國立交通大學電子工程學系

CHAPTER 1
THE FOUNDATIONS: LOGIC AND PROOFS

Iris Hui-Ru Jiang

Spring 2012

Outline

- **Content**
  - Propositional Logic
  - Propositional Equivalences
  - Predicates and Quantifiers
  - Nested Quantifiers
  - Rules of Inference
  - Introduction to Proofs
- **Reading**
  - Chapter 1

3 Propositional Logic

Propositional Logic

- **A proposition is a declarative sentence that is either true (T) or false (F), but not both.**
- **E.g.,**
  - Propositions
    - Hsinchu is a city in Taiwan.
    - 1+1=2
    - 2+2=3
  - Not propositions
    - What time is it?
    - x+1=2
    - y+2=3

  Can be turned into propositions if we assign values to the variables
- **The area of logic that deals with propositions is called the propositional calculus or propositional logic.**

Remark

- **Strictly speaking, sentences involving variable times/places are not propositions unless a fixed time/place is assumed.**
  - Today is Thursday.
  - At least 10 inches of rain fell today in this city.

- **We will always assume fixed times, fixed places, and particular people in such sentences unless otherwise noted.**

Compound Propositions

- **Compound propositions are formed by combining existing propositions with logical operators**
  - Logical operators are also called connectives

1. Negation
2. Conjunction
3. Disjunction
4. Exclusive or
5. Implication (conditional)
6. Biconditional

p	q	$p \wedge q$	$p \vee q$	$p \oplus q$	$p \rightarrow q$	$p \leftrightarrow q$
F	F	F	F	F	T	T
F	T	F	T	T	T	F
T	F	F	T	T	F	F
T	T	T	T	F	T	T

Logical Operator: Negation ($\neg$)

- **Let p be a proposition. The negation of p is the statement**

  "It is not the case that p."

  The negation of p is denoted by $\neg p$, read "not p." The truth value of $\neg p$ is the opposite of the truth value of p.
- **E.g.,**
  - p: "Today is Monday."
  - $\neg p$: "Today is not Monday."
- **A truth table displays the relationships between the truth values of propositions.**

TABLE 1 The Truth Table for the Negation of a Proposition.

p	$\neg p$
T	F
F	T

Logical Operator: Conjunction ($\wedge$)

- **Let p and q be propositions. The conjunction of p and q is the proposition that is**

  true only when both p and q are true, and false otherwise.

  The conjunction of p and q is denoted by $p \wedge q$, read "p and q."
- **E.g.,**
  - Today is Monday and this semester begins today.

TABLE 2 **The Truth Table for the Conjunction of Two Propositions.**

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

Logical Operator: Disjunction ($\vee$)

- **Let p and q be propositions. The disjunction of p and q is the proposition that is**

  false only when both p and q are false, and true otherwise.

  The disjunction of p and q is denoted by $p \vee q$, read "p or q."
- **E.g.,**
  - Students who have taken calculus or computer science can take this class.

TABLE 3 The Truth Table for the Disjunction of Two Propositions.

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

Inclusive OR (row T, T, T)

Logical Operator: Exclusive OR (⊕)

- **Let p and q be propositions. The exclusive or of p and q is the proposition that is**

  true only when one of p and q is true and false otherwise.

  The exclusive or of p and q is denoted by $p \oplus q$.
- **E.g.,**
  - Students who have taken calculus or computer science, but not both, can enroll in this class.

TABLE 4 **The Truth Table for the Exclusive Or of Two Propositions.**

p	q	$p \oplus q$
T	T	F
T	F	T
F	T	T
F	F	F

Exclusive OR

Ambiguity in English

- **Soup or salad comes before an entrée**
  - Do you think you can get both? ⇨ Exclusive OR
- **You can pay by cash or credit card**
  - Will you pay twice? ⇨ Exclusive OR
- **The prerequisites of algorithms: data structures or discrete mathematics**
  - Should you take one or two? ⇨ Inclusive OR

Logical Operator: Implication ($\rightarrow$)

- **Let p and q be propositions. The implication $p \rightarrow q$ is the proposition that is**

  false only when p is true and q is false, and true otherwise.

  $p \rightarrow q$ is read "if p then q." (a.k.a. conditional statement)
  - "If p then q." "q unless $\neg p$."

p: sufficient condition
q: necessary condition

- **E.g.,**
  - Q: "If 1+1=1, then I am God." True or false?
  - A:

TABLE 5 The Truth Table for the Conditional Statement $p \rightarrow q$.

p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

Converse / Contrapositive / Inverse (1/3)

- **For $p \rightarrow q$**
  - Converse: $q \rightarrow p$
  - Contrapositive: $\neg q \rightarrow \neg p$
  - Inverse: $\neg p \rightarrow \neg q$
- **E.g.,**
  - "The home team wins whenever it is raining."
  - i.e., If it is raining, then the home team wins.
  - Contrapositive: If the home team does not win, then it is not raining.
  - Converse: If the home team wins, then it is raining.
  - Inverse: If it is not raining, then the home team does not win.

  - Q: Which one is equivalent to the original statement?
  - A:

Converse / Contrapositive / Inverse (2/3)

- **For $p \rightarrow q$**
  - Converse: $q \rightarrow p$
  - Contrapositive: $\neg q \rightarrow \neg p$
  - Inverse: $\neg p \rightarrow \neg q$
- **Equivalent: two compound propositions always have the same truth value**
  - Converse $\equiv$ inverse
  - Contrapositive $\equiv$ itself
    - Proof by truth table:

p	q	$p \rightarrow q$	$\neg q$	$\neg p$	$\neg q \rightarrow \neg p$
T	T	T			
T	F	F			
F	T	T			
F	F	T			

Converse / Contrapositive / Inverse (3/3)

- **The following English statement can be written in the form**
  "if …, then…"
  Yet in some cases there is an implied "only if";
  that is, the converse is implied.
- **E.g.,**
  - Q: Do you think that the following statement has an implied converse?
    "If you have a dollar, then you can buy coffee from the vending machine."
  - A: (Hint: Converse ≡ inverse)
  - If you don't have a dollar, then you probably can't buy coffee from the vending machine (unless the machine accepts a larger bill you might have).
  - This proposition probably has an implied converse.

Logical Operator: Biconditional ($\leftrightarrow$)

- **Let p and q be propositions. The biconditional $p \leftrightarrow q$ is the proposition that is true when p and q have the same truth value, and false otherwise.**
  $p \leftrightarrow q$ is read "p if and only if q."
- **E.g.,** iff: if and only if
  - You can take the flight if and only if you buy a ticket.
  - 劍在 $\leftrightarrow$ 人在

$$p \leftrightarrow q \equiv (p \rightarrow q) \land (q \rightarrow p)$$

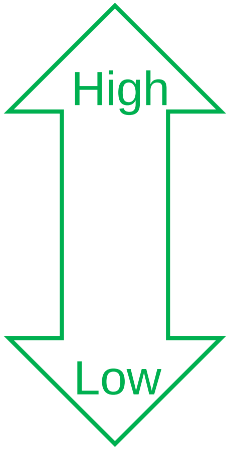
TABLE 6 The Truth Table for the Biconditional $p \leftrightarrow q$.

p	q	$p \leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

Precedence of Logical Operators

TABLE 8 Precedence of Logical Operators.

