

# Discrete Mathematics for Computer Science

## Lecture 3: Nested Quantifier, Mathematical Proofs

Dr. Ming Tang

Department of Computer Science and Engineering  
Southern University of Science and Technology (SUSTech)  
Email: tangm3@sustech.edu.cn

# Questions from Students: Limitations of Proposition

- $p$ : Every computer in Room 101 is functioning properly.
- $q$ : Computer MATH3 is in Room 101.

Can we conclude  $r$ : “MATH3 is functioning properly” using the rules of propositional logic? NO! Cannot infer  $r$  from  $p$  and  $q$ .

## With predicate and quantifier:

- $C(x)$ : Computer  $x$  is in Room 101.
- $D(x)$ : Computer  $x$  is functioning properly.
- $\forall x(C(x) \rightarrow D(x))$  within the domain of computers: Every computer in Room 101 is functioning properly.
- $C(\text{MATH3})$ : Computer MATH3 is in Room 101.
- $D(\text{MATH3})$ : MATH3 is functioning properly.



# Questions from Students: Translation with Quantifiers

Every student in this class has studied algebra.

- $A(x)$ : “ $x$  has studied algebra”.
- $C(x)$ : “ $x$  is in this class”
- Domain: all students
- $\forall x(C(x) \rightarrow A(x))$

Note: Implication  $p \rightarrow q$ .

How about  $\forall x(C(x) \wedge A(x))$ ? All students are in this class and has studied algebra.

# Questions from Students: Translation with Quantifiers

Some student in this class has visited Mexico.

## Logic Expression 2:

- $M(x)$ : “ $x$  has visited Mexico”.
- $C(x)$ : “ $x$  is a student in this class.”
- Domain: all people
- $\exists x(C(x) \wedge M(x))$

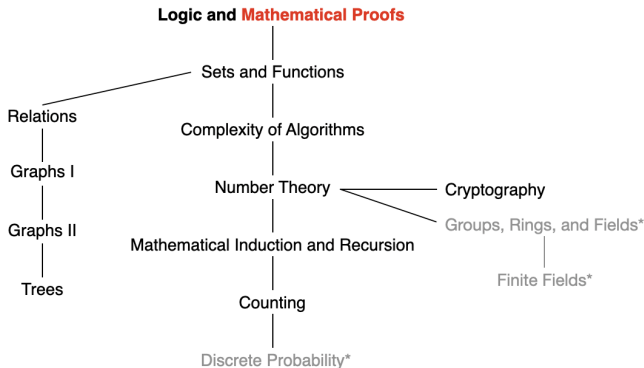
How about  $\exists x(C(x) \rightarrow A(x))$ ? **No!** This is even true when there is some people not in the class.

# Questions from Students: Inference and Implication

- Implication  $p \rightarrow q$ : An operator (analogy: +)
- Inference: “relation between multiple propositions” (analogy: =)

$$\begin{array}{c} p \rightarrow q \\ p \\ \hline \therefore q \end{array}$$

# This Lecture



Mathematical Proofs: **Rules of inference**, introduction to proofs

# Argument

**Argument:** A sequence of **propositions** that end with a conclusion.

## **Premises:**

“If you have a current password, then you can log onto the network.”

“You have a current password.”

## **Conclusion:**

“You can log onto the network.”

# Argument Form

## Premises:

“If you have a current password, then you can log onto the network.”

“You have a current password.”

**Conclusion:** “You can log onto the network.”

An **argument form** in propositional logic is a sequence of compound propositions involving **propositional variables**.

- $p$ : “You have a current password”
- $q$ : “You can log onto the network” or “You can change your grade”

$$\begin{array}{c} p \rightarrow q \\ p \\ \hline \therefore q \end{array}$$



# Validity

**Validity of Argument Form:** The **argument form** with premises  $p_1, p_2, \dots, p_n$  and conclusion  $q$  is **valid**, if

$(p_1 \wedge p_2 \wedge \dots \wedge p_n) \rightarrow q$  is a **tautology**.

