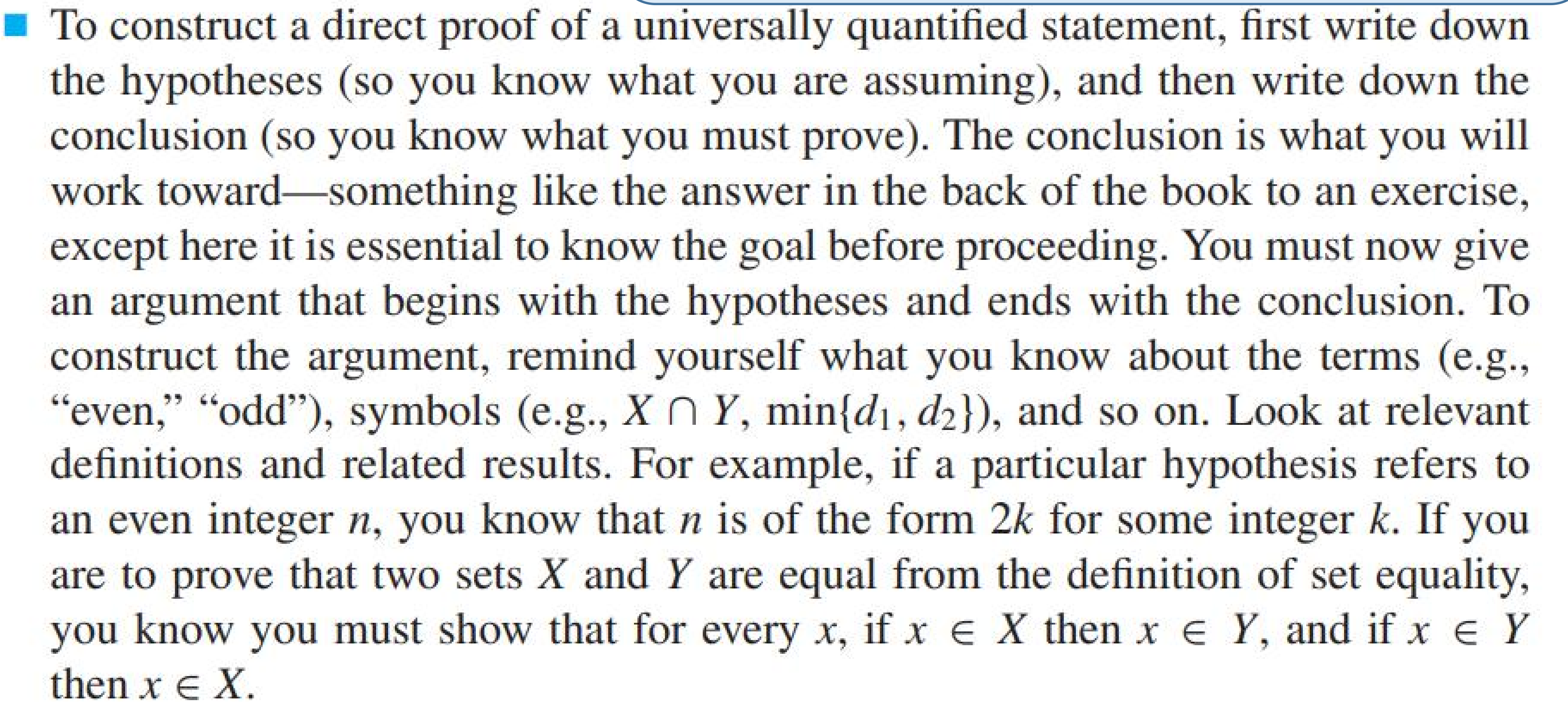
A counterexample is n = 3.

Disproving a Universally Quantified Statement 证明全称量词语句为假

Example 2.1.15 If statement $(A \cap B) \cup C = A \cap (B \cup C)$, for all sets $A, B, \text{and } C$ is true, prove it; otherwise, give a counterexample.

