Today's learning goals

• Distinguish between a theorem, an axiom, lemma, a corollary, and a conjecture.
• Recognize direct proofs
• Recognize proofs by contraposition
• Recognize proofs by contradiction
• Recognize fallacious “proofs”
• Evaluate which proof technique(s) is appropriate for a given proposition
  • Direct proof
  • Proofs by contraposition
  • Proofs by contradiction
  • Proof by cases
  • Constructive existence proofs
• Correctly prove statements using appropriate style conventions, guiding text, notation, and terminology

Textbook references: Sections 1.7-1.8 (with reference to 1.6)
"A proof is a valid argument that establishes the truth of a statement"
A proof is a valid argument that establishes the truth of a statement

Valid: truth of the conclusion (final statement) is guaranteed by the truth of the premises (preceding statements)

Argument: sequence of statements ending with a conclusion
For the sake of argument

Rosen p. 81

Axioms:
statements assumed to be true

Rules of inference + definitions

Theorem
Proposition
Fact
Result
Lemma
Corollary
What rules of inference are allowed?  

Rosen 1.6

Argument form is valid if no matter which propositions are substituted in, the conclusion is true if all the premises are true.
What about quantifiers?

Which of the following is not a valid argument?

A. All outdoor art on campus is intact after the storm. Therefore, the stone bear is intact after the storm.

B. The stone bear is intact after the storm. Therefore, all outdoor art on campus is intact after the storm.

C. The stone bear is intact after the storm. Therefore, some outdoor art on campus is intact after the storm.

D. The stone bear is intact after the storm. Therefore, not all outdoor art on campus was destroyed by the storm.

E. I don't understand the meaning of the concept "valid argument".
Fancy names

- Modus ponens
- Modus tollens
- Hypothetical syllogism ...
- Universal instantiation
- Universal generalization
- Existential instantiation
- Existential generalization

Rosen 1.6
Translating to proof strategy

- Modus ponens
- Direct proof

To prove that "If P, then Q"
- Assume P is true.
- Use rules of inference, axioms, definitions to...
- … conclude Q is true.
Translating to proof strategy

- Modus tollens

To prove that "If P, then Q"
- Assume Q is false.
- Use rules of inference, axioms, definitions to...
- ... conclude P is also false.

Both modus ponens and modus tollens apply when proving a conditional statement
What's the main logical connective in the following sentence?

\[ n^2 + 1 \geq 2^n \text{ when } n \text{ is a positive integer with } 1 \leq n \leq 4 \]

A. Conditional (p \rightarrow q)
B. Universal statement
C. Conjunction ("AND")
D. Inequality (\geq)
E. What's a "main logical connective"?
What's the main logical connective in the following sentence?

\[ n^2 + 1 \geq 2^n \text{ when } n \text{ is a positive integer} \]

A. Conditional (p \( \rightarrow \) q)
B. Universal statement
C. Conjunction ("AND")
D. Inequality (\(\geq\))
E. What's a "main logical connective"?
Main connective

Are these statements true?

I. \( n^2 + 1 \geq 2^n \) when \( n \) is a positive integer with \( 1 \leq n \leq 4 \)
II. \( n^2 + 1 \geq 2^n \) when \( n \) is a positive integer

A. Both are true.
B. Both are false.
C. I is true and II is false.
D. II is true and I is false.
E. I don't know how to evaluate the truth value of these sentences.
Universal conditionals

\[ n^2 + 1 \geq 2^n \] when \( n \) is a positive integer with \( 1 \leq n \leq 4 \)

\[ n^2 + 1 \geq 2^n \] when \( n \) is a positive integer

can be translated to

\[ \forall n \ (\ldots \rightarrow \ldots) \]
Universal conditionals

\[ \forall n \ (\ldots \rightarrow \ldots) \]

To prove this statement is **false**:

To prove this statement is **true**:
Universal conditionals

\( \forall n \ ( \ldots \rightarrow \ldots ) \)

To prove this statement is false:
Find a counterexample.

To prove this statement is true:
Select a general element of the domain, use rules of inference (e.g. direct proof, proof by contrapositive, etc.) to prove that the conditional statement is true of this element, conclude that it holds of all members of the domain.
Universal conditionals

Claim: \( n^2 + 1 \geq 2^n \) when \( n \) is a positive integer is false.

