Discrete Mathematics
MH1812

Topic 4.1 - Proof Techniques
Dr. Wang Huaxiong

Topic Overview

What's in store…

- **D**irect Proof
- **P**roof by Induction
- **P**roof by Contradiction

Types of Proof Techniques

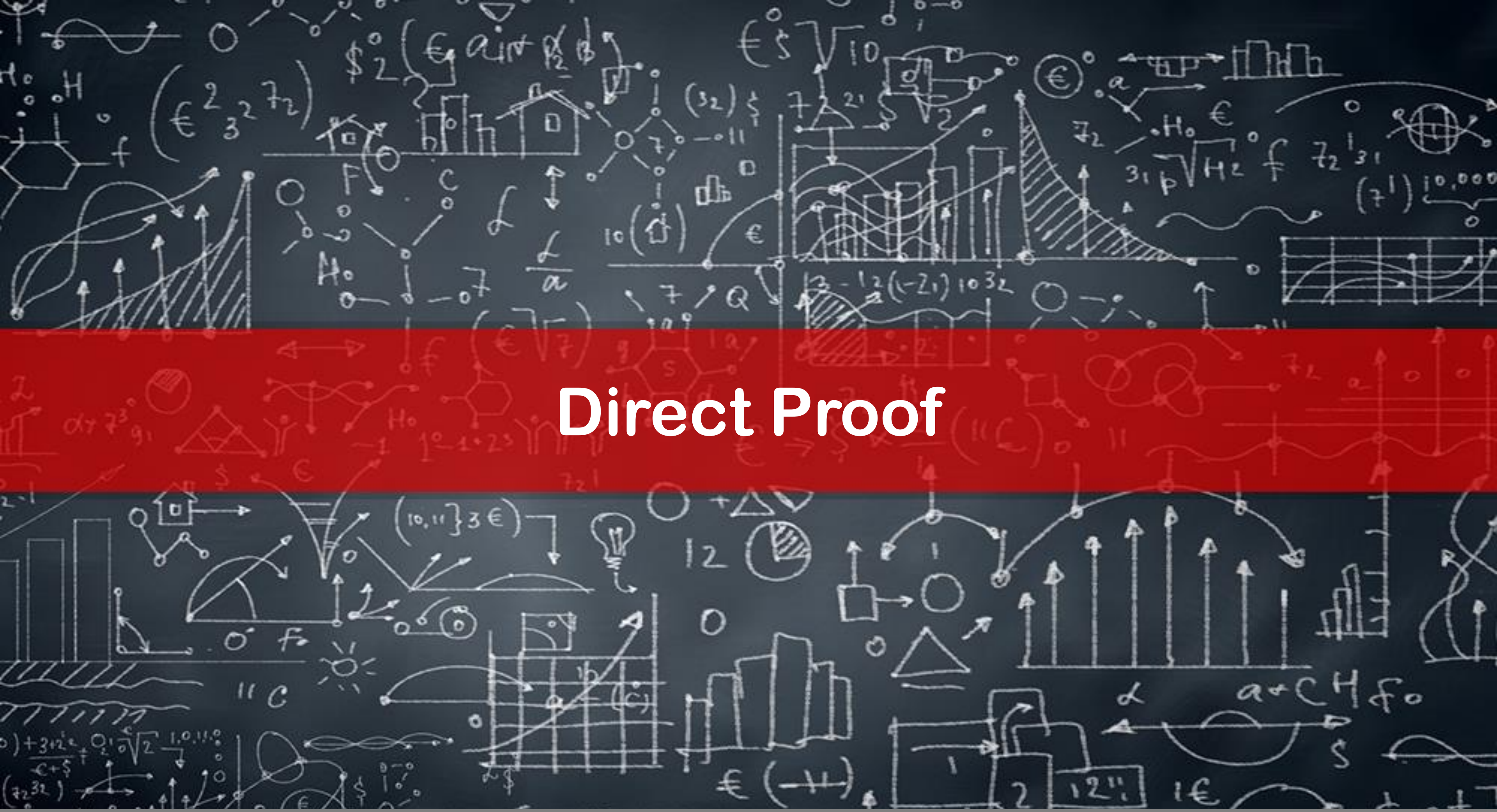
A **valid proof** is a valid argument, i.e., the conclusion **follows** from the given assumptions.

Three Techniques

- Direct Proof
- Proof by Induction
- Proof by Contradiction

By the end of this lesson, you should be able to…

- Use the direct proof technique.
- Use the proof by induction technique.
- Use the proof by contradiction technique.



