CSE215
Foundations of Computer Science

Instructor: Zhoulai Fu

State University of New York, Korea

We have studied these proof strategies

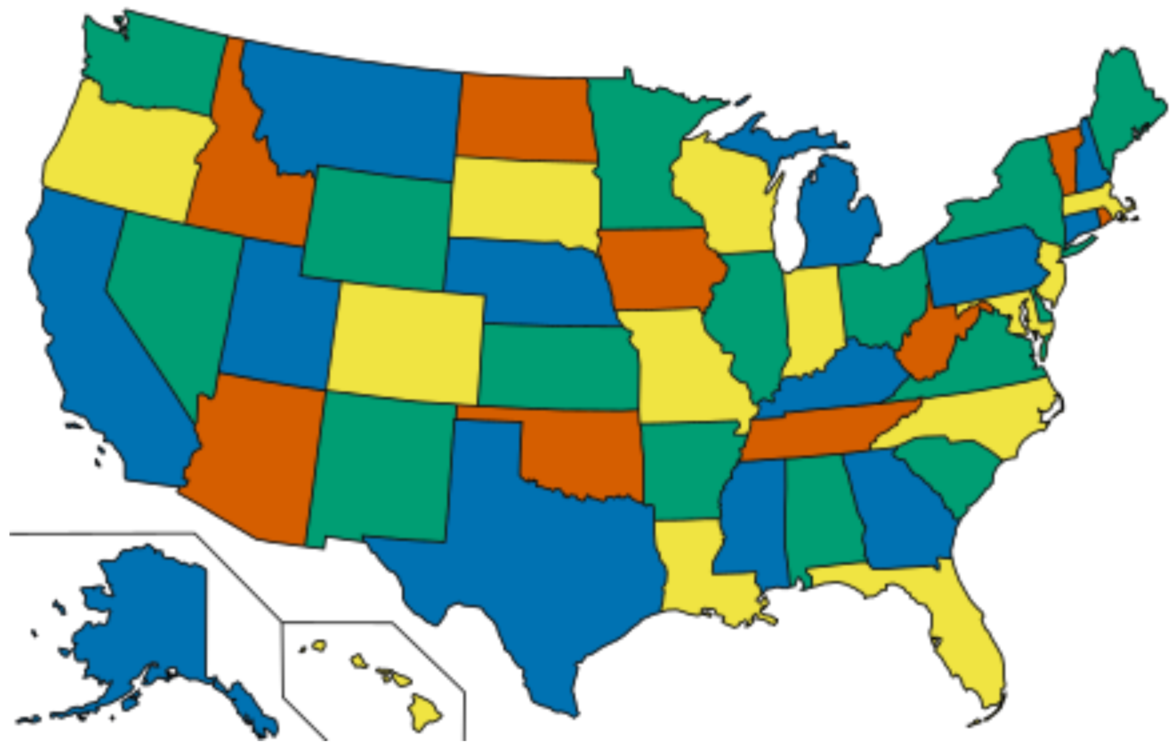
- Direct proof
- Proof by contradiction
- Proof by contraposition

Plan for today

- A new proof strategy: Proof by dividing into cases
- Disproof

Part 1:
Proof by dividing into cases

The four color theorem



- Theorem: No more than four colors are required to color the regions of any map so that no two adjacent regions have the same color.
- Proved by reducing maps into 1,834 configurations

Proof by dividing into cases

- You are asked to prove Q and you consider an **exhaustive** list cases. For each case, Q is true.
- Proof
    - We use proof by dividing into cases to proceed
    - We consider N cases.
    - Case 1: ____….. Therefore Q
    - Case 2: ____….. Therefore Q
    - …
    - Case N: ____….. Therefore Q
- QED.

Example 1: Prove the following statement

Proposition If $n \in \mathbb{N}$, then $1+(-1)^n(2n-1)$ is a multiple of 4.

Proposition If $n \in \mathbb{N}$, then $1+(-1)^n(2n-1)$ is a multiple of 4.

Proof. Suppose $n \in \mathbb{N}$.
Then n is either even or odd. Let's consider these two cases separately.

Case 1. Suppose n is even. Then $n = 2k$ for some $k \in \mathbb{Z}$, and $(-1)^n = 1$.
Thus $1+(-1)^n(2n-1) = 1+(1)(2\cdot 2k-1) = 4k$, which is a multiple of 4.

Case 2. Suppose n is odd. Then $n = 2k+1$ for some $k \in \mathbb{Z}$, and $(-1)^n = -1$.
Thus $1+(-1)^n(2n-1) = 1-(2(2k+1)-1) = -4k$, which is a multiple of 4.

These cases show that $1+(-1)^n(2n-1)$ is always a multiple of 4. ■

Example 2: Prove the following statement

Every multiple of 4 equals $1+(-1)^n(2n-1)$ for some $n \in \mathbb{N}$.

Proposition Every multiple of 4 equals $1+(-1)^n(2n-1)$ for some $n \in \mathbb{N}$.

