EECS 660: FUNDAMENTALS OF COMPUTER ALGORITHMS

MODULE I: LOGIC AND PROOF

DISCLAIMER

- This document is intended to be used for studying EECS 660 Data Structures, only by students who are currently enrolled in the course.

- This document is a copyright of Dr. Cuncong Zhong. Distribution of this document, or use it for any purpose other than what is stated above, is considered as a copyright infringement. Dr. Cuncong Zhong reserves the right to take necessary legal action.

- If you disagree, please delete the document immediately.

ACKNOWLEDGEMENT

- Many of the figures, unless otherwise stated, come from ***Algorithm Design*** 4th edition, by Jon Kleinberg and Eva Tardos.

RECAP OF PROOF LOGIC

- Proof is an important part in algorithm, as we need to show that the algorithm we propose correctly solves the problem.
- The construction of proof is another piece of art, just like algorithm design.
- But there are guidelines that help us judge whether a proof is correct.
- Here we will quickly review some basic topics in Discrete Math.

PROOF LOGIC: STATEMENT

- A mathematical proof can be broken down into a number of sentences.
- For each sentence we must be able to determine whether it is true of not.
  - for example, we can determine the truth value of "one plus one equals to two"
  - but we cannot determine the truth value of "she feels happy", nor "how beautiful the ocean is!"
- Such sentences are called statements.

PROOF LOGIC: STATEMENT

- There are two ways to make a statement.
- The first way is to state an axiom (which is always true) or contradiction (which is always false). And it is trivial to tell their truth values.
- The second way is to through specifying or quantifying parameters for open statement forms.
  - For example: "She is a student of KU" is an open statement form, also called a predicate.
  - It is open because we cannot know its truth value unless who "she" is is specified.

PROOF LOGIC: STATEMENT

- Specifying parameters of a predicate:
  - Once the parameters (or arguments) of a predicate are specified, a predicate becomes a statement and we can determine its truth value.
  - For example, we will be able to determine the truth value of "Mary is a student of KU".
  - We can also write a statement in the form of function, say $P(x)$, where $P(.)$ indicates the predicate ". is a student of KU", and x indicates a specific women.

- Note that a predicate can take multiple parameters, just like regular math functions
  - for example, a predicate "x is a student of y" takes two parameters x and y and can be written as $P(x, y)$

PROOF LOGIC: STATEMENT

- Quantifying parameters of a predicate:
  - using either the universal quantifier ∀ or the existential quantifier ∃
  - *For the predicate $Q(x)$ "x is a student of KU", we can combine the existential quantifier with it and say "there exists a person, and the person is a student of KU". The sentence is now a statement because we can verify whether there is a person enrolled in KU. We can denote the statement derived from combining a quantifier and a statement as $\exists x, Q(x)$.*

- Similarly, for a given predicate, multiple quantifiers on multiple parameters may apply.
  - $\exists x, y\ Q(x, y)$ means "there exists a women who attends a university".
  - $\exists x, \forall y\ Q(x, y)$ means "there exists a women who has attended all universities of the world"

PROOF LOGIC: STATEMENT

- In many cases, we may also specify the domain for the parameters when using quantifiers. If no domain is specified, the default domain is the universe.
  - *Let $P(x, y)$ be "x is a student of y". $\exists x \in \{Mary, Jack\}, y \in \{KU, KSU\}, Q(x, y)$ indicates: one of the following four statements is true: 1) Mary enrolled in KU; 2) Mary enrolled in KSU; 3) Jack enrolled in KU; and 4) Jack enrolled in KSU.*

PROOF LOGIC: STATEMENT

- Determining the truth value of a statement associated with the universal quantifier ∀:
  - A statement derived from a universal quantifier ∀ is true if, for every combination of the parameters within their respective domains, it is true.
  - A statement derived from a universal quantifier ∀ is false if, for any combination of the parameters within their respective domain, it is false.
  - *Let $Q(x)$ be "x is a student of KU". The statement $\forall x \in \{Mary, Jack\}, Q(x)$ is true if all people named Mary or Jack enrolled in KU. The statement is false if there exists a person whose name is either Mary or Jack and is not enrolled in KU.*
  - In a word, we can disprove a universal statement by counterexample.

