# Proof Techniques

CSE2315, Chapter 2-1

# Proof Techniques

- Informal proof methods :
  - Inductive reasoning
  - Deductive reasoning
  - Proof by exhaustion
  - Direct proof
  - Proof by contraposition
  - Proof by contradiction
  - Serendipity
- A few terms for proof:
  - Axioms: Statements that are assumed true.
    - Example: Given two distinct points, there is exactly one line that contains them.
  - Theorem: A proposition that has been proved to be true.
    - Two special kinds of theorems: Lemma and Corollary.
    - Lemma: A theorem that is usually not too interesting in its own right but is useful in proving another theorem.
    - Corollary: A theorem that follows quickly from another theorem.

# Deductive Reasoning: Counter Example

- Inductive Reasoning: Drawing a conclusion from a hypothesis based on experience. Hence the more cases you find where Q follows from P, the more confident you are about the conjecture P $\rightarrow$ Q.
- Usually, deductive reasoning is also applied to the same conjecture to ensure that it is indeed valid.
- Deductive reasoning looks for a counter example that disproves the conjecture, i.e. a case when P is true but Q is false.
- Example: Prove that "For every positive integer $n$, $n! \leq n^2$."
  - Start testing some cases say, $n$ = 1, 2, 3 etc.
  - It might seem like it is true for some cases but how far do you test, say $n$ = 4.
  - We get $n!$ = 24 and $n^2$ = 16 which is a counter example for this theorem. Hence, even finding a single case that doesn't satisfy the condition is enough to disprove the theorem.

# Counter Example

- More examples of counterexample:
  - All animals living in the ocean are fish.
  - Every integer less than 10 is bigger than 5.

- Counter example is not trivial for all cases, so we have to use other proof methods.

# Exhaustive Proof

- If dealing with a finite domain in which the proof is to be shown to be valid, then using the exhaustive proof technique, one can go over all the possible cases for each member of the finite domain.
- Final result of this exercise: you prove or disprove the theorem but you could be definitely exhausted.
- Example: For any positive integer less than or equal to 5, the square of the integer is less than or equal to the sum of 10 and 5 times the integer.

| $n$ | $n^2$ | $10+5n$ | $n^2 \leq 10+5n$ |
|---|---|---|---|
| 1 | 1 | 15 | yes |
| 2 | 4 | 20 | yes |
| 3 | 9 | 25 | yes |
| 4 | 16 | 30 | yes |
| 5 | 25 | 35 | yes |

# Example: Exhaustive Proof

- If an integer between 1 and 20 is divisible by 6, then it is also divisible by 3.

TABLE 2.1

| Number | Divisible by 6 | Divisible by 3 |
|---|---|---|
| 1 | no | |
| 2 | no | |
| 3 | no | |
| 4 | no | |
| 5 | no | |
| 6 | yes: $6 = 1 \times 6$ | yes: $6 = 2 \times 3$ |
| 7 | no | |
| 8 | no | |
| 9 | no | |
| 10 | no | |
| 11 | no | |
| 12 | yes: $12 = 2 \times 6$ | yes: $12 = 4 \times 3$ |
| 13 | no | |
| 14 | no | |
| 15 | no | |
| 16 | no | |
| 17 | no | |
| 18 | yes: $18 = 3 \times 6$ | yes: $18 = 6 \times 3$ |
| 19 | no | |
| 20 | no | |

# Direct Proof

- **Direct Proof:**
- Used when exhaustive proof doesn't work. Using the rules of propositional and predicate logic, prove P $\rightarrow$ Q.
- Assume the hypothesis P and then try to prove Q. Hence, a formal proof would require a proof sequence to go from P to Q.
- Consider the conjecture

  $x$ is an even integer $\Lambda$ y is an even integer $\rightarrow$ the product $xy$ is an even integer.

# Direct Proof Example

- A complete formal proof sequence might look like the following:

| | | |
|---|---|---|
| 1. | $x$ is an even integer $\wedge$ $y$ is an even integer | hyp |
| 2. | $(\forall x)[x$ is even integer $\rightarrow(\exists k)(k$ is an integer $\wedge\ x = 2k)]$ (definition of even integer) | number fact |
| 3. | $x$ is an even integer $\rightarrow(\exists k)(k$ is an integer $\wedge\ x = 2k)$ | 2,ui |
| 4. | $y$ is an even integer $\rightarrow(\exists k)(k$ is an integer $\wedge\ y = 2k)$ | 2,ui |
| 5. | $x$ is an even integer | 1,sim |
| 6. | $(\exists k)(k$ is an integer $\wedge\ x = 2k)$ | 3,5,mp |
| 7. | $m$ is an integer $\wedge\ x = 2m$ | 6, ei |
| 8. | $y$ is an even integer | 1,sim |
| 9. | $(\exists k)(k$ is an integer $\wedge\ y = 2k)$ | 4,8,mp |
| 10. | $n$ is an integer and $y = 2n$ | 9, ei |