Operator	*Precedence*
$\neg$	1
$\wedge$	2
$\vee$	3
$\rightarrow$	4
$\leftrightarrow$	5



- **Use parenthesis whenever needed**

Truth Tables of Compound Propositions

- **E.g.,**
  - $(p \vee \neg q) \rightarrow (p \wedge q)$
- **Sol:**
  1. $\neg q$
  2. $(p \vee \neg q)$
  3. $(p \wedge q)$
  4. $(p \vee \neg q) \rightarrow (p \wedge q)$

TABLE 7 **The Truth Table of $(p \vee \neg q) \rightarrow (p \wedge q)$.**

p	q	$\neg q$	$p \vee \neg q$	$p \wedge q$	$(p \vee \neg q) \rightarrow (p \wedge q)$
T	T	F			
T	F	T			
F	T	F			
F	F	T			

System Specifications (1/3)

- **Translating sentences in natural language into logical expressions is an essential part of specifying both hardware and software systems (c.f. Unit 4 in Logic Design)**
- **E.g., express the following specification:**
  - "The diagnostic message is stored in the buffer or it is retransmitted."
  - "The diagnostic message is not stored in the buffer."
  - "If the diagnostic message is stored in the buffer, then it is retransmitted."

System Specifications (2/3)

- **E.g., express the following specification:**
  - "The diagnostic message is stored in the buffer **or** it is retransmitted."
  - "The diagnostic message is **not** stored in the buffer."
  - "**If** the diagnostic message is stored in the buffer, **then** it is retransmitted."
- **Sol:**
  - Let p denote "The diagnostic message is stored in the buffer", and q denote "The diagnostic message is retransmitted."
  - Then the above specification can be formulated as follows.
  - $p \vee q$
  - $\neg p$
  - $p \rightarrow q$

System Specifications (3/3)

- **System specification should be consistent, i.e., without conflicting requirements.**
- **E.g., in the above example,**
  - $p \vee q$
  - $\neg p$
  - $p \rightarrow q$
  - We can take *p* to be false and *q* to be true for consistency.
- **E.g., what if adding the following specification?**
  - "The diagnostic message is not retransmitted."
- **Sol:**

Logic Puzzles (1/2)

- **Logic puzzles: puzzles that can be solved using logical reasoning**
- **Knight and Knave puzzle**
  - Knights always tell the truth while knaves always lie.
  - A: “B is a knight”
  - B: “The two of us are opposite types”
  - What are A and B?

Logic Puzzles (2/2)

- **Sol:**
  - Let p denote "A is a knight" and q for "B is a knight."
  - We would like to find the truth values for p and q.

  - Suppose p is true. Then A tells the truth. So q is true.
  - But then B must also tell the truth.
  - Since p and q are both true, B cannot tell the truth. A contradiction.

  - On the other hand, Suppose p is false. Then A lies and q is false. Since q is false, B lies. Thus both p and q must have the same truth value. This is exactly the case.
  - We now conclude A and B are knaves.

Logic Game: Wolf Sheep & Cabbage

Logic and Bit Operations

- A **bit** (**bi**nary digi**t**) is a symbol with 2 possible values, 0 and 1.
- A **Boolean variable** is a variable whose value is either true or false.
- A Boolean variable can be represented by a bit.
  - True : 1 false : 0
- A **bit string** is a sequence of zero or more bits. The **length** of this string is the number of bits in the string.
- E.g.,

```
01 1011 0110
11 0001 1101
------------
11 1011 1111  bitwise OR
01 0001 0100  bitwise AND
10 1010 1011  bitwise XOR
```

Propositional Equivalences

- A **tautology** is a compound proposition that is **always true**.
- A **contradiction** is a compound proposition that is **always false**.
- A **contingency** is a compound proposition that is neither a tautology nor a contradiction.

TABLE 1 Examples of a Tautology and a Contradiction.

p	$\neg p$	$p \vee \neg p$	$p \wedge \neg p$
T	F	T	F
F	T	T	F

Contingencies (columns p, $\neg p$) — Tautology ($p \vee \neg p$) — Contradiction ($p \wedge \neg p$)

Logical Equivalence

- **The propositions p and q are called logically equivalent if**

  $p \leftrightarrow q$ is a tautology.

  We write $p \Leftrightarrow q$ or $p \equiv q$ when p and q are logically equivalent.
- **Remark:**
  - $p \equiv q$ is not a compound proposition.
  - $p \leftrightarrow q$ is a compound proposition.
- **E.g., the De Morgan Laws**

TABLE 2 De Morgan's Laws.
$\neg(p \wedge q) \equiv \neg p \vee \neg q$
$\neg(p \vee q) \equiv \neg p \wedge \neg q$

Two syntactically (i.e., textually) different compound propositions may be the semantically identical (i.e., have the same meaning). We call them equivalent.

Example: Logical Equivalence

TABLE 4 **Truth Tables for $\neg p \vee q$ and $p \rightarrow q$.**

p	q	$\neg p$	$\neg p \vee q$	$p \rightarrow q$
T	T	F	T	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

TABLE 3 **Truth Tables for $\neg(p \vee q)$ and $\neg p \wedge \neg q$.**

p	q	$p \vee q$	$\neg(p \vee q)$	$\neg p$	$\neg q$	$\neg p \wedge \neg q$
T	T	T	F	F	F	F
T	F	T	F	F	T	F
F	T	T	F	T	F	F
F	F	F	T	T	T	T

Summary on Logical Equivalence (1/2)

Equivalence	Name
$p \wedge T \equiv p$ $p \vee F \equiv p$	Identity laws
$p \vee T \equiv T$ $p \wedge F \equiv F$	Domination laws
$p \vee p \equiv p$ $p \wedge p \equiv p$	Idempotent laws
$\neg(\neg p) \equiv p$	Double negation law
$p \vee q \equiv q \vee p$ $p \wedge q \equiv q \wedge p$	commutative laws
$(p \vee q) \vee r \equiv p \vee (q \vee r)$ $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	Associative laws
$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	Distributive laws

Summary on Logical Equivalence (2/2)

$\neg(p \wedge q) \equiv \neg p \vee \neg q$ $\neg(p \vee q) \equiv \neg p \wedge \neg q$	De Morgan's laws
$p \vee (p \wedge q) \equiv p$ $p \wedge (p \vee q) \equiv p$	Absorption laws
$p \vee \neg p \equiv T$ $p \wedge \neg p \equiv F$	Negation laws
$p \rightarrow q \equiv \neg p \vee q$ $p \rightarrow q \equiv \neg q \rightarrow \neg p$ $(p \rightarrow q) \wedge (p \rightarrow r) \equiv p \rightarrow (q \wedge r)$ $(p \rightarrow r) \wedge (q \rightarrow r) \equiv (p \vee q) \rightarrow r$ $(p \rightarrow q) \vee (p \rightarrow r) \equiv p \rightarrow (q \vee r)$ $(p \rightarrow r) \vee (q \rightarrow r) \equiv (p \wedge q) \rightarrow r$	
$p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$ $p \leftrightarrow q \equiv (p \wedge q) \vee (\neg p \wedge \neg q)$ $\neg(p \leftrightarrow q) \equiv p \leftrightarrow \neg q$	