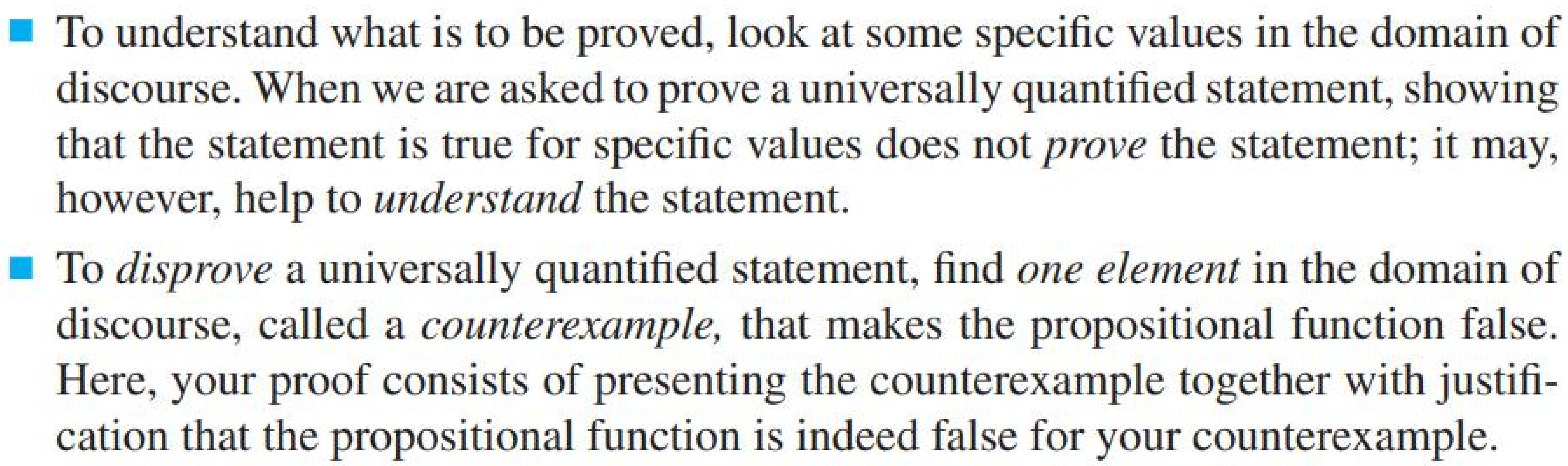
Problem-Solving Tips

Proof Let m and n be arbitrary integers, and suppose that m is odd and n is even. We prove that $m + n$ is odd. By definition, since m is odd, there exists an integer k_1 suchthat $m = 2k_1+1$. Also, by definition, since n is even, there exists an integer k_2 such that $n = 2k_2$. Now the sum is $m + n = (2k_1+1) + (2k_2) = 2(k_1 + k_2) + 1$.
Thus, there exists an integer k (namely $k = k_1 + k_2$) such that $m + n = 2k+1$. Therefore, $m + n$ is odd.



- To construct a direct proof of a universally quantified statement, first write down the hypotheses (so you know what you are assuming), and then write down the conclusion (so you know what you must prove). The conclusion is what you will work toward—something like the answer in the back of the book to an exercise, except here it is essential to know the goal before proceeding. You must now give an argument that begins with the hypotheses and ends with the conclusion. To construct the argument, remind yourself what you know about the terms (e.g., “even,” “odd”), symbols (e.g., $X \cap Y$, $\min\{d_1, d_2\}$), and so on. Look at relevant definitions and related results. For example, if a particular hypothesis refers to an even integer n, you know that n is of the form $2k$ for some integer k. If you are to prove that two sets X and Y are equal from the definition of set equality, you know you must show that for every x, if $x \in X$ then $x \in Y$, and if $x \in Y$ then $x \in X$.