**Validity of Argument:** The validity of an **argument follows from** the validity of the form of the argument.

# Validity

Is the following argument valid?

- If you do every problem in this book, then you will learn discrete mathematics.
- You learned discrete mathematics.
- Therefore, you did every problem in this book.

**No!**  $((p \rightarrow q) \wedge q) \rightarrow p$  is not a tautology.

How to show a compound proposition is NOT a tautology?

# Validity

Is the following argument valid?

- If you do every problem in this book, then you will learn discrete mathematics.
- You did not do every problem in this book.
- Therefore, you did not learn discrete mathematics.

**No!**  $((p \rightarrow q) \wedge \neg p) \rightarrow \neg q$  is not a tautology.

# Rules of Inference for Propositional Logic

To see the validity of  $(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \rightarrow q$ , we need to draw a table with  $2^{n+1}$  row. **A tedious approach!**

Construct **complicated** valid argument forms using the validity of some relatively **simple** argument forms, called **rules of inference**.

- **modus ponens** (*law of detachment*) 肯定前件式

$$\begin{array}{c} p \rightarrow q \\ p \\ \hline \therefore q \end{array} \quad \text{corresponding tautology:} \quad (p \wedge (p \rightarrow q)) \rightarrow q$$

# Rules of Inference for Propositional Logic

## ■ **modus tollens** 否定后件式

$$\frac{p \rightarrow q \quad \neg q}{\therefore \neg p}$$

corresponding tautology:  
 $(\neg q \wedge (p \rightarrow q)) \rightarrow \neg p$

## ■ **hypothetical syllogism** 假言三段论

$$\frac{p \rightarrow q \quad q \rightarrow r}{\therefore p \rightarrow r}$$

corresponding tautology:  
 $((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$

# Rules of Inference for Propositional Logic

## ■ **disjunctive syllogism** 选言三段论

$$\frac{p \vee q \quad \neg p}{\therefore q}$$

corresponding tautology:  
 $(\neg p \wedge (p \vee q)) \rightarrow q$

## ■ **Addition**

$$\frac{p}{\therefore p \vee q}$$

corresponding tautology:  
 $p \rightarrow (p \vee q)$

## ■ **Simplification**

$$\frac{p \wedge q}{\therefore p}$$

corresponding tautology:  
 $(p \wedge q) \rightarrow p$

# Rules of Inference for Propositional Logic

## ■ Conjunction

$$\frac{p}{q} \quad \frac{q}{\therefore p \wedge q}$$

corresponding tautology:

$$((p) \wedge (q)) \rightarrow (p \wedge q)$$

## ■ Resolution

$$\frac{\neg p \vee r}{p \vee q} \quad \frac{p \vee q}{\therefore q \vee r}$$

corresponding tautology:

$$((p \vee q) \wedge (\neg p \vee r)) \rightarrow (q \vee r)$$

## Example

Show that the premises (i)  $(p \wedge q) \vee r$  and (ii)  $r \rightarrow s$  imply the conclusion  $p \vee s$ .

- |    |                                |                               |
|----|--------------------------------|-------------------------------|
| 1. | $(p \vee r) \wedge (q \vee r)$ | Premise (i), Distributive Law |
| 2. | $p \vee r$                     | Simplification from step 1    |
| 3. | $\neg r \vee s$                | Premise (ii), Useful Law      |
| 4. | $p \vee s$                     | Resolution                    |



# Using Rules of Inference to Build Arguments

- “It is not sunny this afternoon and it is colder than yesterday.”

$$\neg p \wedge q$$

- “We will go swimming only if it is sunny this afternoon.”

$$r \rightarrow p$$

- “If we do not go swimming then we will take a canoe trip.”

$$\neg r \rightarrow s$$

- “If we take a canoe trip, then we will be home by sunset.”

$$s \rightarrow t$$

- Show the **conclusion** that “we will be home by sunset.”

$$t$$

- $p$ : It is sunny this afternoon.