PROOF LOGIC: STATEMENT

- Determining the truth value of a statement associated with the existential quantifier ∃:
  - A statement derived from a universal quantifier ∃ is true if, for any combination of the parameters within their respective domains, it is true.
  - A statement derived from a universal quantifier ∃ is false if, for every combination of the parameters within their respective domain, it is false.
  - *Let $Q(x)$ be "x is a student of KU". The statement $\exists x \in \{Mary, Jack\}, Q(x)$ is true there exists a person named Mary or Jack and is enrolled in KU. The statement is false if no student enrolled in KU is named Mary nor Jack.*
  - In a word, we can prove an existential statement by example.

PROOF LOGIC: STATEMENT

- Summary
  - A statement is a sentence for which we can determine its truth value
  - A statement could be an axiom/contradiction, a predicate with specified parameters, or a predicate with quantified parameters

- For simplicity, we will denote statements as lower-case letters instead of using its function notation
  - we will use, say p, to indicate statements when its function form $Q(x, y)$ is not required

PROOF LOGIC: COMPOUND STATEMENT

- Multiple statements can be combined to form a new statement, i.e., a compound statement.

- There are four elementary **logical operators** to combine two statements
  - conjunction (AND)
  - disjunction (OR)
  - negation (NOT)
  - condition (IF)

- Other logical operators, such as XOR (either but not both), can be derived from these four elementary logical operators.

PROOF LOGIC: COMPOUND STATEMENT

- A conjunction (AND) statement if true if both of its elementary statements are true, and is false if either of its elementary statements is false.

- *Example: Let p be "Mary is a student of KU", and q be "Mary received an A in EECS 660". The conjunction of p and q gives a new statement: "Mary is a student of KU, and she received an A in EECS 660". The conjunction of p and q is denoted as $p \wedge q$ and read "p and q". The statement is true when both Mary is a student of KU (i.e., p) is true and Mary received an A in EECS 660 (i.e., q) is true. The statement is false when either statement is false.*

PROOF LOGIC: COMPOUND STATEMENT

- A disjunction (OR) statement if true if either of its elementary statements is true, and is false if both of its elementary statements are false.

- *Example: Let p be "We ate McDonalds today", and q be "We ate Pizza Hut today". The disjunction of p and q gives a new statement: "Either we ate McDonalds or Pizza Hut today". The disjunction of p and q is denoted as $p \vee q$ and read "p or q". The statement is true if either we ate McDonalds or Pizza Hut today, and is false if we didn't eat McDonalds nor Pizza Hut today.*

PROOF LOGIC: COMPOUND STATEMENT

- A disjunction (NOT) statement if true if its elementary statement is false, and is false if its elementary statements is true.

- *Example: Let p be "Mary is a student of KU". The negation of p is "Mary is not a student of KU". The negation of p is denoted as $\neg p$ and read "not p".*

PROOF LOGIC: COMPOUND STATEMENT

- A conditional statement (IF) consists of one statement as the condition, and another as the conclusion. A conditional statement is false only if the condition is true and the conclusion is false.

- *Example: Let p be "Today is sunny", and q be "We play soccer". The conditional statement that combines p and q is: "If today is sunny, then we will play soccer". The conditional statement of p and q is denoted as $p \rightarrow q$ and read "if p then q" or "p implies q".*

PROOF LOGIC: COMPOUND STATEMENT

- A special note on conditional statement

- If the condition is false, then no matter whether the conclusion is true or not, the conditional statement is true.
  - e.g., If 1+1=0, a professor will be rich.
  - Since you will never be able to know whether a professor is rich in a world where 1+1=0, you cannot claim the statement is false. Hence it is true.

PROOF LOGIC: TRUTH TABLE

- Truth tables summarize how we determine the truth values of the above four component statements, given different combinations of truth values for their elementary statements.

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

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

p	$\neg p$
T	F
F	T

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

PROOF LOGIC: COMPLEX COMPOUND STATEMENTS

- We know that simple compound statements are constructed via a single conjunction, disjunction, negation, or condition.

- More complex statements can be constructed by recursively applying any combination of conjunction, disjunction, negation, and condition.

PROOF LOGIC: COMPLEX COMPOUND STATEMENTS

- The precedence of the four elementary logical operators is (from high to low):
  - NOT
  - AND
  - OR
  - IF

- For clarity, use parenthesis.

PROOF LOGIC: COMPLEX COMPOUND STATEMENTS

- The truth value of complex compound statements can be worked out using truth table.
- The number of rows of the truth table should be the number of different truth value combinations of the elementary statements.
- The number of columns should be the number of elementary statements plus the number of logical operators (or less).