Proof:
Universal conditionals

Claim: $n^2 + 1 \geq 2^n$ when $n$ is a positive integer is false.

Proof: Since this is a universal conditional statement, to prove that it is false, it's enough to find one counterexample. That is, we need a specific value of $n$ which is a positive integer and for which

- A. $n^2 + 1 > 2^n$
- B. $n^2 + 1 < 2^n$
- C. $n^2 + 1 \leq 2^n$
- D. $n^2 + 1 \geq 2^n$
- E. What's a universal conditional?
Universal conditionals

Claim: \( n^2 + 1 \geq 2^n \) when \( n \) is a positive integer is false.

Proof: Since this is a universal conditional statement, it's enough to find one counterexample. That is, we need a specific value of \( n \) which is a positive integer and for which \( n^2 + 1 < 2^n \). Consider \( n = \)

A. \( n = 0 \)
B. \( n = 1 \)
C. \( n = 4 \)
D. \( n = 6 \)
E. None of the above
Universal conditionals

Claim: \( n^2 + 1 \geq 2^n \) when \( n \) is a positive integer is false.

Proof: Since this is a universal conditional statement, it's enough to find one counterexample. That is, we need a specific value of \( n \) which is a positive integer and for which \( n^2 + 1 < 2^n \). Consider \( n = 5 \). Then, for this example, the LHS of the inequality evaluates to \( 5^2 + 1 = 26 \) and the RHS evaluates to \( 2^5 = 32 \). Therefore, LHS < RHS, contradicting the statement. Thus, there is (at least) one counterexample to the universal statement and hence the universal statement is false.
Universal conditionals

Claim: $n^2 + 1 \geq 2^n$ when $n$ is a positive integer with $1 \leq n \leq 4$ is true.

Proof: WTS $\forall n (1 \leq n \leq 4 \rightarrow n^2 + 1 \geq 2^n)$

Let $n$ be a positive integer (a general element of the domain). For a direct proof, assume

A. $n \geq 1$
B. $n^2 + 1 \geq 2^n$
C. $n \leq 4$
D. $n^2 + 1 < 2^n$
E. None of the above
Universal conditionals

**Claim**: $n^2 + 1 \geq 2^n$ when $n$ is a positive integer with $1 \leq n \leq 4$ is true.

**Proof**: WTS $\forall n \ (1 \leq n \leq 4 \rightarrow n^2 + 1 \geq 2^n)$

Let $n$ be a positive integer (a general element of the domain). For a direct proof, assume that $1 \leq n \leq 4$.

**Goal**: WTS that $n^2 + 1 \geq 2^n$

*How can we use the hypothesis?*
Universal conditionals

Claim: $n^2 + 1 \geq 2^n$ when $n$ is a positive integer with $1 \leq n \leq 4$ is true.

Proof: WTS $\forall n \ (1 \leq n \leq 4 \rightarrow n^2 + 1 \geq 2^n)$

Let $n$ be a positive integer (a general element of the domain). For a direct proof, assume that $1 \leq n \leq 4$.

Goal: WTS that $n^2 + 1 \geq 2^n$

Since we assume that $n$ is an integer between 1 and 4, there are only four possible cases. We check that the conclusion is true in each one.
Universal conditionals

Claim: $n^2 + 1 \geq 2^n$ when $n$ is a positive integer with $1 \leq n \leq 4$ is true.

Proof: WTS \ $\forall n \ (1 \leq n \leq 4 \rightarrow n^2 + 1 \geq 2^n)$

Let $n$ be a positive integer (a general element of the domain). For a direct proof, assume that $1 \leq n \leq 4$.

Goal: WTS that $n^2 + 1 \geq 2^n$

Case 1: Assume $n=1$. Then LHS is $1^2+1 = 2$; RHS is $2^1=2$ so LHS $\geq$ RHS. 😊

Case 2: Assume $n=2$. Then LHS is $2^2+1 = 5$; RHS is $2^2=4$ so LHS $\geq$ RHS. 😊

Case 3: Assume $n=3$. Then LHS is $3^2+1 = 10$; RHS is $2^3=8$ so LHS $\geq$ RHS. 😊

Case 4: Assume $n=4$. Then LHS is $4^2+1 = 17$; RHS is $2^4=16$ so LHS $\geq$ RHS. 😊
Universal conditionals

Claim: \( n^2 + 1 \geq 2^n \) when \( n \) is a positive integer. This statement is true.