- $s$ : We will take a canoe trip.

- $q$ : It is colder than yesterday.

- $t$ : We will be home by sunset.

- $r$ : We will go swimming.

# Using Rules of Inference to Build Arguments

- $p$ : It is sunny this afternoon.
- $q$ : It is colder than yesterday.
- $r$ : We will go swimming.
- $s$ : We will take a canoe trip.
- $t$ : We will be home by sunset.

**Premises:**  $\neg p \wedge q, r \rightarrow p, \neg r \rightarrow s, s \rightarrow t$

**Conclusion:**  $t$

Step	Reason
1. $\neg p \wedge q$	Premise
2. $\neg p$	Simplification using (1)
3. $r \rightarrow p$	Premise
4. $\neg r$	Modus tollens using (2) and (3)
5. $\neg r \rightarrow s$	Premise
6. $s$	Modus ponens using (4) and (5)
7. $s \rightarrow t$	Premise
8. $t$	Modus ponens using (6) and (7)

# Rules of Inference for Quantified Statements

- **Universal Instantiation (UI)**

$$\frac{\forall x P(x)}{\therefore P(c)}$$

- **Universal Generalization (UG)**

$$\frac{P(c) \text{ for an arbitrary } c}{\therefore \forall x P(x)}$$

- **Existential Instantiation (EI)**

$$\frac{\exists x P(x)}{\therefore P(c) \text{ for some element } c}$$

- **Existential Generalization (EG)**

$$\frac{P(c) \text{ for some element } c}{\therefore \exists x P(x)}$$

# Applying Rules of Inference for Quantified Statements

- “A student in this class has not read the book.”

$$\exists x(C(x) \wedge \neg B(x))$$

- “Everyone in this class passed the first exam.”

$$\forall x(C(x) \rightarrow P(x))$$

- Show the **conclusion** that “Someone who passed the first exam has not read the book.”

$$\exists x(P(x) \wedge \neg B(x))$$

- $C(x)$ :  $x$  is in this class.
- $B(x)$ :  $x$  has read the book.
- $P(x)$ :  $x$  passed the first exam.
- Domain of  $x$ : all students

# Applying Rules of Inference for Quantified Statements

- $C(x)$ :  $x$  is in this class.
- $B(x)$ :  $x$  has read the book.
- $P(x)$ :  $x$  passed the first exam.
- Domain of  $x$ : all students

**Premises:**  $\exists x(C(x) \wedge \neg B(x))$ ,  $\forall x(C(x) \rightarrow P(x))$

**Conclusion:**  $\exists x(P(x) \wedge \neg B(x))$

Step	Reason
1. $\exists x(C(x) \wedge \neg B(x))$	Premise
2. $C(a) \wedge \neg B(a)$	Existential instantiation from (1)
3. $C(a)$	Simplification from (2)
4. $\forall x(C(x) \rightarrow P(x))$	Premise
5. $C(a) \rightarrow P(a)$	Universal instantiation from (4)
6. $P(a)$	Modus ponens from (3) and (5)
7. $\neg B(a)$	Simplification from (2)
8. $P(a) \wedge \neg B(a)$	Conjunction from (6) and (7)
9. $\exists x(P(x) \wedge \neg B(x))$	Existential generalization from (8)

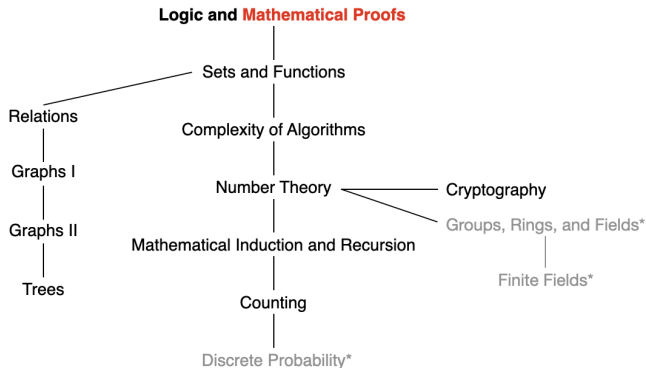
## Example: Game of Logic

- “Logic is difficult or not many students like logic.”
- “If mathematics is easy, then logic is not difficult.”