PROOF LOGIC: COMPLEX COMPOUND STATEMENTS

- Determine the truth value of $\neg(p \vee q)$ (under all truth value combinations of p and q.

- We should construct a truth table with four rows (all truth value combination of two element statements p and q) and four columns (two elementary statements and two logical operators: negation and conjunction).

PROOF LOGIC: COMPLEX COMPOUND STATEMENTS

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

PROOF LOGIC: LOGICAL EQUIVALENCE

- Although we can construct an arbitrarily complex compound statement, but it is not easy to compute the truth value and difficult to understand when translated to human language.
- We can transform complex component statements into different forms for simplicity and clarity with logical equivalence.
- Two statements are called logically equivalent if for any given combination of values of the elementary statements, the truth values for both statements are identical. Denote logical equivalence with "≡".

PROOF LOGIC: LOGICAL EQUIVALENCE

- A set of laws can used to establish logical equivalence between compound statements.
- In many cases, our goal is to establish logical equivalence between a seemingly long and complicated statement and a short and easy statement.

PROOF LOGIC: LOGICAL EQUIVALENCE

- An important law is de Morgan low, which states that $\neg(p \wedge q) \equiv \neg p \vee \neg q$ and $\neg(p \vee q) \equiv \neg p \wedge \neg q$.

- We can prove it using truth table.

PROOF LOGIC: LOGICAL EQUIVALENCE

- Prove that $\neg(p \vee q) \equiv \neg p \wedge \neg q$:

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

PROOF LOGIC: LOGICAL EQUIVALENCE

- Prove that $\neg(p \wedge q) \equiv \neg p \vee \neg q$:

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

PROOF LOGIC: LOGICAL EQUIVALENCE

- Commutative laws: $p \wedge q \equiv q \wedge p$, and $p \vee q \equiv q \vee p$
- Associative laws: $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$, and $(p \vee q) \vee r \equiv p \vee (q \vee r)$
- Distributive laws: $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$, and $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
- Identity laws: $p \wedge t \equiv p$, and $p \vee c \equiv p$
- Negation laws: $p \vee \neg p \equiv t$, and $p \wedge \neg p \equiv c$
- Contraposition law: $p \rightarrow q \equiv \neg q \rightarrow \neg p$

PROOF LOGIC: LOGICAL EQUIVALENCE

- Double negative law: $\neg(\neg p) \equiv p$
- Idempotent laws: $p \wedge p \equiv p$, and $p \vee p \equiv p$
- Universal bound laws: $p \vee t \equiv t$, and $p \wedge c \equiv c$
- de Morgan's laws: $\neg(p \wedge q) \equiv \neg p \vee \neg q$, and $\neg(p \vee q) \equiv \neg p \wedge \neg q$
- Absorption laws: $p \vee (p \wedge q) \equiv p$, and $p \wedge (p \vee q) \equiv p$
- Negations of t and c: $\neg t \equiv c$, and $\neg c \equiv t$

PROOF LOGIC: ARGUMENT

- When proving, we are trying to argue what we are trying to prove is correct.
- So, we are constructing an argument.
- Formally, an argument is a collection of ordered statements.
  - it matters a lot regarding how we order our statements

PROOF LOGIC: ARGUMENT

- They way we order our statements is called argument form.

- Invalid argument form may lead to absurd arguments:
  - *Example: Let p be the statement "The suspect robbed a bank", q be "The suspect is rich", and the conditional compound statement $p \rightarrow q$ be "If the suspect robbed a bank, he/she will be rich". You can make the following absurd argument by presenting these statements in a wrong way: "If the suspect robbed a bank; the suspect is rich, therefore, the suspect robbed a bank." This argument can also be denoted as $p \rightarrow q$, q, then p. This argument is absurd if you plug in "Bill Gates" to replace the "suspect".*

PROOF LOGIC: ARGUMENT

- So, there must be a way that can objectively determine whether a given statement form is valid or not.

- To discuss the objective way, we first define premises and conclusion:
  - the last statement of an argument is called the conclusion
  - all the other statements of an argument are called the premises

PROOF LOGIC: ARGUMENT

- An argument form is valid if and only if that, for any combination of the truth value of the statements, if all the premises are true, then the conclusion is true.

- Proving the validity of an argument for can again be done using truth table.