Example: Logical Equivalence

Iris H.-R. Jiang

- **Show that**
  - $\neg(a \lor (\neg a \land b)) \equiv \neg a \land \neg b$
- **Sol 1: Truth table**
- **Sol 2:**
  - $\neg(a \lor (\neg a \land b)) \equiv \neg a \land \neg(\neg a \land b)$ by De Morgan's law
    $\equiv \neg a \land [\neg(\neg a) \lor \neg b]$ by De Morgan's law
    $\equiv \neg a \land (a \lor \neg b)$ by double negation
    $\equiv (\neg a \land a) \lor (\neg a \land \neg b)$ by distributive law
    $\equiv \mathbf{F} \lor (\neg a \land \neg b)$ by negation law
    $\equiv (\neg a \land \neg b) \lor \mathbf{F}$ by commutative law
    $\equiv \neg a \land \neg b$ by identity law

Example: Logical Equivalence

- **Show that**
  - $a \to (b \vee c) \equiv (a \wedge \neg b) \to c$
- **Sol 1: Truth table**
- **Sol 2:**
  - Hint: $p \to q \equiv \neg p \vee q$
  - $a \to (b \vee c) \equiv \neg a \vee (b \vee c)$

    $\equiv (\neg a \vee b) \vee c$

    $\equiv \neg(a \wedge \neg b) \vee c$

    $\equiv (a \wedge \neg b) \to c$

Summary

- **Atomic propositions:** p, q, r, …
- **Boolean operators:** $\neg\ \wedge\ \vee\ \oplus\ \rightarrow\ \leftrightarrow$
- **Compound propositions:** $s :\equiv (p \wedge \neg q) \vee r$
- **Equivalences:** $p \wedge \neg q \equiv \neg(p \rightarrow q)$
- **Proving equivalences using:**
  - Truth tables.
  - Symbolic derivations. $p \equiv q \equiv r$ …

What's Wrong with Truth Tables?

- **A truth table of a compound proposition with *n* different propositions requires 2^n rows in truth table.**
- **Truth tables work well when the number of propositions (variables) keeps small**
  - 2~16
- **What if the number goes larger?**
  - E.g., 20; you might need a computer program
  - If the number is 1000, what can you do?

Propositional Satisfiability

- **Satisfiability (SAT)**
  - Find a truth assignment to the variables making the compound proposition true
  - A compound proposition is **satisfiable** if such an assignment can be found
  - A compound proposition is **unsatisfiable** if no such assignment exists, meaning that the proposition is always false
  - A compound proposition is unsatisfiable if its negation is a tautology

36

Predicates and Quantifiers

Predicates

Predicate: The part of the sentence that makes a statement about the subject. It always includes "the sentence verb".

- **Recap propositional logic:**
  - "$x > 3$" is not a proposition since x is a variable
- **In English**

"*x* is greater than 3."

subject (*x*) — predicate (is greater than 3)

- **Let $P(x)$ be a proposition with x as its parameter. Then P is called a predicate or propositional function.**

- **Q: Let $P(x)$ denote "$x > 3$." What are the truth values for $P(4)$?**
- **A: $P(4)$: true**

- **We can generalize to multiple parameters: A statement of the form $P(x_1, x_2, \ldots, x_n)$ is the value of the propositional function P at the n-tuple $(x_1, x_2, \ldots, x_n)$. P is also called a predicate.**

Quantifiers

- **In addition to assign values to parameters, we can also make predicates become propositions by quantification. The area of logic that deals with predicates and quantifiers is called the predicate calculus.**
  - Universal quantification
  - Existential quantification

Universal Quantifier (∀) FOR∀LL

- **The universal quantification of $P(x)$ is the proposition**
  "$P(x)$ is true for all values of x in the domain."
  The universal quantification of $P(x)$ is denoted by $\forall x P(x)$, read "for all x $P(x)$."
  - $\forall x P(x) \equiv P(x_1) \wedge P(x_2) \wedge \ldots \wedge P(x_n)$, where the domain of x includes $x_1, x_2, \ldots, x_n$.
- **Specifying the domain is mandatory when quantifiers are used.**
  - The truth value of a quantified statement depends on which elements are in this domain (universe).
- **E.g.,**
  - What is the truth value of $\forall x\ (x^2 \geq x)$ when x ranges over integers and real numbers respectively?
- **Sol:**
  - If x ranges over integers, $x^2 \geq x$. Hence $\forall x\ (x^2 \geq x)$ is true.
  - On the other hand, $x^2 < x$ when $0 < x < 1$. Therefore $\forall x\ (x^2 \geq x)$ is false when x ranges over real numbers.

Counterexamples

- **To disprove $\forall x P(x)$**
  - You need only find just one value of x within the domain such that $P(x)$ is false
- **Such a value of x is called a counterexample**
- **E.g.,**
  - “交大無帥哥”

Existential Quantifier (∃) ∃XIST

- **The existential quantification of $P(x)$ is the proposition "There exists an element x in the domain such that $P(x)$ is true." The existential quantification of $P(x)$ is denoted by $\exists x P(x)$, read "for some x $P(x)$."**
  - $\exists x P(x) \equiv P(x_1) \vee P(x_2) \vee \ldots \vee P(x_n)$, where the domain of x includes $x_1, x_2, \ldots, x_n$.
- **E.g.,**
  - Let $Q(x)$ be "$x \neq x$." What is the truth value of $\exists x Q(x)$?
- **Sol:**
  - False, apparently.

Universal vs. Existential

- **Meaning**

Statement	When true?	When false?
$\forall x P(x)$	$P(x)$ is true for **every** x	There is **an** x for which $P(x)$ is false
$\exists x P(x)$	There is **an** x for which $P(x)$ is true	$P(x)$ is false for **every** x

- **Precedence**
  - The quantifiers $\forall$ and $\exists$ have higher precedence than all logical operators from propositional calculus.
  - Q: $\exists x P(x) \vee Q(x) \equiv ?$
    1. $(\exists x P(x)) \vee Q(x)$
    2. $\exists x (P(x) \vee Q(x))$
  - A:

Binding Variables

- **When a quantifier is used on the variable *x* or when we assign a value of it, we say that this occurrence of *x* is bound.**
- **An occurrence of a variable that is not bound is said to be free.**
- **The part of a logical expression where a quantifier is applied is called the scope of the quantifier.**
- **A predicate without free variables is a proposition**
- **E.g., $\exists x(x + y = 1)$**
  - x is bound; y is free.
- **E.g., $\exists x(P(x) \wedge Q(x)) \vee \forall x R(x)$ vs. $\exists x(P(x) \wedge Q(x)) \vee \forall y R(y)$**
  - Remark: in common usage, the same letter is often used to represent variables bound by different quantifiers with scopes that do not overlap

