CS 2336
Discrete Mathematics

Lecture 4

Proofs: Methods and Strategies

Outline

- What is a Proof ?
- Methods of Proving
- Common Mistakes in Proofs
- Strategies : How to Find a Proof ?

What is a Proof ?

- A proof is a valid argument that establishes the truth of a theorem (as the conclusion)
- Statements in a proof can include the axioms (something assumed to be true), the premises, and previously proved theorems
- Rules of inference, and definitions of terms, are used to draw intermediate conclusions from the other statements, tying the steps of a proof
- Final step is usually the conclusion of theorem

Related Terms

- Lemma : a theorem that is not very important
  - We sometimes prove a theorem by a series of lemmas
- Corollary : a theorem that can be easily established from a theorem that has been proved
- Conjecture : a statement proposed to be a true statement, usually based on partial evidence, or intuition of an expert

Methods of Proving

- A direct proof of a conditional statement

  $$p \to q$$

  first assumes that p is true, and uses axioms, definitions, previously proved theorems, with rules of inference, to show that q is also true

- The above targets to show that the case where p is true and q is false never occurs
  - Thus, $p \to q$ is always true

Direct Proof (Example 1)

- Show that

  if n is an odd integer, then n^2 is odd.

- Proof :

  Assume that n is an odd integer. This implies that there is some integer k such that

$$n = 2k + 1.$$

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

Thus, n^2 is odd.

Direct Proof (Example 2)

- Show that

  if m and n are both square numbers,

  then m n is also a square number.

- Proof :

  Assume that m and n are both squares. This implies that there are integers u and v such that

  $$m = u^2 \quad \text{and} \quad n = v^2.$$

  Then $m\,n = u^2 v^2 = (uv)^2$. Thus, m n is a square.

Methods of Proving

- The proof by contraposition method makes use of the equivalence

$$p \rightarrow q \equiv \neg q \rightarrow \neg p$$

- To show that the conditional statement $p \rightarrow q$ is true, we first assume $\neg q$ is true, and use axioms, definitions, proved theorems, with rules of inference, to show $\neg p$ is also true

Proof by Contraposition (Example 1)

- Show that

  if $3n + 2$ is an odd integer, then n is odd.

- Proof :

  Assume that n is even. This implies that

  $$n = 2k \text{ for some integer } k.$$

  Then, $3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1)$, so that $3n + 2$ is even. Since the negation of conclusion implies the negation of hypothesis, the original conditional statement is true

Proof by Contraposition (Example 2)

- Show that

  if $n = ab$, where a and b are positive,

  then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

- Proof :

  Assume that both a and b are larger than $\sqrt{n}$. Thus, $ab > n$ so that $n \neq ab$. Since the negation of conclusion implies the negation of hypothesis, the original conditional statement is true

Methods of Proving

- The proof by contradiction method makes use of the equivalence

$$p \equiv \neg p \rightarrow F_0$$

where F_0 is any contradiction

- One way to show that the latter is as follows: First assume $\neg p$ is true, and then show that for some proposition r, r is true and $\neg r$ is true

- That is, we show $\neg p \rightarrow (r \wedge \neg r)$ is true

Proof by Contradiction (Example 1)

- Show that

  if $3n + 2$ is an odd integer, then n is odd.

- Proof :

  Assume that the statement is false. Then we have $3n + 2$ is odd, and n is even.

  The latter implies that $n = 2k$ for some integer k, so that $3n + 2 = 3(2k) + 2 = 2(3k + 1)$.

  Thus, $3n + 2$ is even. A contradiction occurs (where ?), so the original statement is true

Proof by Contradiction (Example 2)

- Show that

  $\sqrt{2}$ is irrational.

- Proof :

  Assume on the contrary that it is rational.

  Then it can be expressed as a / b, for some positive integers a and b with $b \neq 0$.

  Further, we may restrict a and b to have no common factor.

Proof by Contradiction (Example 2)

- Proof (continued):

  It follows that $a^2 = 2b^2$ so that a is even.

  Then $a = 2c$ for some integer c, so that

  $$(2c)^2 = 2b^2 .$$

  It follows that $b^2 = 2c^2$ so that b is even.

  A contradiction occurs (where ?), so that the original statement is true.