PROOF LOGIC: ARGUMENT

- Consider the previous example, which has an argument form of $p \rightarrow q$, q, *then* p.
- We identify the premises as:
  - $p \rightarrow q$
  - q
- We identify the conclusion as:
  - p

PROOF LOGIC: ARGUMENT

- We can construct the following truth table:

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

- We see that there is a case (highlight in red) where all premises are true, but the conclusion is false. Therefore, the argument form $p \rightarrow q, q,$ *then* p is invalid.

PROOF LOGIC: ARGUMENT

- Another example: prove that the argument form $p \rightarrow q, p, then\ q$ is a valid argument form.

- Identify the premises:
  - $p \rightarrow q$
  - p

- Identify the conclusion:
  - q

PROOF LOGIC: ARGUMENT

- Construct the truth table:

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

- We see that the there exists only one case where all premises are true (highlight in red), and the corresponding conclusion is also true. Therefore, the argument form $p \rightarrow q, p, then\ q$ is valid.

PROOF LOGIC: ARGUMENT

- (More than two statements) *Prove that* $(p \vee q) \rightarrow r, p \vee q$, *then* r *is a valid argument form.*

p	q	$p \vee q$	r	$(p \vee q) \rightarrow r$	$p \vee q$	r
T	T	T	T	T	T	T
T	F	T	T	T	T	T
F	T	T	T	T	T	T
F	F	F	T	T	F	T
T	T	T	F	F	T	F
T	F	T	F	F	T	F
F	T	T	F	F	T	F
F	F	F	F	T	F	F

PROOF LOGIC: ARGUMENT

- Modus Ponens (if $p \rightarrow q, p$, then q)
  - *If today is sunny I will go play soccer. Today is sunny. I will go play soccer.*
- Modus Tollens (if $p \rightarrow q, \neg q$, then $\neg p$)
  - *If I am hungry, I will have lunch. I didn't have lunch. I am not hungry.*
- Generalization (p, then $p \vee q$; or q, then $p \vee q$)
  - *I like apple. Therefore I like apple or orange.*
- Specialization ($p \wedge q$, then p; or $p \wedge q$, then q)
  - *I like apple and orange. Therefore I like apple.*

PROOF LOGIC: ARGUMENT

- Elimination ($p \vee q, \neg p$, then q; or $p \vee q, \neg q$, then p)
  - *The outcome of my die rolling is either 3 or 5. It is not 3. So it must be 5.*
- Transitivity ($p \rightarrow q$ and $q \rightarrow r$, then $p \rightarrow r$)
  - *If today is sunny then I will go play soccer. If I go play soccer then I will need a shower. Today is sunny, then I will need a shower.*
- Proof by division into cases ($p \vee q, p \rightarrow r$, and $q \rightarrow r$, then r)
  - *I will either order noodles or hamburger from the restaurant. If I ordered noodles, I will love the restaurant. If I ordered hamburger, I will also love the restaurant. Therefore, I will love this restaurant.*

PROOF LOGIC: ARGUMENT

- We have now defined what is an valid argument form.

- A sound argument has two components
  - all premises are true
  - the argument form is valid
  - note that the definition of a valid argument form ensures that, when all premises are true, the conclusion (what we are trying to prove) must be true
  - consider a court case, to win it, you must collect sufficient evidences (i.e., the premises), and present them to the judge in a logical way (i.e., the valid argument form)

PROOF LOGIC: ARGUMENT

- An argument is unsound if it only has a valid argument form and not all of its premises are true.

- *Example: Let p be "John is a rock star", and q be "John has red hair". Consider the Modus Ponens argument form "if $p \rightarrow q$, p, then q", which is correct. However, the resulting argument "if John is a rock star, then John has red hair; John is a rock star, then John has a red hair" is obviously incorrect. This is because one of its premises: $p \rightarrow q$ is false (some rock star named John does not have red hair, e.g. John Lennon).*

PROOF LOGIC: ARGUMENT

- An argument is unsound if all of its premises are true but has an invalid argument form.

- *Example: Assume that you know a person named Tom who is a vegetarian. Let p be "Tom is a vegetarian", and q be "Tom does not eat meat on Friday". Consider the argument form "if $p \rightarrow q$, q, then p". However, the resulting argument "if Tom is a vegetarian, then Tom will not eat meat on Friday; Tom does not eat meat on Friday, then Tom is a vegetarian" is incorrect. Note that although all premises, and even the conclusion is true, the argument form "if $p \rightarrow q$, q, then p" is invalid. And Tom may just be a meat-lover who failed to catch his Jerry on Friday.*

PROOF TECHNIQUES

- In general, any proof is sound if all of its premises are true and are presented in a correct statement form.