Negating Quantified Expressions

- **De Morgan's laws for quantifiers**
  - $\neg\forall x P(x) \equiv \exists x \neg P(x)$
  - $\neg\exists x P(x) \equiv \forall x \neg P(x)$

Negation	Equivalent statement	When is negation true?	When false?
$\neg\forall x P(x)$	$\exists x \neg P(x)$	There is **an** x for which $P(x)$ is false	$P(x)$ is true for **every** x
$\neg\exists x P(x)$	$\forall x \neg P(x)$	For **every** x, $P(x)$ is false	There is **an** x for which $P(x)$ is true

  - $\forall x P(x)$ means "for all values of x, $P(x)$ is true"
  - Negation: "it is not the case that all values of x, $P(x)$ is true."
  - i.e., there is a value for x s.t. $P(x)$ is false. Hence, $\exists x \neg P(x)$
- E.g., "All students in EE103 have taken DM"

  quantifier (All) domain (students in EE103) predicate (have taken DM)
- Negation: "There is a student in EE103 who has not taken DM"

Example: Negating Quantified Expressions

- **E.g., what is the negation of $\forall x(x^2 > x)$?**
- **Sol:**
  - $\neg\forall x(x^2 > x) \equiv$
- **E.g., what is the negation of $\exists x(x^2 = 2)$?**
- **Sol:**
  - $\neg\exists x(x^2 = 2) \equiv$

Example: Quantified Expressions

- **E.g., consider the following two statements:**
  1. "All lions are fierce."
  2. "Some lions do not drink coffee."

  Can you deduce "some fierce creatures do not drink coffee?"
- **Sol:**
  - Let $P(x)$ be the statement "x is a lion."
    $Q(x)$ "x is fierce."
    $R(x)$ "x drinks coffee."
  - Then we have
    1. $\forall x(P(x) \rightarrow Q(x))$ (We cannot express as $\forall x(P(x) \wedge Q(x))$, why?)
    2. $\exists x(P(x) \wedge \neg R(x))$
  - We shall prove/disprove $\exists x(Q(x) \wedge \neg R(x))$
  - By $\exists x(P(x) \wedge \neg R(x))$, we have an x_0 s.t. $P(x_0) \wedge \neg R(x_0)$
  - Since $\forall x(P(x) \rightarrow Q(x))$, $P(x_0) \rightarrow Q(x_0)$
  - Therefore, $Q(x_0) \wedge \neg R(x_0)$
  - By taking x to x_0, we have $\exists x(Q(x) \wedge \neg R(x))$

1. Instantiate: Remove $\exists$ / $\forall$
2. Deduce …
3. Generalize: Take $\exists$ / $\forall$ back

Nested Quantifiers

- **We can have nested quantification.**
- **In fact, you have seen it in calculus!**
- **E.g., the definition of limit uses nested quantifiers.**
  - Recall the definition of

    $\lim_{x \to a} f(x) = b$
  - $\forall \varepsilon \exists \delta (|x - a| < \delta \to |f(x) - b| < \varepsilon)$

- **Nested quantifiers**
  - Quantifiers that occur **within the scope** of other quantifiers

- **Think of quantification as loops**
  - Nested quantification $\Leftrightarrow$ nested loops
    - $\forall x \forall y P(x, y)$
    - $\forall x \exists y P(x, y)$

Nested Quantifiers

- **The order of nested quantification is important.**
  - Unless all quantifiers are universal ones or existential ones, the order of quantifiers make differences
- **E.g., what are the truth values of the following statements?**
  - Q: $\forall x \exists y(x = y)$ =?
  - A:
  - Q: $\exists y \forall x\ (x = y)$ =?
  - A:
  - Q: $\forall x \exists y(y \leq |x|)$ =?
  - A:
  - Q: $\exists y \forall x(y \leq |x|)$ =?
  - A:
- **In fact, we have $\exists y \forall x P(x, y) \rightarrow \forall x \exists y P(x, y)$.**
  - Pf: DIY

Example

- **Show that $\exists y \forall x P(x, y) \rightarrow \forall x \exists y P(x, y)$.**
- **Pf:**
  - By $\exists y \forall x P(x, y)$, we have some y_0 and arbitrary x_0 s.t. $P(x_0, y_0)$
  - $\exists y P(x_0, y)$
  - $\forall x \exists y P(x, y)$

1. Instantiate: Remove $\exists$ / $\forall$
2. Deduce …
3. Generalize: Take $\exists$ / $\forall$ back

- **Disprove $\forall x \exists y P(x, y) \rightarrow \exists y \forall x P(x, y)$**
  - DIY

A More Complex Example

- **Translate the following statement into English**

  $\forall x(C(x) \lor \exists y(C(y) \land F(x, y)))$,

  where $C(x)$ is "x has a computer,"

  $F(x, y)$ is "x and y are friends," and

  the domain of x and y are students in NCTU

- **Sol:**
  - For every student x in NCTU, x has a computer or there is a student y s.t. y has a computer and x and y are friends.
  - i.e., "Every NCTU student has a computer or has an friend in NCTU student has a computer."

Combinations of Nested Quantifiers

Statement	When true?	When false?
$\forall x \forall y P(x,y)$ $\forall y \forall x P(x,y)$	$P(x,y)$ is true for every (x,y) pair	There is a (x,y) pair for which $P(x,y)$ is false
$\forall x \exists y P(x,y)$	For every x there is a y for which $P(x,y)$ is true	There is an x for which $P(x,y)$ is false for every y
$\exists x \forall y P(x,y)$	There is an x for which $P(x,y)$ is true for every y	For every x there is a y for which $P(x,y)$ is false
$\exists x \exists y P(x,y)$ $\exists y \exists x P(x,y)$	There is a (x,y) pair for which $P(x,y)$ is true	$P(x,y)$ is false for every (x,y) pair

Negating Nested Quantifiers

- **E.g.,**
  - Q: $\neg\forall x\exists y(xy = 1) \equiv ?$
  - A: $\neg(\forall x\exists y(xy = 1)) \equiv \exists x\neg(\exists y(xy = 1))$
    $\equiv \exists x\forall y\neg(xy = 1)$
    $\equiv \exists x\forall y(xy \neq 1)$
    true, take x to be 0
  - Q: $\neg\forall x\exists y(xy = 0) \equiv ?$
  - A: $\neg\forall x\exists y(xy = 0) \equiv \exists x\neg\exists y(xy = 0)$
    $\equiv \exists x\forall y\neg(xy = 0)$
    $\equiv \exists x\forall y(xy \neq 0)$
    false, take y to be 0