Which of the followings are valid conclusions?

- 1 That mathematics is not easy, if many students like logic.
- 2 That not many students like logic, if mathematics is not easy.
- 3 That mathematics is not easy or logic is difficult.
- 4 That logic is not difficult or mathematics is not easy.
- 5 That if not many students like logic, then either mathematics is not easy or logic is not difficult.

# This Lecture



Mathematical Proofs: Rules of inference, **introduction to proofs**

# Proofs

A proof is a **valid argument** that establishes the truth of a mathematical statement. (Note: the truth of all its premises implies that the conclusion is true.)

## Premises:

- hypotheses of the theorem
- axioms assumed to be true
- previously proven theorems or lemmas

## Conclusion:

- the truth of the statement

## Using rules of inference

- **Axiom**: a statement or proposition which is regarded as being established.
- **Theorem**: a statement that can be shown to be true.
- **Lemma**: a statement that can be proved to be true and is used in proving a theorem or proposition.



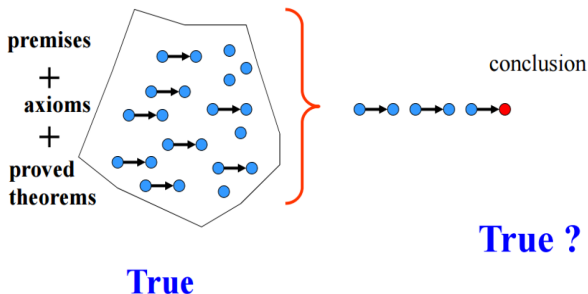
**SUSTech**

Southern University  
of Science and  
Technology



# Formal Proofs

**Formal proofs:** steps follow logically from the set of premises, axioms, lemmas, and other theorems.



# Formal Proof and Informal Proof

Step	Reason
1. $\exists x(C(x) \wedge \neg B(x))$	Premise
2. $C(a) \wedge \neg B(a)$	Existential instantiation from (1)
3. $C(a)$	Simplification from (2)
4. $\forall x(C(x) \rightarrow P(x))$	Premise
5. $C(a) \rightarrow P(a)$	Universal instantiation from (4)
6. $P(a)$	Modus ponens from (3) and (5)
7. $\neg B(a)$	Simplification from (2)
8. $P(a) \wedge \neg B(a)$	Conjunction from (6) and (7)
9. $\exists x(P(x) \wedge \neg B(x))$	Existential generalization from (8)

In practice, **informal proofs**: steps are not expressed in any formal language of logic; steps may be skipped; the axioms being assumed and the rules of inference used are not explicitly stated; ...

# Methods of Proving Theorems

Premises:  $p$ ; Conclusion:  $q$

- **Direct proof**

If  $p$  is true, then  $q$  follows

- **Proof by contrapositive**

Show the contrapositive: If  $\neg q$  is true, then  $\neg p$  follows

- **Proof by contradiction**

show that  $(p \wedge \neg q)$  contradicts the assumptions

- **Proof by cases**

give proofs for all possible cases

- **Proof of equivalence**

If  $p$  is true, then  $q$  follows; If  $q$  is true, then  $p$  follows

A proof is a valid argument. We work on **propositions** in proofs.



**SUSTech**

Southern University  
of Science and  
Technology

# Direct Proof

If  $p$  is true, then  $q$  follows.