- Proof is an art, but there are some commonly-see proof techniques we could try to begin with.
  - direct proof
  - indirect proof
  - mathematical induction

PROOF TECHNIQUES: DIRECT PROOF

- Direct proof: to construct an argument to show the conclusion (what we need to prove) is true.

- Generally speaking, we simply provide evidence for people to verify that the conclusion is true.

PROOF TECHNIQUES: DIRECT PROOF

- *Example: Prove that there exists an integer x such that $2x = x^2$.*
  - *Proof: There exists an integer 2 such that $2x = x^2$. (This is a single statement $\exists x\, Q(x)$, and we can prove it is true by giving an example.)*

- *Example: Show that the following statement "for all integers a and b, if $a^2 = b^2$ then $a = b$" is false.*
  - *Proof: Let $a = -1$ and $b = 1$. $a^2 = b^2$ and $a \neq b$. Therefore, the proposition is false. (This is a single statement $\forall x, y\, Q(x, y)$, and we can prove it is false by giving a counterexample.)*

PROOF TECHNIQUES: DIRECT PROOF

- *Example: Prove that for every integer x where $4 \leq x \leq 10$, it can be written as the sum of two primes.*
  - *Proof: Since x is an integer where $4 \leq x \leq 10$, it can only take values 4, 5, 6, 7, 8, 9, 10. We will show that each of these numbers can be written as the sum of two primes, as follows:*

    4=2+2, 5=2+3, 6=3+3, 7=2+5, 8=3+5, 9=2+7, 10=3+7

    Therefore, for every integer x where $4 \leq x \leq 10$, it can be written as the sum of two primes.

- In this example, we have a countable domain ($4 \leq x \leq 10$). We then present all the premises (e.g., 4=2+2, which are easy to be verified to be true) in an argument form of prove by division into cases. (Also called prove by exhaustion.) As a result, our proof is correct.

PROOF TECHNIQUES: DIRECT PROOF

- Previously, we are dealing with cases with finite and countable domains.
  - proving existential statement
  - disproving universal statement
  - a more general case with finite countable domain which we can exhaust

- In some case, we are facing infinite or uncountable domains (such as some properties on all real numbers).
  - we can use generalization of a generic particular

PROOF TECHNIQUES: DIRECT PROOF

- Generalization of a generic particular:
  - When the domain is unlimited or not countable, we can try to prove the conclusion by selecting an arbitrary particular from the domain, and show that choosing the generic particular can lead to the conclusion (particular). Note that we only expect the chosen particular to possess properties that are common to all elements in the domain under investigation (generic). Since the particular is chosen arbitrarily, it follows that every element within the domain must also lead to the conclusion (generalization).

PROOF TECHNIQUES: DIRECT PROOF

- *Example: Prove that for any real number, if you add that number by 5, multiply by 4, subtract 6, divide by 2, and subtract twice the original number, then you will have a final result of 7.*
  - *Prove: Since the domain (real number) is unlimited and not countable, we assume that x is an arbitrary real number. Let r be the resulting number after applying the set of operations on x, and we have:*

$$r = \frac{(x+5)*4-6}{2} - 2x = \frac{4x+14}{2} - 2x = 2x + 7 - 2x = 7$$

Since x is chosen as an arbitrary real number, the operations when applied to any real number must also result in an answer of 7.

- Note that we did not assume/use any property regarding x, except that it is a real number, which is given as a precondition.

PROOF TECHNIQUES: DIRECT PROOF

- In other cases, we do not need to provide concrete evidence, but only argue based on facts/axioms. This is called non-constructive direct proof, as we are not directly constructing evidences.

- *Example: Prove that there exists at least one node in a non-empty graph.*
  - *Proof: Since the definition of a non-empty graph is a graph with at least one node. Therefore, there exists at least one node in a non-empty graph.*

- Note that in many cases, even seem to be obvious, such argument is necessary to ensure the completeness of an argument, especially if we are using the conclusion as a premise for a larger proof. (We would rather be tedious than incomplete.)