Direct Proof

Direct Proof: The Mathematician

Carl F. Gauss
(1777 - 1855)

Carl F. Gauss by Christian Albrecht Jensen under WikiCommons (PD-US)

Direct Proof: Example

Prove that $\forall n \in N, \sum_{i=0}^{n} i = \frac{n(n+1)}{2}$

Define: $S = \sum_{i=0}^{n} i = \underbrace{0+1+2+\ldots+n-1+n}_{n+1 \text{ Terms}}$

Note: $S = \sum_{i=0}^{n} i = n+n-1+\ldots+2+1+0$

Sum up: $2S = \overbrace{n+n+\ldots+n+n+n}^{n+1 \text{ Terms}}$

$2S = (n+1)\,n$

Thus: $S = \frac{n(n+1)}{2}$

Proof by Induction

Proof by Induction: Mathematical Induction

Prove propositions of the form: $\forall n P(n)$

The proof consists of two steps.

Basis Step 1

The proposition $P(1)$ is shown to be true.

Inductive Step 2

Assume $P(k)$ is true (when $n = k$), then prove $P(k + 1)$ is true (when $n = k + 1$).

When both steps are complete, we have proved that "$\forall n P(n)$" is true.

Proof by Induction: Why Does it Work?

From Step 2	$P(1) \rightarrow P(2)$ by Universal Instantiation
From Step 1	$P(1)$
Applying Modus Ponen	$P(2)$

Repeat the process to get $P(3)$, $P(4)$, $P(5)$, etc.

So, all $P(k)$ are true, i.e., $\forall n P(n)$.

Inductive step

$$[P(1) \wedge \forall k(P(k) \rightarrow P(k+1))] \rightarrow \forall n P(n)$$

Basis Step Hypothesis Valid Argument

Proof by Induction: Mathematical Induction (Example)

Prove that $\forall n \in N, \sum_{i=0}^{n} i = \frac{n(n+1)}{2}$

Let $P(n)$ **denote:** $\left[\sum_{i=0}^{n} i = \frac{n(n+1)}{2} \right]$

Basis Step 1

$P(1)$ **is true.**

$$1 = \frac{1(1+1)}{2}$$

Proof by Induction: Mathematical Induction (Example)

(Inductive Step) Assume $P(k)$ true, $k > 0$:

$$\sum_{i=0}^{k} i = \frac{k(k+1)}{2}$$

Prove $P(k+1)$ true:

$$\sum_{i=0}^{k+1} i = \sum_{i=0}^{k} i + (k+1) = \frac{k(k+1)}{2} + (k+1)$$

$$= \frac{(k+1)(k+2)}{2} = \frac{(k+1)[(k+1)+1]}{2}$$

So, $P(n)$ is true for $n = k + 1$ and thus true for all n: $\forall n P(n)$ is true.

Proof by Induction: Complete Induction

Prove propositions of the form: $\forall n P(n)$

The proof consists of two steps.

Basis Step 1

The proposition $P(1)$ is shown to be true.

Inductive Step 2

Assume for $k > 1$, $P(m)$ is true for every $m < k$, then prove $P(k)$ is true.

When both steps are complete, we have proved that "$\forall n P(n)$" is true.

Proof by Induction: Completed Induction (Example)

Prove that every natural number $n > 1$ is either a prime, or a product of primes.

$P(n)$ = "($n = 1$) ∨ (n is prime) ∨ (n can be factored into primes)"