**Example:** Prove that “if  $n$  is odd, then  $n^2$  is odd”

**Proof:**

Assume that (the hypothesis is true, i.e.,  $n$  is odd)

$n = 2k + 1$  where  $k$  is an integer.

Then

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1.$$

Therefore,  $n^2$  is odd.

# Proof by Contrapositive

If  $\neg q$  is true, then  $\neg p$  follows.

**Example:** Prove that “if  $3n + 2$  is odd, then  $n$  is odd”

**Proof:**

Assume that  $n$  is even, i.e.,  $n = 2k$ , where  $k$  is an integer. Then

$$3n + 2 = 3(2k) + 2 = 2(3k + 1).$$

Therefore,  $3n + 2$  is even.

# Proof by Contrapositive

Prove that if  $n = ab$ , where  $a$  and  $b$  are positive integers, then  $a \leq \sqrt{n}$  or  $b \leq \sqrt{n}$ .

## Proof:

- Assume that  $a > \sqrt{n}$  and  $b > \sqrt{n}$ .
- Then,  $ab > n$ , that is  $ab \neq n$ .

# Proof by Contradiction

Assume that  $p$  is true but  $q$  is false (i.e.,  $p \wedge \neg q$ ). Then show a contradiction to  $p$ , or  $\neg q$ , or other settled results.

**Example:** Prove that “if  $3n + 2$  is odd, then  $n$  is odd”

## Proof:

Assume that  $3n + 2$  is odd and  $n$  is even, i.e.,  $n = 2k$ , where  $k$  is an integer. Then

$$3n + 2 = 3(2k) + 2 = 2(3k + 1).$$

Thus,  $3n + 2$  is even. This is a contradiction to the assumption that  $3n + 2$  is odd. Therefore,  $n$  is odd.

# Proof by Contradiction

Assume that  $p$  is true but  $q$  is false (i.e.,  $p \wedge \neg q$ ). Then show a contradiction to  $p$ , or  $\neg q$ , or other settled results.

**Example:** Suppose we choose any 22 days. At least four of them fall on the same day of the week.

- Suppose we choose any 22 days; and at most three of them fall on the same day of the week.
- There are seven days of the week.
- Thus, at most 21 days could have been chosen. **Contradiction!**



# Proof by Contradiction

Prove that  $\sqrt{2}$  is **irrational**. (Rational numbers are those of the form  $\frac{m}{n}$ , where  $m$  and  $n$  are integers.)

**Proof:** Suppose that  $\sqrt{2}$  is rational. Then, there exist integers  $a$  and  $b$  with  $\sqrt{2} = a/b$ , where  $b \neq 0$  and  $a$  and  $b$  have no common factors (so that the fraction  $a/b$  is in lowest terms.)

Since  $\sqrt{2} = a/b$ , it follows that  $2b^2 = a^2$ . By the definition of an even integer, it follows that  $a^2$  is even, so  $a$  is even (see Exercise 16).

Since  $a$  is even,  $a = 2k$  for some integer  $k$ . Thus,  $b^2 = 2k^2$ . This implies that  $b^2$  is even, so  $b$  is even.

As a result,  $a$  and  $b$  have a common factor 2, which contradicts our assumption.

# Proof by Cases

We want to show

- Premises:  $p_1 \vee p_2 \vee \dots \vee p_n$ ; Conclusion:  $q$

This is equivalent to showing

- Premise 1:  $p_1$ ; conclusion:  $q$  and
- Premise 2:  $p_2$ ; conclusion:  $q$  and
- ... and
- Premise  $n$ :  $p_n$ ; conclusion:  $q$

Why?

$$\begin{aligned} & (p_1 \vee p_2 \vee \dots \vee p_n) \rightarrow q \\ \equiv & \neg(p_1 \vee p_2 \vee \dots \vee p_n) \vee q \\ \equiv & (\neg p_1 \wedge \neg p_2 \wedge \dots \wedge \neg p_n) \vee q \\ \equiv & (\neg p_1 \vee q) \wedge (\neg p_2 \vee q) \wedge \dots \wedge (\neg p_n \vee q) \\ \equiv & (p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \dots \wedge (p_n \rightarrow q) \end{aligned}$$

# Proof by Cases

We want to show  $(p_1 \vee p_2 \vee \dots \vee p_n) \rightarrow q$ . This is equivalent to  $(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \dots \wedge (p_n \rightarrow q)$ . Why?