Rules of Inference

- **An argument in propositional logic is a sequence of propositions. The final proposition in an argument is called the conclusion; the others are called premises.**

argument:

$$\left.\begin{array}{c} A_1 \\ A_2 \\ \cdots \\ A_n \end{array}\right\} \text{premises}$$

$$\overline{\qquad\qquad}$$

$\therefore B$ ⇨ conclusion

$\therefore$ therefore

- A conclusion is true if a set of premises are all true, i.e.,

$$\frac{A_1 \wedge A_2 \wedge \ldots \wedge A_n}{\therefore B}$$

Rules of Inference (1/2)

- **Some rules of inference are useful when you write proofs.**

Rule of Inference	Name
$\dfrac{p}{\therefore \quad p \vee q}$	Addition
$\dfrac{p \wedge q}{\therefore \quad p}$	Simplification
$\dfrac{p \qquad q}{\therefore \quad p \wedge q}$	Conjunction
$\dfrac{p \qquad p \rightarrow q}{\therefore \quad q}$	Modus ponens
$\dfrac{\neg q \qquad p \rightarrow q}{\therefore \quad \neg p}$	Modus tollens
$\dfrac{p \rightarrow q \qquad q \rightarrow r}{\therefore \quad p \rightarrow r}$	Hypothetical syllogism

Rules of Inference (2/2)

Rule of Inference	Name
$\dfrac{p \vee q \qquad \neg p}{\therefore \quad q}$	Disjunctive syllogism
$\dfrac{p \vee q \qquad \neg p \vee r}{\therefore \quad q \vee r}$	Resolution
$\dfrac{\forall x P(x)}{\therefore \quad P(c)}$	Universal instantiation
$\dfrac{P(c) \text{ for an arbitrary } c}{\therefore \quad \forall x P(x)}$	Universal generalization
$\dfrac{\exists x P(x)}{\therefore \quad P(c) \text{ for some element} c}$	Existential instantiation
$\dfrac{P(c) \text{ for some element } c}{\therefore \quad \exists x P(x)}$	Existential generalization

Resolution

- **Resolution principle**

$$\begin{array}{ll} & p \lor q \qquad \neg p \lor r \\ \hline \therefore & q \lor r \end{array}$$

- **Pf:**

$$\begin{array}{ll} & p \lor q \equiv \neg q \to p \\ & \neg p \lor r \equiv p \to r \\ \hline \therefore & \neg q \to r \equiv q \lor r \end{array}$$

Example of Inference

- **E.g.,**

  "If today is sunny, we'll have a BBQ today"

  "Today is sunny"

  ∴ "We will have a BBQ today"

- **E.g.,**

  "If today is sunny, we'll have a BBQ today"

  "We won't have a BBQ today"

  ∴ "Today is not sunny"

- **E.g.,**

  "If it's raining today, we won't have a BBQ today"

  "If we don't have a BBQ today, we will have a BBQ tomorrow"

  ∴ "If it is raining today, then we will have a BBQ tomorrow"

Inference for Quantified Statements

- **To prove ¬(∀*x*)*P*(*x*)**
  - Exhibit any member in the domain for which *P*(*x*) is false
  - One counterexample suffices
  - e.g., disprove "交大無帥哥"

- **To prove ¬(∃*x*)*P*(*x*)**
  - Let *x* be an arbitrary (unrestricted) member in the domain and prove that *P*(*x*) is false

59

Proof

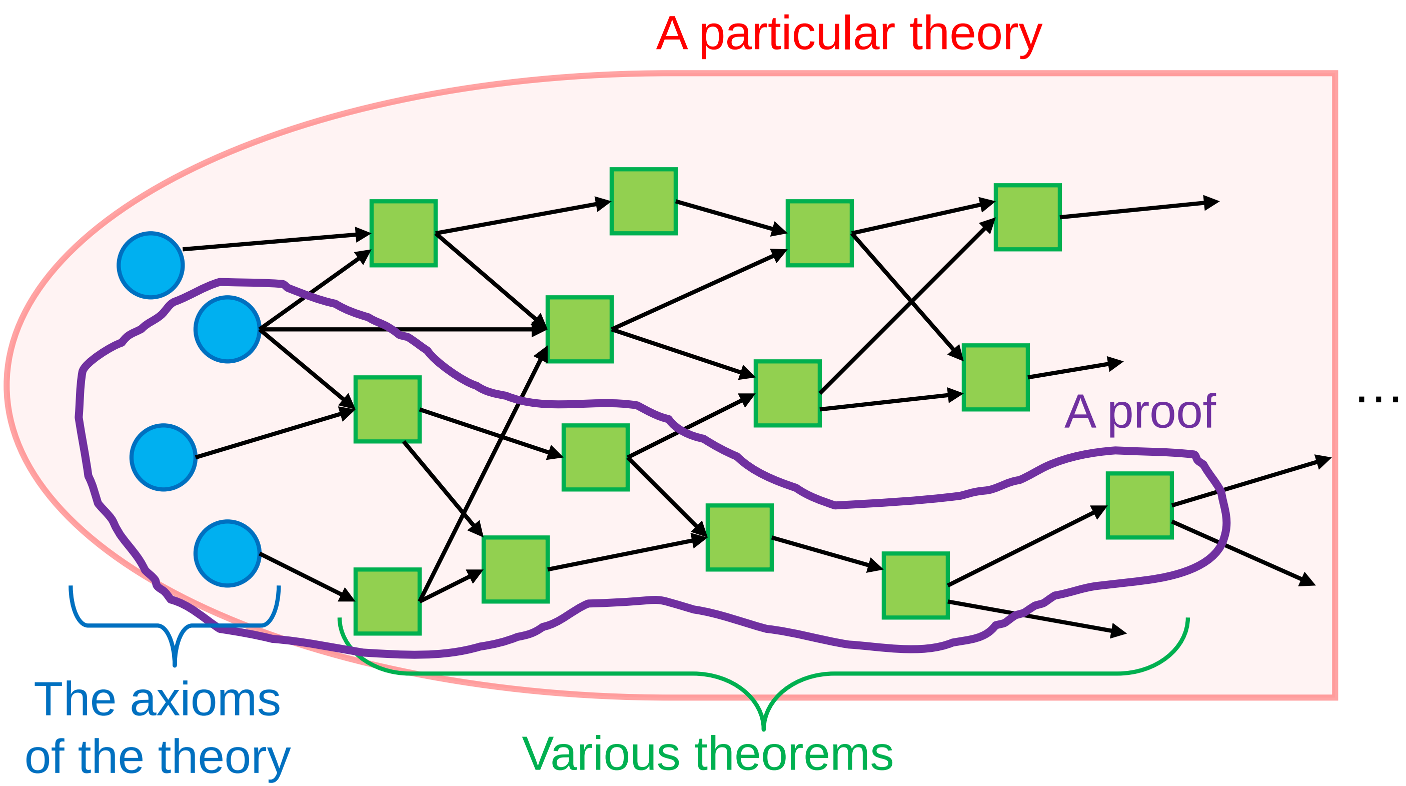
Proof Terminology (1/2)

- **Theorem**
  - A statement that has been proven to be true.
- **Axioms, postulates, hypotheses, premises**
  - Assumptions (often unproven) defining the structures about which we are reasoning.
- **Rules of inference**
  - Patterns of logically valid deductions from hypotheses to conclusions.