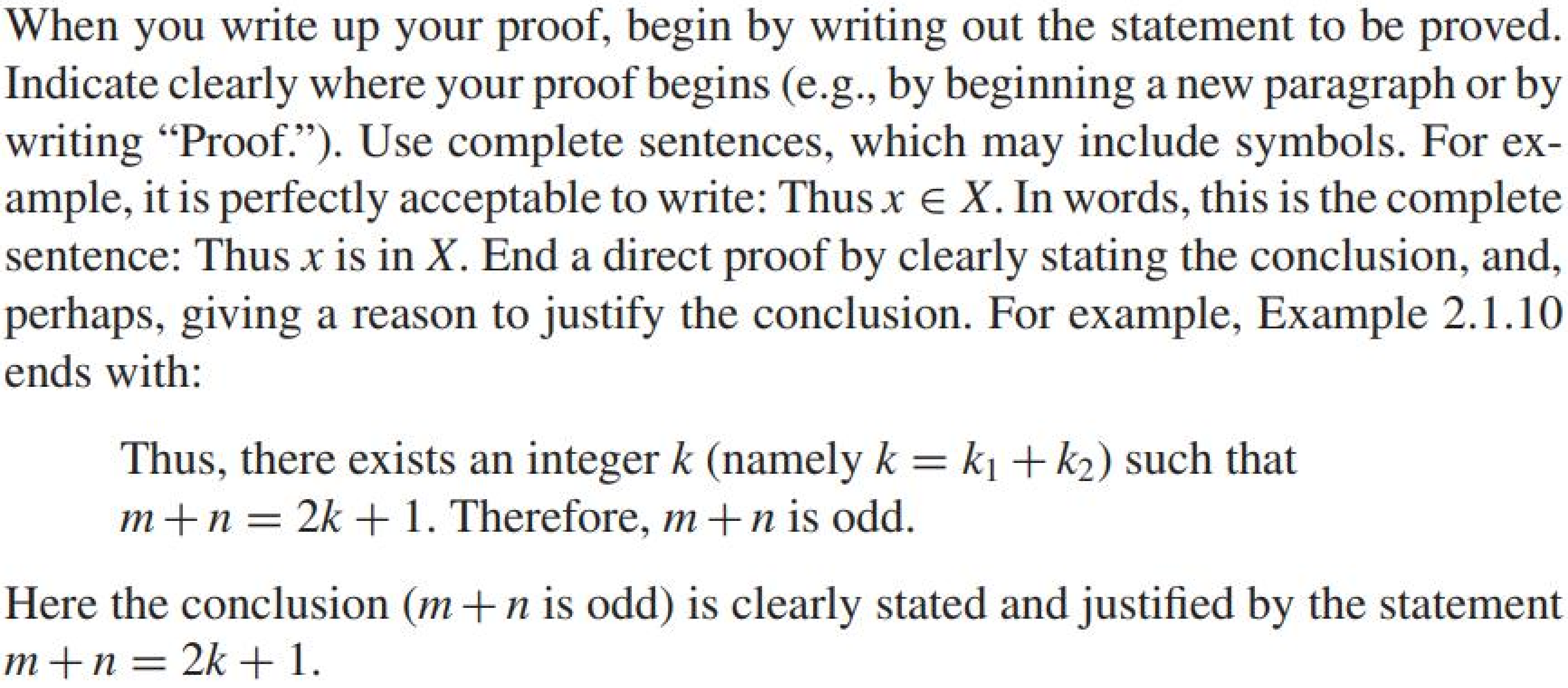
Problem-Solving Tips



- To understand what is to be proved, look at some specific values in the domain of discourse. When we are asked to prove a universally quantified statement, showing that the statement is true for specific values does not *prove* the statement; it may, however, help to *understand* the statement.
- To *disprove* a universally quantified statement, find *one element* in the domain of discourse, called a *counterexample*, that makes the propositional function false. Here, your proof consists of presenting the counterexample together with justification that the propositional function is indeed false for your counterexample.

Problem-Solving Tips

Proof Let m and n be arbitrary integers, and suppose that m is odd and n is even. We prove that $m + n$ is odd. By definition, since m is odd, there exists an integer k_1 suchthat $m = 2k_1+1$. Also, by definition, since n is even, there exists an integer k_2 such that $n = 2k_2$. Now the sum is $m + n = (2k_1+1) + (2k_2) = 2(k_1 + k_2) + 1$.
Thus, there exists an integer k (namely $k = k_1 + k_2$) such that $m + n = 2k+1$. Therefore, $m + n$ is odd.