Proof: WTS \( \forall n \ (1 \leq n \leq 4) \)
Let \( n \) be a positive integer (a general element of the domain). For a direct proof, assume that \( 1 \leq n \leq 4 \).

Goal: WTS that \( n^2 + 1 \geq 2^n \)

Case 1: Assume \( n=1 \). Then LHS is \( 1^2+1 = 2 \); RHS is \( 2^1=2 \) so LHS \( \geq \)RHS.

Case 2: Assume \( n=2 \). Then LHS is \( 2^2+1 = 5 \); RHS is \( 2^2=4 \) so LHS \( \geq \)RHS.

Case 3: Assume \( n=3 \). Then LHS is \( 3^2+1 = 10 \); RHS is \( 2^3=8 \) so LHS \( \geq \)RHS.

Case 4: Assume \( n=4 \). Then LHS is \( 4^2+1 = 17 \); RHS is \( 2^4=16 \) so LHS \( \geq \)RHS.

Exhaustive proof (cf. page 93)
Reminder: perfect squares

An integer \( a \) is a **perfect square** if there is some integer \( b \) such that

\[
a = b^2
\]

Which of the following is **not** a perfect square?

A. 0  
B. 1  
C. 2  
D. 4  
E. More than one of the above
An integer $a$ is a **perfect square** if there is some integer $b$ such that

$$a = b^2$$

Which of the following is **not** true?

A. If $n$ is a perfect square, so is $n^2$.
B. If $n^2$ is a perfect square, so is $n$.
C. If $n^2$ is not a perfect square, neither is $n$.
D. $n^2$ is a perfect square.
E. More than one of the above
Reminder: perfect squares

Theorem: For integers $k>1$, then $2^k-1$ is not a perfect square.

Proof:

What would we assume in a direct proof?
A. $k > 1$
B. $k \leq 1$
C. $2^k-1$ is not a perfect square
D. $2^k-1$ is a perfect square
E. More than one of the above
Reminder: perfect squares

Theorem: For integers $k > 1$, then $2^k - 1$ is not a perfect square.

Proof:

What would we assume in a proof by contraposition?
A. $k > 1$
B. $k \leq 1$
C. $2^k - 1$ is not a perfect square
D. $2^k - 1$ is a perfect square
E. More than one of the above
Reminder: perfect squares

Theorem: For integers $k > 1$, then $2^k - 1$ is not a perfect square.

Proof: ???
Proof by contradiction

Idea: To prove $P$, instead, we prove that the conditional

$$(\neg P) \rightarrow F$$

is true. But, the only way for a conditional to be true if its conclusion is false is for its hypothesis to be false too.

Conclude: $(\neg P)$ is false, i.e. $P$ is true!
Theorem: For integers $k > 1$, then $2^k - 1$ is not a perfect square.

Proof:

What would we assume in a proof by contradiction?
A. $k > 1$
B. $k \leq 1$
C. $2^k - 1$ is not a perfect square
D. $2^k - 1$ is a perfect square
E. More than one of the above
Theorem: For integers $k>1$, then $2^k-1$ is not a perfect square.

Proof: Let $k$ be an integer. Assume that
\begin{itemize}
  \item $k > 1$ and that
  \item $2^k-1$ is a perfect square.
\end{itemize}

Goal: look for a contradiction that is now guaranteed.

Keep going …
Overall strategy

• Do you believe the statement?
  • Try some small examples.
• Determine logical structure + main connective.
• Determine relevant definitions.
• Map out possible proof strategies.
  • For each strategy: what can we assume, what is the goal?
  • Start with simplest, move to more complicated if/when get stuck.
Next up

- Using proofs in the context of sets
Reminder: divisibility

For integers $a, b$ with $a$ nonzero

$$\exists c (b = ac)$$

means

$$a \mid b$$

$$\frac{b}{a} \in \mathbb{Z}$$

"$a$ divides $b$"  "$b$ is an integer multiple of $a$"