Proof Terminology (2/2)

- **Lemma**
  - A minor theorem used as a stepping-stone to proving a major theorem
- **Corollary**
  - A minor theorem proved as an easy consequence of a major theorem
- **Conjecture**
  - A statement whose truth value has not been proven
- **Theory**
  - The set of all theorems that can be proven from a given set of axioms

Graphical Visualization



Proving Theorems

- **The form of a theorem:**
  - $\forall x(P(x) \rightarrow Q(x))$
- **Methods of proving theorems**
  - Direct proof
  - Proof by contraposition
  - Proof by contradiction

- **Please read Section 1.7. It takes effort to know how to write correct proofs. When you read the text, please try to understand how the statements are proved, instead of what the statements are proving.**

Direct Proof

- **Prove $p \rightarrow q$**
  1. The first step: Assume p is true
  2. … rules of inference …
  3. The final step: q must also be true

- **E.g., show that "if n is an odd integer, then n^2 is odd."**
- **Pf:**
  - Assume $n = 2k + 1$, where k is an integer
  - $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$
  - Therefore, n^2 is odd.

Proof by Contraposition (Indirect)

- **Prove $p \to q$**
  - Prove its contrapositive, $\neg q \to \neg p$, instead
    - $p \to q \equiv \neg q \to \neg p$

- **E.g., show that "If 3n + 2 is odd, then n is odd."**
- **Pf.**
  - Assume n is even; $n = 2k$ for some integer k
  - Substituting $2k$ for n, $3n + 2 = 3(2k) + 2 = 2(3k + 1)$
  - $3n + 2$ is even

Proof by Contradiction (1/4)

- **Prove *p***
  - Find a contradiction q s.t. $\neg p \rightarrow q$
    - Since q is false and ($\neg p \rightarrow q$) is true, p is true
    - Key: how to find a contradiction q?

- **We demonstrate some proofs by two simple theorems in elementary number theory. Dr. Hardy (a renowned mathematician) thinks both theorems are of the highest class (in A Mathematician's Apology). They are actually proved by the Greek two thousands years ago!**

Proof by Contradiction (2/4)

- **(Euclid) There are infinitely many primes.**
- **Pf.**
  - Suppose there are finitely many primes;
    2, 3, 5, …, p is the list of all primes.
  - Consider $q = (2 \times 3 \times 5 \times \ldots \times p) + 1$.
  - Clearly, q is not divisible by any of the primes 2, 3, 5, …, p.
    A contradiction.

Proof by Contradiction (3/4)

- **The real number r is rational if there are integers p and $q \neq 0$ s.t. $r = p/q$.**
- **(Pythagoras) $\sqrt{2}$ is not rational.**
- **Pf.**
  - Suppose $\sqrt{2} = a/b$ where gcd(a, b) = 1
  - Then $2 = (a/b)^2$. $a^2 = 2b^2$
  - Since a^2 is even, a must be even
  - Let $a = 2k$. Then $a^2 = 4k^2 = 2b^2$
  - $2k^2 = b^2$, and b must be even
  - This is a contradiction to gcd(a, b) = 1

Proof by Contradiction (4/4)

- **Prove a conditional statement $p \rightarrow q$ by contradiction**
  1. Assume $\neg q$
  2. Arrive at a contradiction using p and $\neg q$
  - $p \rightarrow q \equiv (p \wedge \neg q) \rightarrow \mathbf{F}$

- **Rewrite proof by contraposition as proof by contradiction**
  - Suppose both p and $\neg q$ are true
  - Use the steps proving $\neg q \rightarrow \neg p$ to show that $\neg p$ is true
  - This leads to the contradiction $p \wedge \neg p$

- **Rewrite direct proof as proof by contradiction**
  - Assume both p and $\neg q$ are true
  - Show that q must be true
  - This implies that q and $\neg q$ are both true, a contradiction

Proof by Other Methods

- **Prove by cases**
  - $((p_1 \vee p_2 \vee \ldots \vee p_n) \rightarrow q) \equiv$
    $((p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \ldots \wedge ((p_n \rightarrow q))$
  - e.g., prove $|xy| = |x||y|$ where x and y are real numbers
    - Divide into 4 cases

- **Prove by equivalence**
  - $(p \leftrightarrow q) \equiv ((p \rightarrow q) \wedge (q \rightarrow p))$
  - $(p_1 \leftrightarrow p_2 \leftrightarrow \ldots \leftrightarrow p_n) \equiv (p_1 \rightarrow p_2) \wedge (p_2 \rightarrow p_3) \wedge \ldots \wedge (p_n \rightarrow p_1)$

Uniqueness Proof (1/2)

- **Some theorems assert the existence of a unique element with a particular property**
  - The proof should contain 2 parts
  - 1st part: existence proof
  - 2nd part: uniqueness proof
- **Existence proof**
  - Constructive method: find an element x_0 s.t. $P(x_0)$ is true
  - Nonconstructive method: say, proof by contradiction
- **Uniqueness proof**
  - Show that if $x \neq x_0$, then x does not have the desired property
  - $\exists x(P(x) \wedge \forall y(y \neq x \rightarrow \neg P(y)))$

Uniqueness Proof (2/2)

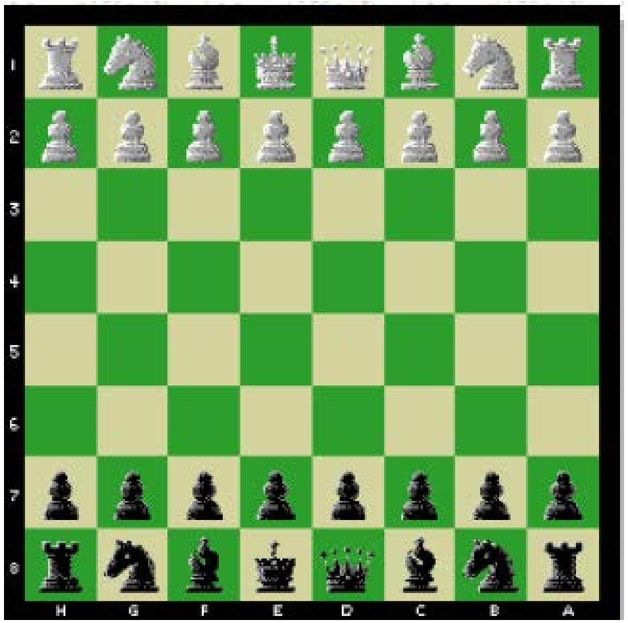
- **Show that if p is an integer, then there exists a unique integer q such that $p + q = 0$.**
- **Pf.**
  - Proving existence
    - $p + q = 0$, take q to be $-p$, q is also an integer
  - Proving uniqueness
    - Assume r is an integer with $r \neq q$ such that $p + r = 0$
    - Then, $p + r = 0$, we have $p + r = 0 = p + q$
    - $r = q$, a contradiction