1 Basis Step

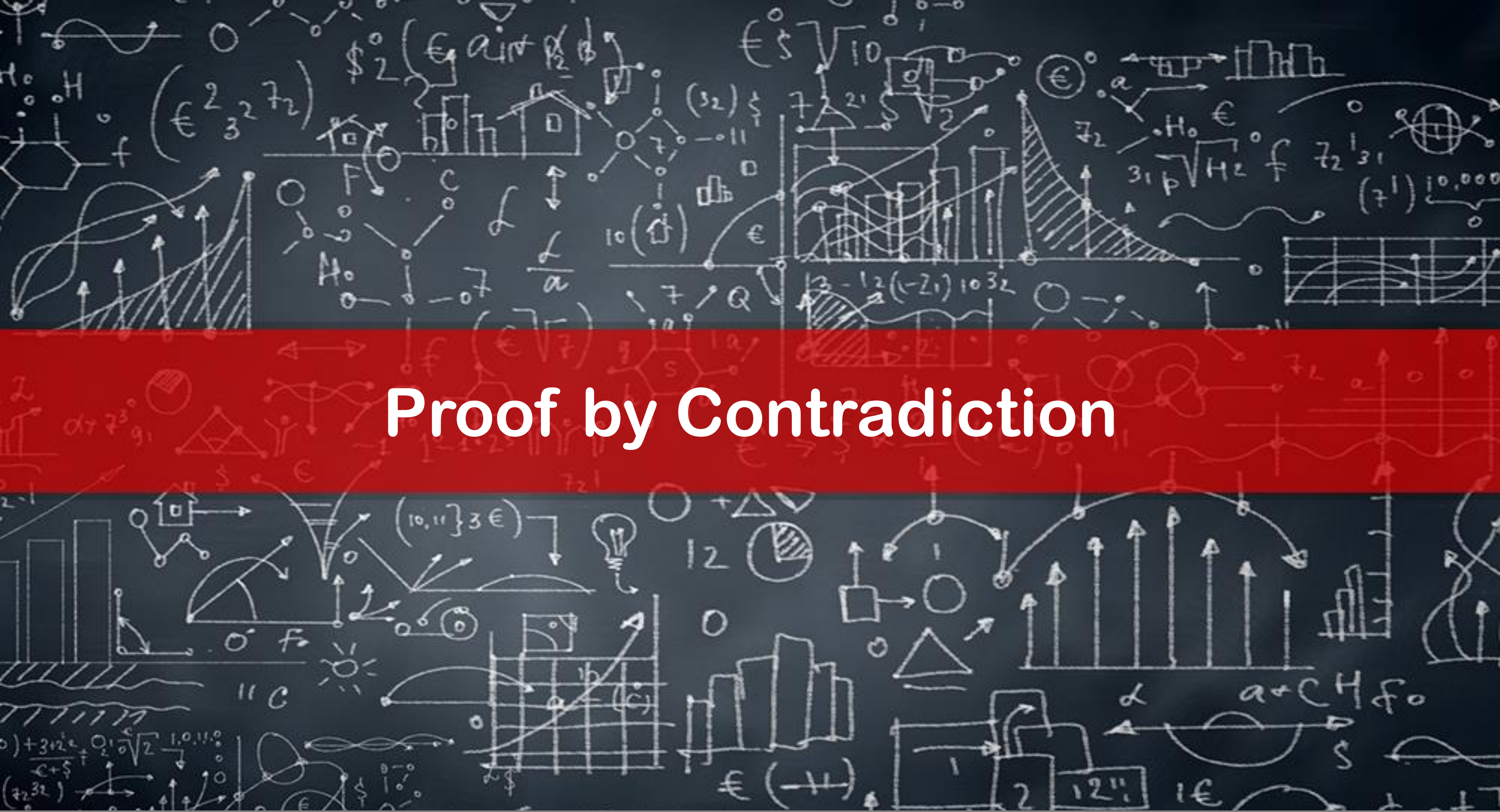
$P(1)$ is true because $n = 1$.

2 Inductive Step

Suppose $k > 1$, and $P(\mathrm{m})$ is true for all $m < k$. We must show that $P(k)$ is true.

Proof by Induction: Completed Induction (Example)

- **If k is prime, then $P(k)$ is true.**
- **Otherwise since $k > 1$, we can factor $k = pq$, with p,q natural numbers $< k$.**
- **The factor p is either prime or factors into prime, by induction hypothesis.**
- **And the same is true for q.**
- **Therefore k factors into primes.**



Proof by Contradiction

Proof by Contradiction

- We want to prove $\boxed{P(n) \to Q(n)}$
- Assume by contradiction that $\boxed{\neg(P(n) \to Q(n))}$
- This happens exactly if $P(n)$ and $\neg Q(n)$
- Suppose that $P(n)$ and $\neg Q(n)$
- Prove that this gives a contradiction, namely $\boxed{\neg(P(n) \to Q(n)) \to C \wedge \neg C}$
- This is equivalent to $\boxed{P(n) \to Q(n)}$ (Truth table!)

Proof by Contradiction: Example

- Prove that if n^2 is even, then n is even, for n integer.
- Let's assume n^2 is even but n is not even ($P(n)$ = "n^2 is even" and $Q(n)$ = "n is even").
- n is not even $\Leftrightarrow$ n is odd, i.e., $n = 2k + 1$, k integer.
- Then:

$$n^2 = (2k+1)^2$$

$$= 4k^2 + 4k + 1$$

$$= 2(2k^2 + 2k) + 1 \text{ (odd)}$$

This concludes the proof!

- This is a contradiction (C = "n^2 is even", $C \wedge \neg C$).

Proof by Contradiction: Proof by Contrapositive

- We want to prove $\boxed{P(n) \rightarrow Q(n)}$

- This is equivalent to proving that $\boxed{\neg Q(n) \rightarrow \neg P(n)}$

Proof by Contradiction: Proof by Contrapositive (Example)

- Prove that if n^2 is even, then n is even.
- $P(n)$ = "n^2 is even" and $Q(n)$ = "n is even".
- n is not even $\Leftrightarrow$ n is odd, i.e., $n = 2k + 1$, k integer.
- Then:

$$n^2 = (2k+1)^2$$

$$= 4k^2 + 4k + 1$$

$$= 2(2k^2 + 2k) + 1 \text{ (odd)}$$

This shows that $\neg P(n)$, and concludes the proof!

Topic Summary

Let's recap…

- Generic proof techniques:
  - Direct proof
  - Mathematical induction (complete induction)
  - Contradiction (contrapositive)