# Direct Proof Example (contd.)

11. $x = 2m$ — 7,sim
12. $y = 2n$ — 10, sim
13. $xy = (2m)(2n)$ — 11, 12, substitution of equals
14. $xy = 2(2mn)$ — 13, multiplication fact
15. $m$ is an integer — 7,sim
16. $n$ is an integer — 10, sim
17. $2mn$ is an integer — 15, 16, number fact
18. $2mn$ is an integer $\wedge$ $xy = 2(2mn)$ — 17, 14, con
19. $(\exists k)(k$ is an integer $\wedge$ $xy = 2k)$ — 18,eg
20. $(\forall x)[(\exists k)(k$ is an integer $\wedge$ $x = 2k) \rightarrow x$ is even integer] — number fact (definition of even integer)
21. $(\exists k)(k$ an integer $\wedge$ $xy = 2k) \rightarrow xy$ is even integer — 20, ui
22. $xy$ is an even integer — 19, 21, mp

# Direct Proof: Contraposition

- If you tried to prove but failed to produce a direct proof of your conjecture $P \rightarrow Q$
- You can use a variant of direct proof, contraposition
- $Q' \rightarrow P'$ is the contrapositive of $P \rightarrow Q$
- Example 1: Prove that "If the square of an integer is odd, then the integer must be odd."
  - P: $n^2$ is odd, Q: $n$ is odd
  - Conjecture: $P \rightarrow Q$
  - Try to prove, $Q' \rightarrow P'$
  - $Q'$ : $n$ is even, $P'$ : $n^2$ is even
  - Since $n$ is even, $n^2 = n \times n$ is even
    ($n=2k$, $n^2=4k^2=2(2k^2)$)

# Direct Proof: Contraposition

- Example 2: Prove that "If $n$+1 separate passwords are issued to $n$ students, then some student gets ≥ 2 passwords."
  - The contrapositive is:
    - If every student gets < 2 passwords, then $n$+1 separate passwords were NOT issued."
  - Suppose every student has < 2 passwords
  - Then, every one of the $n$ students has at most 1 password.
  - The total number of passwords issued is at most $n$, not $n$+1.

# Indirect Proof: Proof by Contradiction

- When we try to prove, $P \rightarrow Q$
- Think about the truth table for $(P \wedge Q' \rightarrow 0) \rightarrow (P \rightarrow Q)$
- It is a tautology
- To prove $P \rightarrow Q$, it is sufficient to prove $P \wedge Q' \rightarrow 0$
- In a proof by contradiction, you assume that the hypothesis and the negation of the conclusion are true and then try to deduce some contradiction from these assumptions.
- Example 1: Prove that "If a number added to itself gives itself, then the number is $0$."
  - The hypothesis (P) is $x + x = x$ and the conclusion (Q) is $x = 0$. Hence, the hypotheses for the proof by contradiction are:
  - $x + x = x$ and $x \neq 0$ (P and Q')
  - Then $2x = x$ and $x \neq 0$,
    hence dividing both sides by $x$,
    the result is $2 = 1$,
    which is a contradiction.
    Hence, $(x + x = x) \rightarrow (x = 0)$, which means we proved $P \rightarrow Q$.

# Indirect Proof: Proof by Contradiction

- Example 2: Prove "For all real numbers $x$ and $y$, if $x + y \geq 2$, then either $x \geq 1$ or $y \geq 1$."
  - P: $x + y \geq 2$ Q: $x \geq 1$ or $y \geq 1$ and try to show $P \wedge Q' \rightarrow 0$
  - Proof: Say the conclusion is false, i.e. $x < 1$ and $y < 1$. (Q')
  - Adding the two conditions, the result is $x + y < 2$.
  - At this point, this condition is P′ if P = $x + y \geq 2$, hence, P Λ P′ which is a contradiction. Hence, the statement above is true.
- Example 3: The sum of even integers is even.
  - Proof: Let $x = 2m$, $y = 2n$ for integers $m$ and $n$ and assume that $x + y$ is odd.
  - Then $x + y = 2m + 2n = 2k + 1$ for some integer $k$.
  - Hence, $2*(m + n - k) = 1$, where $m + n - k$ is some integer.
  - This is a contradiction since 1 is not even.

# Class Exercise

- Prove that √5 is not a rational number.
- What kind of proof method and How?
- Definition of rational number: a number that can be represented as a form of b/a (a,b, integers, a≠0, and a and b have no common factors other than ±1)

# Serendipity

- Serendipity: Fortuitous happening or something by chance or good luck.
- Not a formal proof technique.
- Interesting proofs provided by this method although other methods can be used as well.
- Example: 342 players in a tennis tournament. One winner in the end. Each match is between two players with exactly one winner and the loser gets eliminated.

# Summarizing Proof Techniques

| Proof Technique | Approach to prove $P \rightarrow Q$ | Remarks |
|---|---|---|
| Exhaustive Proof | Demonstrate $P \rightarrow Q$ for all cases | May only be used for finite number of cases |
| Direct Proof | Assume P, deduce Q | The standard approach- usually the thing to try |
| Proof by Contraposition | Assume $Q'$, derive $P'$ | Use this $Q'$ if as a hypothesis seems to give more ammunition then P would |
| Proof by Contradiction | Assume $P \wedge Q'$ , deduce a contradiction | Use this when Q says something is not true |
| Serendipity | Not really a proof technique | Fun to know |

# Further Study

1. Product of any 2 consecutive integers is even.
2. The sum of 3 consecutive integers is even.
3. Product of 3 consecutive integers is even.
4. The square of an odd integer equals $8k+1$ for some integer $k$.
5. The sum of two rational numbers is rational.
6. For some positive integer $x$, $x + 1/x \geq 2$.