**Example:** Prove that “ $|x||y| = |xy|$  for real numbers  $x, y$ ”

**Proof:** Four cases:

- ◇  $x \geq 0, y \geq 0$
- ◇  $x \geq 0, y < 0$
- ◇  $x < 0, y \geq 0$
- ◇  $x < 0, y < 0$

# Proof by Cases

Show that there exist irrational numbers  $x$  and  $y$  such that  $x^y$  is rational.

**Proof:** We know that  $\sqrt{2}$  is irrational. Consider the number  $\sqrt{2}^{\sqrt{2}}$ .

Case 1: If  $\sqrt{2}^{\sqrt{2}}$  is rational, then we have two irrational numbers  $x = \sqrt{2}$  and  $y = \sqrt{2}$  with  $x^y = \sqrt{2}^{\sqrt{2}}$  rational.

Case 2: If  $\sqrt{2}^{\sqrt{2}}$  is irrational, then we let  $x = \sqrt{2}^{\sqrt{2}}$  and  $y = \sqrt{2}$ . We have  $x^y = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = 2$  is rational.

Note that although we do not know which case works, we know that one of the two cases has the desired property.

# Proof of Equivalences

If  $p$  is true, then  $q$  follows; If  $q$  is true, then  $p$  follows

**Example:** Prove that “An integer  $n$  is odd if and only if  $n^2$  is odd”

**Proof:**

- ◇ proof of  $p \rightarrow q$ : direct proof
- ◇ proof of  $q \rightarrow p$ : proof by contrapositive

# Vacuous Proof

Premise:  $p$ ; Conclusion:  $q$

Show that  $p$  (the hypothesis) is always false.

## Example:

- $P(n)$ : if  $n > 1$ , then  $n^2 > n$ .
- Domain: integers

Show  $P(0)$  is true.

**Proof:** Since the premise  $0 > 1$  is always false. Thus  $P(0)$  is true.

Vacuous proofs are often used to establish **special cases** of theorems that state that a conditional statement is true for all positive integers.

# Trivial Proof

Premise:  $p$ ; Conclusion:  $q$

Show that  $q$  (the conclusion) is always true.

**Example:**  $P(n)$ : if  $a \geq b$ , then  $a^n \geq b^n$ . Show  $P(0)$  is true.

**Proof:** Since the conclusion  $a^0 \geq b^0$  is always true for any value of  $a$  and  $b$ . Thus  $P(0)$  is true.

# Proofs with Quantifiers

## Universal quantified statements

- **Prove** the property holds for all examples
  - ▶ proof by cases to divide the proof into different parts
- **Disprove** universal statements
  - ▶ existential quantified statements
  - ▶ counterexamples



# Proofs with Quantifiers

## Existential quantified statements

- Constructive
  - ▶ find a specific example to show the statement holds
- Nonconstructive
  - ▶ any method other than the constructive method
  - ▶ e.g., proof by contradiction
- Disprove: there does not exist any ...
  - ▶ universal quantified statements

# Proofs with Quantifiers

**Uniqueness** proofs: assert the existence of **a unique element** with a particular property.

- **Existence**: We show that an element  $x$  with the desired property exists.
- **Uniqueness**: We show that if  $y \neq x$ , then  $y$  does not have the desired property. Or, if  $y$  has the desired property, then  $y = x$ .