PROOF TECHNIQUES: DIRECT PROOF

- To summarize, we have:

- Direct proof:
  - Constructive proof (provides evidences to verify the conclusion)
    - Prove the existence / disprove the universal by example / counterexample
    - Prove by exhaustion (countable and limited domain)
    - Prove by generalizing a generic particular (disprove the existence / prove the universal)
  - Non-constructive proof (does not provide evidences to verify the conclusion)

PROOF TECHNIQUES: INDIRECT PROOF

- Indirect proof tries to first prove some facts that are related to the conclusion, then indirectly prove the conclusion based on the proven facts.

- The reason we do that is because in some cases, direct proof is difficult to construct.

PROOF TECHNIQUES: INDIRECT PROOF

- For example, we would like to claim Chris like to play RTS (Real-Time Strategy) games.
  - It is hard to argue that Chris likes RTS games based on Chris's personality (e.g., visionary) and hobbies (e.g., like to watch warfare/historical movies)

- Indirect proof:
  - We can show that Chris play Warcraft III the most in his spare time
  - And Warcraft III is an RTS game
  - So we can show Chris like to play RTS game

PROOF TECHNIQUES: INDIRECT PROOF

- Prove by contradiction: it attempts to prove the conclusion by showing that, if the conclusion is false, some contradiction will happen.

- Proof by contradiction usually contains the following three steps:
  - Suppose the statement to be proved is false
  - Show that this supposition leads logically to a contradiction (often w.r.t a well-known fact or a precondition)
  - Conclude that the statement to be proved is true

PROOF TECHNIQUES: INDIRECT PROOF

- Prove by contradiction follows the **elimination** argument form: $p \vee q$, $\neg p$, then q
  - p: the contradiction will be led if the conclusion is false
  - q: the conclusion is true
  - $\neg p$: the contradiction is obviously false
  - q: the conclusion is true (an explicit statement)

PROOF TECHNIQUES: INDIRECT PROOF

- *Example: Prove that for all integers n, if $n^3 + 5$ is odd then n is even.*
  - *Proof: Suppose the proposition is wrong and if $n^3 + 5$ is odd then n is odd (assuming the conclusion we try to prove is wrong).*

  Without loss of generality, let $n = 2k + 1$ for some integer k, because n is odd. In this case, we have

  $$n^3 + 5 = (2k + 1)^3 + 5 = 8k^3 + 12k^2 + 6k + 6 = 2 * (4k^3 + 6k^2 + 3k + 3)$$

  and therefore, $n^3 + 5$ is an even number. The fact is contradicting with the condition that $n^3 + 5$ is odd, thus supposing n is an odd number leads to a contradiction (demonstrate the contradiction with the precondition).

  Therefore, if $n^3 + 5$ is odd then n is an even number (explicitly state that the conclusion must be true; the proof will not be complete if this step is missing).

PROOF TECHNIQUES: INDIRECT PROOF

- Proof by contraposition: instead of directly proving a conditional statement is true, we will indirectly prove its contraposition is true.

- Recall the contraposition law for logical equivalence: $p \rightarrow q \equiv \neg q \rightarrow \neg p$

PROOF TECHNIQUES: INDIRECT PROOF

- *Example: Prove that for all integers, if n^2 is even then n is even.*
  - *Proof: Let $n = 2k + 1$ be an odd number, where k is an arbitrary integer.*

  Then, $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$. Therefore, for all integers, if n is not an even number then n^2 cannot be even. And, for all integers, if n^2 is even then n is even.

- If we try to use direct prove: *n^2 is even then n is even,* then we need to argue the numerical properties of square root, which is difficult.
- If we try to use indirect prove: *n is odd then n^2 is odd,* then we only need to argue the numerical properties of squares, which is much easier.

PROOF TECHNIQUES: INDIRECT PROOF

- Note that a proof by contraposition can sometimes be very similar to proof by contradiction.

- *Example: Prove that for all integers, if n^2 is even then n is even, using proof by contradiction.*
  - *Proof: Suppose that if n^2 is even then n is odd (step 2).*

    Let $n = 2k + 1$ be an odd number, where k is an arbitrary integer. Then, $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$ and n^2 is odd. This leads to a contradiction with the fact that n^2 is even (step 2).

    Therefore, if n^2 is even then n is even.