Mistakes in Proofs

- **Q: What is wrong with the following "proof" of 1 = 2?**
  1. Let a and b be two equal positive numbers. Hence, $a = b$.
  2. We multiply both sides by a and have $a^2 = ab$
  3. Subtract b^2 from both sides, we have $a^2 - b^2 = ab - b^2$
  4. Thus, $(a + b)(a - b) = b(a - b)$
  5. Therefore $a + b = b$
  6. Since $a = b$, we have $2b = b$ and $2 = 1$.
- **A:**

Covering a Chessboard

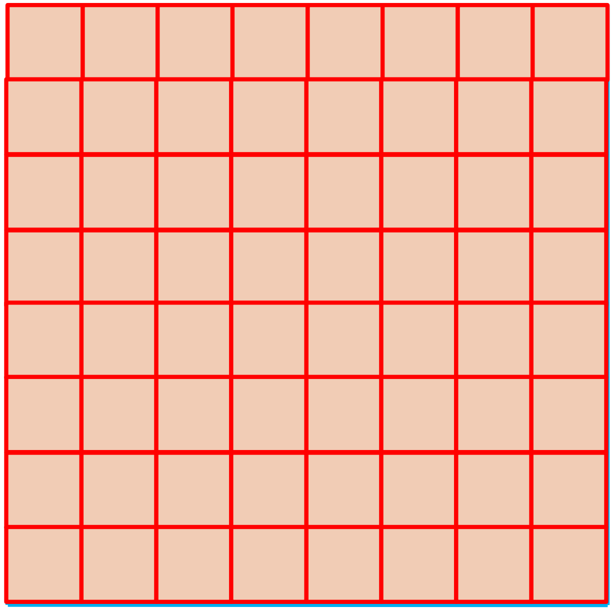
- It all begins with a chessboard

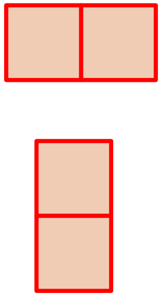


by Courtesy of Prof. C. L. Liu

Covering a Chessboard

- **Cover the 8x8 chessboard with thirty-two 2x1 dominoes.**
- **Is it possible?**
- **A: Yes. 8x8 = 64 = 32x(2x1)**



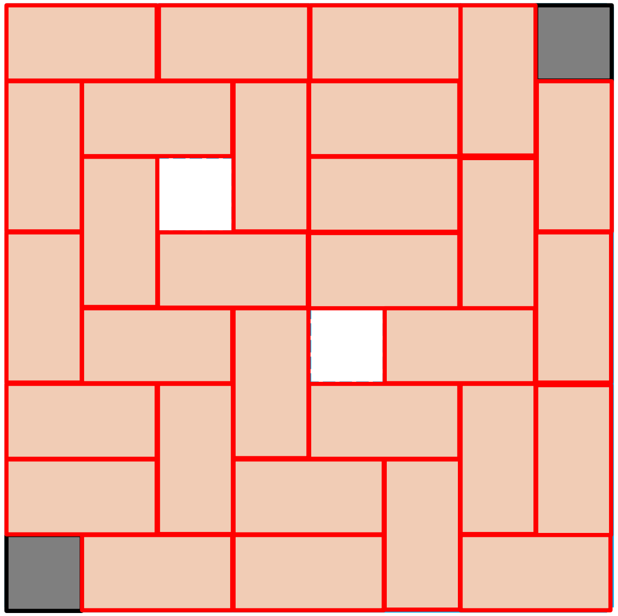


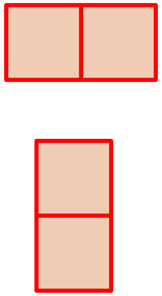
2x1 domino

by Courtesy of Prof. C. L. Liu

A Truncated Chessboard

- Cover the truncated 8x8 chessboard with thirty-one 2x1 dominoes. Is it possible?
- First attempt: 8x8 – 2 = 62 = 31x(2x1)



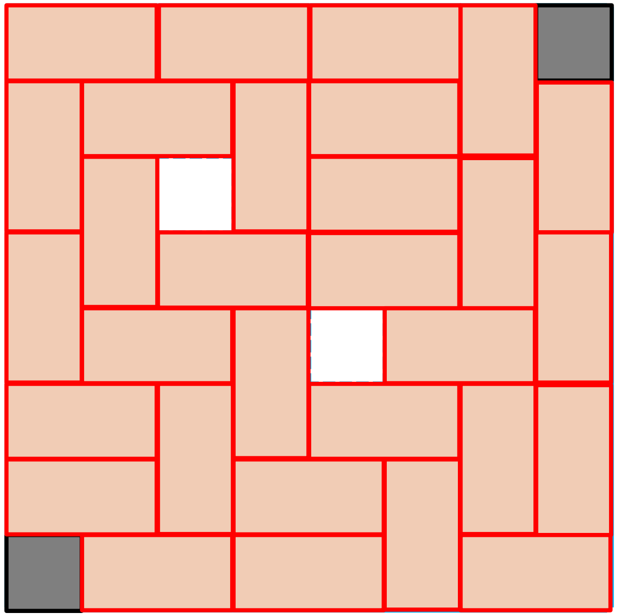


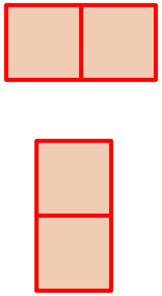
2x1 domino

by Courtesy of Prof. C. L. Liu

Proof of Impossibility

- **Impossible to cover the truncated 8x8 chessboard with thirty-one dominoes.**



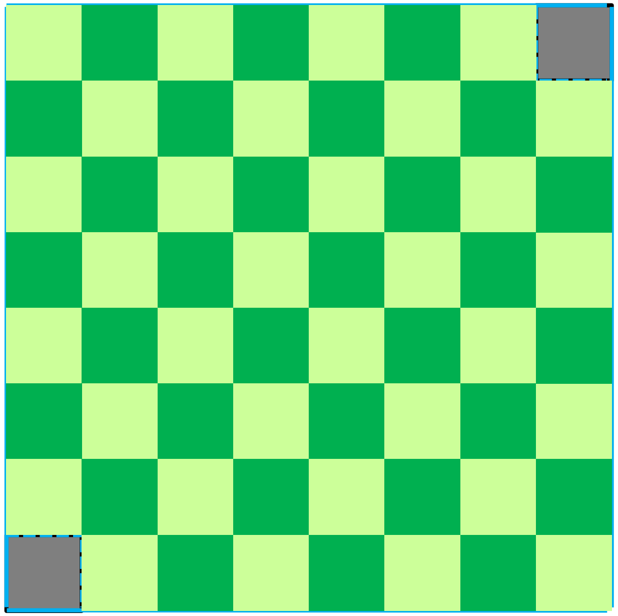


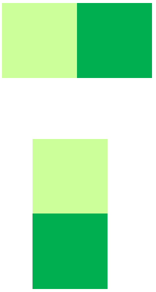
2x1 domino

by Courtesy of Prof. C. L. Liu

Proof of Impossibility

- **Impossible to cover the truncated 8x8 chessboard with thirty-one dominoes.**
- **There are thirty-two white squares and thirty black squares**
- **A 2x1 domino always covers a white and a black square**