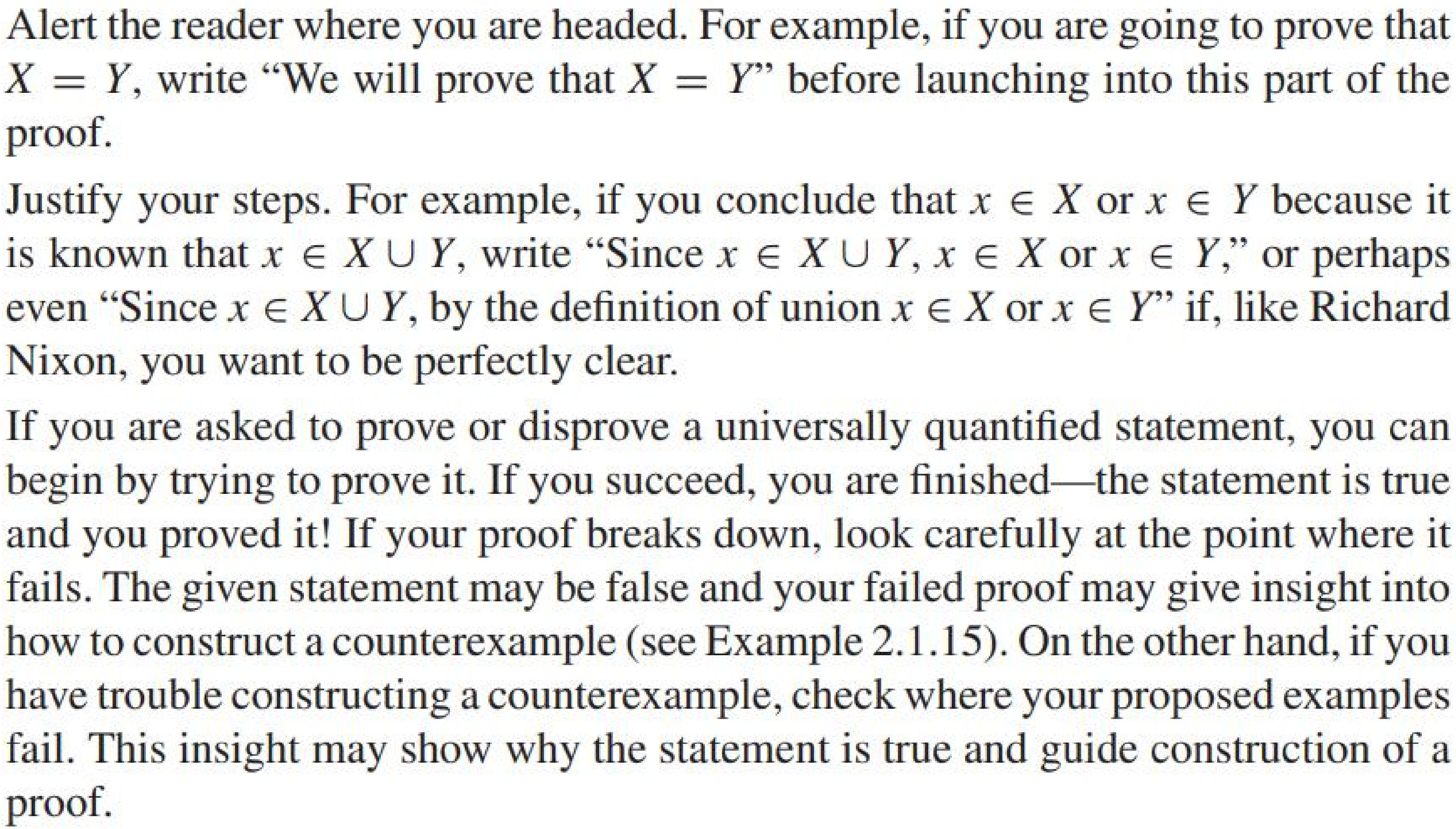


- When you write up your proof, begin by writing out the statement to be proved. Indicate clearly where your proof begins (e.g., by beginning a new paragraph or by writing “Proof.”). Use complete sentences, which may include symbols. For example, it is perfectly acceptable to write: Thus $x \in X$. In words, this is the complete sentence: Thus x is in X. End a direct proof by clearly stating the conclusion, and, perhaps, giving a reason to justify the conclusion. For example, Example 2.1.10 ends with:

  > Thus, there exists an integer k (namely $k = k_1 + k_2$) such that $m + n = 2k + 1$. Therefore, $m + n$ is odd.

  Here the conclusion ($m + n$ is odd) is clearly stated and justified by the statement $m + n = 2k + 1$.

Problem-Solving Tips



- Alert the reader where you are headed. For example, if you are going to prove that $X = Y$, write "We will prove that $X = Y$" before launching into this part of the proof.
- Justify your steps. For example, if you conclude that $x \in X$ or $x \in Y$ because it is known that $x \in X \cup Y$, write "Since $x \in X \cup Y$, $x \in X$ or $x \in Y$," or perhaps even "Since $x \in X \cup Y$, by the definition of union $x \in X$ or $x \in Y$" if, like Richard Nixon, you want to be perfectly clear.
- If you are asked to prove or disprove a universally quantified statement, you can begin by trying to prove it. If you succeed, you are finished—the statement is true and you proved it! If your proof breaks down, look carefully at the point where it fails. The given statement may be false and your failed proof may give insight into how to construct a counterexample (see Example 2.1.15). On the other hand, if you have trouble constructing a counterexample, check where your proposed examples fail. This insight may show why the statement is true and guide construction of a proof.

Exercise 1 Prove that if $X \subseteq Y$, then $X \cap Z \subseteq Y \cap Z$ for all sets X, Y and Z.

A is a subset of B (i.e., $A \subseteq B$) if for every x if $x \in A$, then $x \in B$.

Exercise 2 Prove that if $X \cap Y = X \cap Z$ and $X \cup Y = X \cup Z$, then $Y = Z$ for all sets X, Y and Z.