- **It is very important to indicate clearly the underlying logic based on which the proof is constructed (or you may lose some points in the exam).**

PROOF TECHNIQUES: INDIRECT PROOF

- Indirect proof:
  - prove by contradiction
  - prove by contraposition

PROOF TECHNIQUES: MATHEMATICAL INDUCTION

- Mathematical induction is a technique to prove statements made on a sequence of entities.

- A sequence is defined as a function whose domain is either the list of all integers that are larger than or equal to a given integer (called an open domain), or the list of all integers between two given integers (called a closed domain).
  - *Example:* a_m, a_{m+1}, a_{m+2} *... denotes an infinite sequence in an open domain, and* $a_m, a_{m+1}, a_{m+2}, \ldots, a_n$ *denotes a finite sequence in a closed domain. While* $a_m, a_{m+2}, a_{m+4}, \ldots, a_n$ *is not a sequence because some indexes are not included; and it is not where math induction would be applicable.*

PROOF TECHNIQUES: MATHEMATICAL INDUCTION

- The goal of using math induction is to prove the conclusion is true on the entire (open or closed) domain.

- The naive idea of math induction is the follows:
  - the conclusion is true on the initial terms (a sequence starting from the very first index of the domain, i.e., $a_m, a_{m+1}, a_{m+2} \ldots a_{m+k}$); this can usually be shown by constructive direct prove (because the we only have a finite and countable number of initial terms) (the basis step)
  - show a_{m+k+1} is also true based on the proven fact that $a_m, a_{m+1}, a_{m+2} \ldots a_{m+k}$ are true (you may or may not need all of them to be true; **strong vs. weak induction**) (the induction step)
  - it implies that, once we have proven $a_m, a_{m+1}, a_{m+2} \ldots a_{m+k}, a_{m+k+1}$ are true, we can prove a_{m+k+2} is true
  - ……
  - generalize the index k to cover the entire domain (the conclusion step)

PROOF TECHNIQUES: MATHEMATICAL INDUCTION

- *Example: Prove that for every positive integer n, $11^n - 6$ is divisible by 5.*
  - *Proof: (basis step) We first show that when $n = 1$ (which is the very first index in the domain), $11^n - 6 = 11^1 - 6 = 5$, which is divisible by 5. (here we don't need multiple indexes as the basis, one is enough)*

  (induction step) We assume that for a positive integer $n \geq 1$, $11^n - 6$ is divisible by 5. To show that $11^{n+1} - 6$ is also divisible by 5, we have

  $$11^{n+1} - 6 = 11 * 11^n - 6 = 11 * (11^n - 6 + 6) - 6$$

  Since we $11^n - 6$ is divisible by 5, we assume that $11^n - 6 = 5x$ for some integer x. Therefore,

  $$11 * (11^n - 6 + 6) - 6 = 11 * (5x + 6) - 6 = 55x + 66 - 6 = 55x + 60 = 5 * (11x + 12)$$

  Since x is an integer, $11^{n+1} - 6$ is also divisible by 5. (Note that we have shown the case is true when $n = 1$, and we can plug in $n = 1$ to show the case is true when $n = 2$; we can then plug in $n = 2$ to show the case is true when $n = 3$……)

  (conclusion) Therefore, for every positive integer n, $11^n - 6$ is divisible by 5. (This is a must-have statement!)

PROOF TECHNIQUES: MATHEMATICAL INDUCTION

- *Example: Prove that for all integers $k \geq 8$, k cents can be obtained using 3-cent and 5-cent coins (use strong induction).*
  - *Proof: (basis step) We first show that when $k = 8$, we can make the change of 8 cents using one 3-cent and one 5-cent coin. We can also obtain when $k = 9$ using three 3-cent coins, and when $k = 10$ using two 5-cent coins. Therefore, the conclusion is true when $k = 8,9,10$. (We need all three cases as the basis; hence it is a strong induction.)*

  (induction step) We assume that for an integer $8 \leq x \leq k$ where $k \geq 10$, k cents can be obtained using 3-cent and 5-cent coins. Since $k - 2$ cents can be obtained using only 3-cent and 5-cent coins (because it is within the domain of our induction assumption), we can obtain $k + 1$ cents by adding one 3-cent coin.

  (conclusion) Therefore, for all integers $k \geq 8$, k cents can be obtained using 3-cent and 5-cent coins.