2x1 domino

by Courtesy of Prof. C. L. Liu

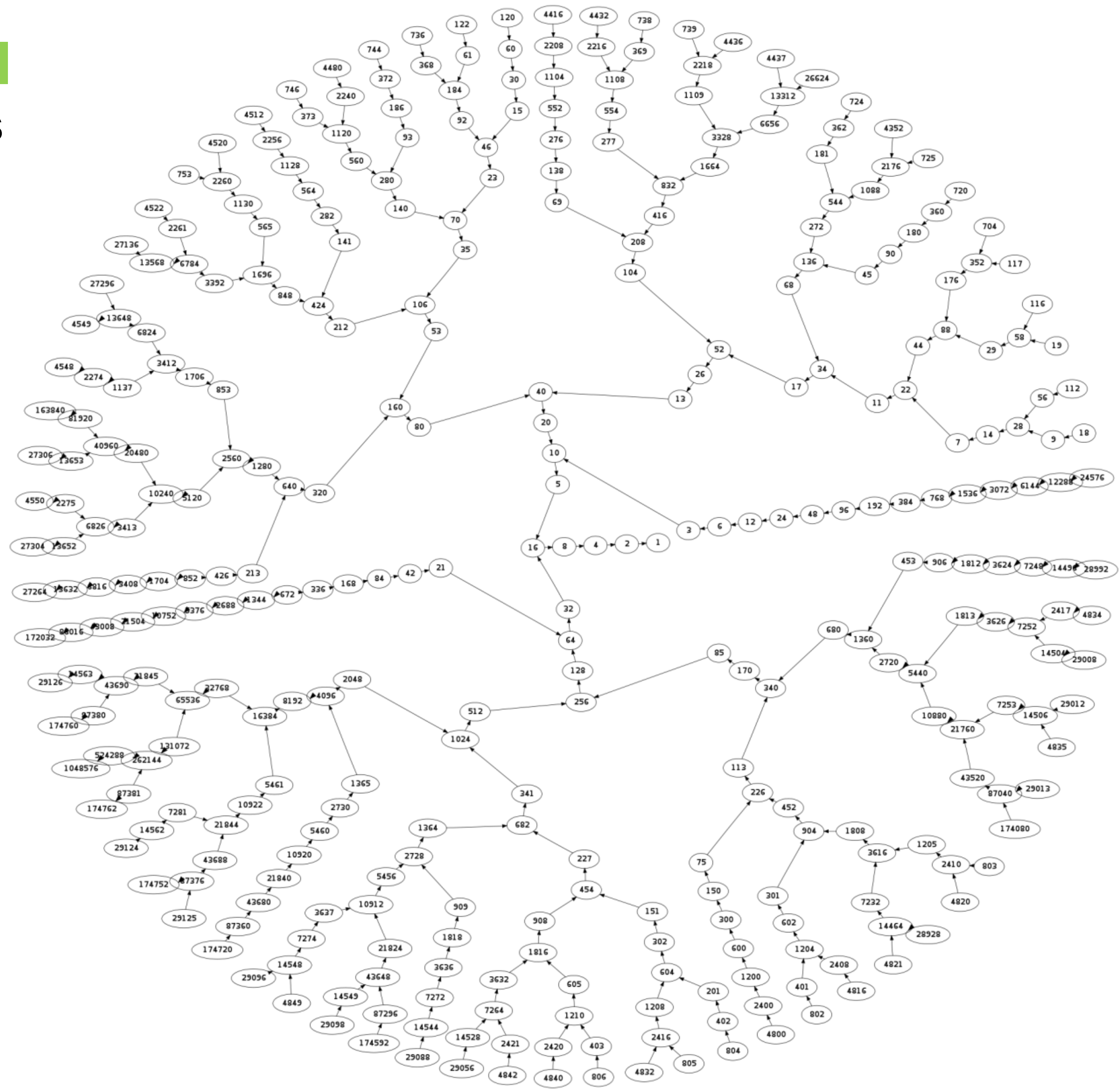
Conjecture

- **Sometimes, we may make a statement without knowing whether it is true or not. Such statements are called conjectures. When a conjecture is made, we can either prove it and make it a theorem. Or, we can find a counterexample to illustrate the conjecture is false.**
- **E.g., the 3*n*+1 conjecture**
  - Define the function $T: Z+ \to Z+$
    - $$T(n) = \begin{cases} k & \text{if } n = 2k \\ 3n + 1 & \text{if } n = 2k + 1 \end{cases}$$
  - The 3*n*+1 conjecture states that for all positive integer *n*, we will eventually reach 1 if we apply *T* repeatedly.

http://mathworld.wolfram.com/CollatzProblem.html

3*n*+1 Conjecture

- The first 20 levels



- Show that $A \leftrightarrow B \equiv (\neg A \land \neg B) \lor (A \land B)$
- $A \leftrightarrow B \equiv (A \to B) \land (B \to A) \equiv (\neg A \lor B) \land (\neg B \lor A)$

$$\equiv (\neg A \land \neg B) \lor (\neg A \land A) \lor (B \land \neg B) \lor (B \land A)$$

$$\equiv (\neg A \land \neg B) \lor F \lor F \lor (B \land A)$$

$$\equiv (\neg A \land \neg B) \lor (B \land A)$$

$$\equiv (\neg A \land \neg B) \lor (A \land B)$$

Why to Learn Logic?

- **Q: Why should we learn logic? It's like we are just reviewing what we have learned from "logic design."**
- **A:**
  - Much more than logic design. We are just trying to link the topic with what we learned before.
  - The rules of logic specify the meaning of mathematical statements.
  - Students must understand mathematical reasoning in order to read, comprehend, and construct mathematical arguments.
    - We start with a discussion of mathematical logic—the foundation of methods of proof.

Muddy Children Puzzle (1/2)

- **Muddy children puzzle**
  - After playing in their backyard, John and Mary get mud on their foreheads without knowing it. (But each can see the other's forehead is dirty, though.)
  - When they go home, their mother says "At least one of you has a muddy forehead," and asks the children to answer the question: "Do you know whether you have a muddy forehead?" The mother asks the question twice.
  - What will the children answer each time the question is asked?
  - Assume both are honest and answer questions simultaneously.

Muddy Children Puzzle (2/2)

- **Sol:**
  - Let j and m denote John and Mary has a muddy forehead.
  - When the mother asks the question the first time, both know $j \vee m$ is true. Although they can see the mud in the other's forehead, no one can tell whether his or her forehead is dirty. Hence both can only answer “No” to the question.
  - After the question is asked, John knows his forehead is dirty by the following reasoning. If his forehead was clean, Mary would know immediately that her forehead is dirty. Since Mary answers “No” to the question, John realizes his forehead must be dirty. Symmetrically, Mary knows her forehead is dirty after the question is asked.
  - Hence when the mother asks the question the second time, both will answer “Yes” to the question.