Proof. In conditional form, the proposition is as follows:
If k is a multiple of 4, then there is an $n \in \mathbb{N}$ for which $1+(-1)^n(2n-1) = k$.
What follows is a proof of this conditional statement.
Suppose k is a multiple of 4.
This means $k = 4a$ for some integer a.
We must produce an $n \in \mathbb{N}$ for which $1+(-1)^n(2n-1) = k$.
This is done by cases, depending on whether a is zero, positive or negative.
Case 1. Suppose $a = 0$. Let $n = 1$. Then $1+(-1)^n(2n-1) = 1+(-1)^1(2-1) = 0$ $= 4 \cdot 0 = 4a = k$.
Case 2. Suppose $a > 0$. Let $n = 2a$, which is in $\mathbb{N}$ because a is positive. Also n is even, so $(-1)^n = 1$. Thus $1+(-1)^n(2n-1) = 1+(2n-1) = 2n = 2(2a) = 4a = k$.
Case 3. Suppose $a < 0$. Let $n = 1-2a$, which is an element of $\mathbb{N}$ because a is negative, making $1-2a$ positive. Also n is odd, so $(-1)^n = -1$. Thus $1+(-1)^n(2n-1) = 1-(2n-1) = 1-(2(1-2a)-1) = 4a = k$.

The above cases show that no matter whether a multiple $k = 4a$ of 4 is zero, positive or negative, $k = 1+(-1)^n(2n-1)$ for some $n \in \mathbb{N}$. ■

Example 3: Prove the following statement

if n is an integer, then $2n^2 + n + 1$ is not divisible by 3.

When n is divided by 3, the possible remainders are 0, 1, or 2. I consider these three cases.

Case 1. When n is divided by 3, the remainder is 0.

Then $n = 3q + 0 = 3q$ for some integer q. So

$$\begin{aligned} 2n^2 + n + 1 &= 2(3q)^2 + (3q) + 1 \\ &= 18q^2 + 3q + 1 \\ &= 3(6q^2 + q) + 1 \end{aligned}$$

The last expression shows that in this case when $2n^2 + n + 1$ is divided by 3, the remainder is 1. Hence, $2n^2 + n + 1$ is not divisible by 3.

Case 2. When n is divided by 3, the remainder is 1.

Then $n = 3q + 1$ for some integer q. So

$$\begin{aligned} 2n^2 + n + 1 &= 2(3q + 1)^2 + (3q + 1) + 1 \\ &= 18q^2 + 15q + 4 \\ &= 3(6q^2 + 5q + 1) + 1 \end{aligned}$$

The last expression shows that in this case when $2n^2 + n + 1$ is divided by 3, the remainder is 1. Hence, $2n^2 + n + 1$ is not divisible by 3.

Case 3. When n is divided by 3, the remainder is 2.

Then $n = 3q + 2$ for some integer q. So

$$\begin{aligned} 2n^2 + n + 1 &= 2(3q + 2)^2 + (3q + 2) + 1 \\ &= 18q^2 + 27q + 11 \\ &= 3(6q^2 + 9q + 3) + 2 \end{aligned}$$

The last expression shows that in this case when $2n^2 + n + 1$ is divided by 3, the remainder is 2. Hence, $2n^2 + n + 1$ is not divisible by 3.

Since in every case $2n^2 + n + 1$ is not divisible by 3, it follows that $2n^2 + n + 1$ is not divisible by 3 for any integer n. $\square$

Example 4: Prove the following statement

Suppose a is an integer. If $7|4a$, then $7|a$.

- Proof: (Proof by dividing into cases)
  - Suppose 7 | 4a
    - 4a = 7k for some integer k.
    - a = 7/4 k (*)
    - k mod 4 can be 0, 1, 2, or 3
    - Case 1: k = 4k’ for some integer k’. In this case, a = 7k’
    - Case 2: k = 4k’ + 1 for some integer k’. In this case, LHS in (*) = a, RHS in (*) 7k’ + 1/4 which is not an integer. So this case is not possible.
    - Case 3: k = 4k’ + 2 for some integer k’. In this case, LHS in (*) = a, RHS in (*) 7k’ + 1/2 which is not an integer. So this case is not possible.
    - Case 2: k = 4k’ + 3 for some integer k’. In this case, LHS in (*) = a, RHS in (*) 7k’ + 3/4 which is not an integer. So this case is not possible.
  - Therefore 7 | a
- QED.

- Proof: (direct proof)
  - Suppose $7 \mid 4a$
    - $4a = 7k$ for some integer k.
    - k must be even. So $k = 2k'$ for some integer k'
    - $4a = 14k'$. So $2a = 7k'$.
    - k' must be even So $k' = 2k''$ for some integer k''
    - $2a = 14k''$. So $a = 7k''$
  - Therefore $7 \mid a$
- QED.

Exercises

Prove the following statement

If $n \in \mathbb{Z}$, then $n^2 + 3n + 4$ is even.

Prove the following statement

Prove that if n is an integer, then $3n^2 + n + 14$ is even.

Prove the following statement

Prove that for all integers n, $n - 2$ is not divisible by 4. (hint: consider the odd and even cases separately)