PROOF TECHNIQUES: COMMON ERRORS

- Some common mistakes found
  - the gold standard to judge whether a proof is correct is to ensure that all premises are true and the argument form is valid
  - here we provide some representative errors, but it is by no means exhaustive

PROOF TECHNIQUES: COMMON ERRORS

- Inverse errors: The inference "$p \to q, \neg p$, then $\neg q$" is wrong.
  - *Example: "If you have attended every class, you will receive an A for this course. Because you didn't attend every class, you will not get an A."*

- You can also show that the argument form is wrong using a truth table: we have a case where all premises are true but the conclusion is false.

p	q	$p \to q$	$\neg p$	$\neg q$
T	T	T	F	F
T	F	F	F	T
F	T	T	T	F
F	F	T	T	T

PROOF TECHNIQUES: COMMON ERRORS

- Converse error: The inference "$p \to q, q$, then p" is wrong.
  - *Example: "If you have attended every class, you will receive an A for this course; you received an A, so you must have attended every class."*

- We can also show that the argument form is wrong using a truth table: we have a case where all premises are true but the conclusion is false.

p	q	$p \to q$	q	p
T	T	T	T	T
T	F	F	F	T
F	T	T	T	F
F	F	T	F	F

PROOF TECHNIQUES: COMMON ERRORS

- Arguing from examples: Only showing examples that fail to cover the entire domain is wrong.
  - *Example: m = 2 and n = 6, which are both even, then m + n = 6, which is also even. m = 8 and n = 16, which are both even, then m + n = 24, which is also even. Therefore, the sum of two even integers must also be even.*
- We are trying to prove: $\forall m \in \{even\ integers\}, \forall n \in \{even\ integers\}: m + n \in \{even\ integers\}$
- This is a wrong argument form, because we have not exhausted all combinations of possible values of the respective domains of the variables. That is, we have not argue the cases where m and n take other even integers. (To prove this, consider using generalization of a generic particular.)
- Note that arguing from example would be correct if we are working on proving existential or disproving universal statements/conclusions.

PROOF TECHNIQUES: COMMON ERRORS

- Ambiguous premises: The truth value of a premise should be able to be determined unambiguously. *Example: "Women love shopping, Jane is a woman, so Jane loves shopping".*

- The error here is that the premise "*Women love shopping*" is ambiguous, as one can interpret it as "there exists some women who love shopping", "most (>50%) women love shopping", "all women love shopping". And based on the interpretation, the premise can be either true or false. As a result, there is no way we can unambiguously determine the truth value of the premise.

- This is where most controversies stem from. Students think they have made the point clear but we (the graders or I) do not. What is obvious in your mind does not mean it is obvious in our mind. So, take it serious and try to argue clearly and unambiguously.

PROOF TECHNIQUES: COMMON ERRORS

- Jumping into the conclusion: The premises and conclusion must be logically connected and consecutive.
  - *Example: "Suppose m and n are any even integers. By definition of even, $m = 2r$ and $n = 2s$ for some integers r and s. Then $m + n = 2r + 2s$. So $m + n$ is even."*
  - *The following premises should be included to make the argument complete "$2r + 2s = 2(r + s)$, since r and s are integers, $r + s$ must also be an integer; Therefore $2(r + s)$ is even and $m + n$ is also even".*

- This resembles eliminating a column from the truth table. We cannot verify the corresponding truth values and assert that the argument form is valid.
- Correct, complete, and concise are my favorites. But I do prefer wordy then incomplete in the exam!!!

PROOF TECHNIQUES: COMMON ERRORS

- Circular reasoning: Circular reasoning means assuming what is to be proved.
  - *Example: "Am I be making money from buying this stock?" "Oh yes, because the stock price will rise in the future, you can buy the stock now with a lower price and sell in 10 years later with a higher price. Then you make money!" The broker assumes that "the stock price will rise", which is equivalent to the customer's question "how to make money". So, the broker assumed what it is being asked or to be proved.*
  - *Note that sometimes circular reasoning are not easy to detect. For example "make money with buying stock" has the same meaning as "the stock price will rise in the future", but they are said in different ways.*

- If you use an unproven statement as a premise, then the premise is not necessarily true. Hence this is not a valid argument form.

SUMMARY

- Algorithms
- Elements of proof: statements
  - truth value of statements
  - compound statements
  - logical equivalence
- Argument
  - premises and conclusion
  - valid argument form

SUMMARY

- Common proof techniques:
  - direct proof
  - indirect proof
  - mathematical induction
- Common proof errors