## Example

Show that if  $a$  and  $b$  are real numbers and  $a \neq 0$ , then there is a unique real number  $r$  such that  $ar + b = 0$ .

### Solution:

- Existence: The real number  $r = -b/a$  is a solution of  $ar + b = 0$ . Consequently, a real number  $r$  exists for which  $ar + b = 0$ .
- Uniqueness: Suppose that  $s$  is a real number such that  $as + b = 0$ . Then,  $ar + b = as + b$ , where  $r = -b/a$ . Dividing both sides of this last equation by  $a$ , which is nonzero, we see that  $r = s$ .

# Proof Exercise

Prove that there are infinitely many prime numbers.

**Proof:** Suppose that there are only a finite number of primes. Then, there exists a prime number  $p$  that is the largest of all the prime numbers. Also, we can list the prime numbers in ascending order:  $2, 3, 5, 7, 11, \dots, p$

Let  $n = (2 \times 3 \times 5 \times \dots \times p) + 1$ . Then,  $n > 1$ , and  $n$  cannot be divided by any prime number in the list above (to be proven in number theory section). This means that  $n$  is also a prime.

Clearly,  $n$  is larger than all the primes in the list above. This is contrary to the assumption that all primes are in the list.

# Proof Exercise

Prove that there are infinitely many solutions in positive integers  $x$ ,  $y$ , and  $z$  to the equation  $x^2 + y^2 = z^2$ .

## Proof:

- $x = m^2 - n^2$ ,  $y = 2mn$ , and  $z = m^2 + n^2$
- $m$  and  $n$  are integers

# Proof Exercise

Prove that if  $x$  is irrational and  $x \geq 0$ , then  $\sqrt{x}$  is irrational.

# Proof Exercise

- Write the numbers  $1, 2, 3, \dots, 2n$  on a blackboard, where  $n$  is an odd integer.
- Pick any two of the numbers,  $j$  and  $k$ , write  $|j - k|$  on the board and erase  $j$  and  $k$ . Continue this process until only one integer is written on the board.

Prove that this integer must be odd.

# Proof Exercise

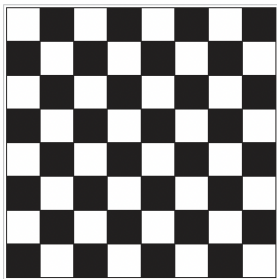


FIGURE 2 The Standard Checkerboard.

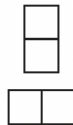


FIGURE 3  
Two Dominoes.

We say that a board is **tiled** by dominoes when all its squares are covered with no overlapping dominoes and no dominoes overhanging the board.

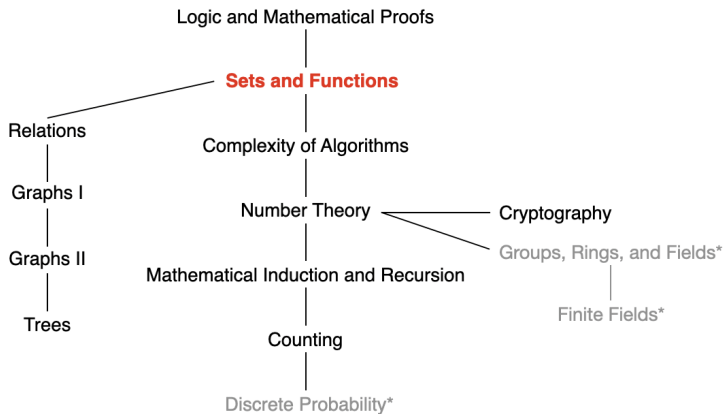
- Q1 Can we tile the standard checkerboard using dominoes?
- Q2 What if we remove the upper left corner square?
- Q3 What if we remove the upper left and lower right corner squares?



SUSTech  
Southern University  
of Science and  
Technology



# Next Lecture



**SUSTech**

Southern University  
of Science and  
Technology