Methods of Proving

- The proof by cases method makes use of the equivalence

$$(p_1 \vee p_2 \vee \dots \vee p_k) \rightarrow q$$
$$\equiv (p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \dots \wedge (p_k \rightarrow q)$$

- Sometimes, to prove $p \rightarrow q$ is true, it may be easy to use an equivalent disjunction $p_1 \vee p_2 \vee \dots \vee p_k$ instead of p as the hypothesis

Proof by Cases (Example)

- Show that

  if an integer n is not divisible by 3,

  then $n^2 = 3k + 1$ for some integer k.

- Proof :

  "n is not divisible by 3" is equivalent to

  "$n = 3m + 1$ for some integer m" or

  "$n = 3m + 2$ for some integer m".

Proof by Cases (Example)

- Proof (continued):

If it is the first case :

$$n^2 = (3m + 1)^2 = 9m^2 + 6m + 1$$

$$= 3(3m^2 + 2m) + 1 = 3k + 1 \text{ for some } k.$$

If it is the second case :

$$n^2 = (3m + 2)^2 = 9m^2 + 12m + 4$$

$$= 3(3m^2 + 4m + 1) + 1 = 3k + 1 \text{ for some } k.$$

We obtain the desired conclusion in both cases, so the original statement is true.

Methods of Proving

- When proving bi-conditional statement, we may make use of the equivalence

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

- In general, when proving several propositions are equivalent, we can use the equivalence

$$p_1 \leftrightarrow p_2 \leftrightarrow \ldots \leftrightarrow p_k$$
$$\equiv (p_1 \rightarrow p_2) \land (p_2 \rightarrow p_3) \land \ldots \land (p_k \rightarrow p_1)$$

Proofs of Equivalence (Example)

- Show that the following statements about the integer n are equivalent :

  $p :=$ "n is even"

  $q :=$ "$n - 1$ is odd"

  $r :=$ "n^2 is even"

- To do so, we can show the three propositions

  $$p \rightarrow q, \quad q \rightarrow r, \quad r \rightarrow p$$

  are all true. Can you do so ?

Methods of Proving

- A proof of the proposition of the form $\exists x$ P(x) is called an existence proof
- Sometimes, we can find an element s, called a witness, such that P(s) is true

  This type of existence proof is constructive
- Sometimes, we may have non-constructive existence proof, where we do not find the witness

Existence Proof (Examples)

- Show that there is a positive integer that can be written as the sum of cubes of positive integers in two different ways.
- Proof: $1729 = 1^3 + 12^3 = 9^3 + 10^3$

- Show that there are irrational numbers r and s such that r^s is rational.
- Hint: Consider $(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}}$

Common Mistakes in Proofs

- Show that $1 = 2$.
- Proof : Let a be a positive integer, and $b = a$.

Step	**Reason**
1. $a = b$	Given
2. $a^2 = a\,b$	Multiply by a in (1)
3. $a^2 - b^2 = a\,b - b^2$	Subtract by b^2 in (2)
4. $(a - b)(a + b) = b(a - b)$	Factor in (3)
5. $a + b = b$	Divide by $(a - b)$ in (4)
6. $2b = b$	By (1) and (5)
7. $2 = 1$	Divide by b in (6)

Common Mistakes in Proofs

- Show that

  if n^2 is an even integer, then n is even.

- Proof :

  Suppose that n^2 is even.

  Then $n^2 = 2k$ for some integer k.

  Let $n = 2m$ for some integer m.

  Thus, n is even.

Common Mistakes in Proofs

- Show that

  if x is real number, then x^2 is positive.
- Proof : There are two cases.

  Case 1: x is positive

  Case 2: x is negative

  In Case 1, x^2 is positive.

  In Case 2, x^2 is also positive

  Thus, we obtain the same conclusion in all cases, so that the original statement is true.

Proof Strategies

- Adapting Existing Proof
- Show that

  $\sqrt{3}$ is irrational.

- Instead of searching for a proof from nowhere, we may recall some similar theorem, and see if we can slightly modify (adapt) its proof to obtain what we want

Proof Strategies

- Sometimes, it may be difficult to prove a statement q directly
- Instead, we may find a statement p with the property that p $\rightarrow$ q, and then prove p

  Note: If this can be done, by Modus Ponens, q is true
- This strategy is called backward reasoning

Backward Reasoning (Example)

- Show that for distinct positive real numbers x and y,

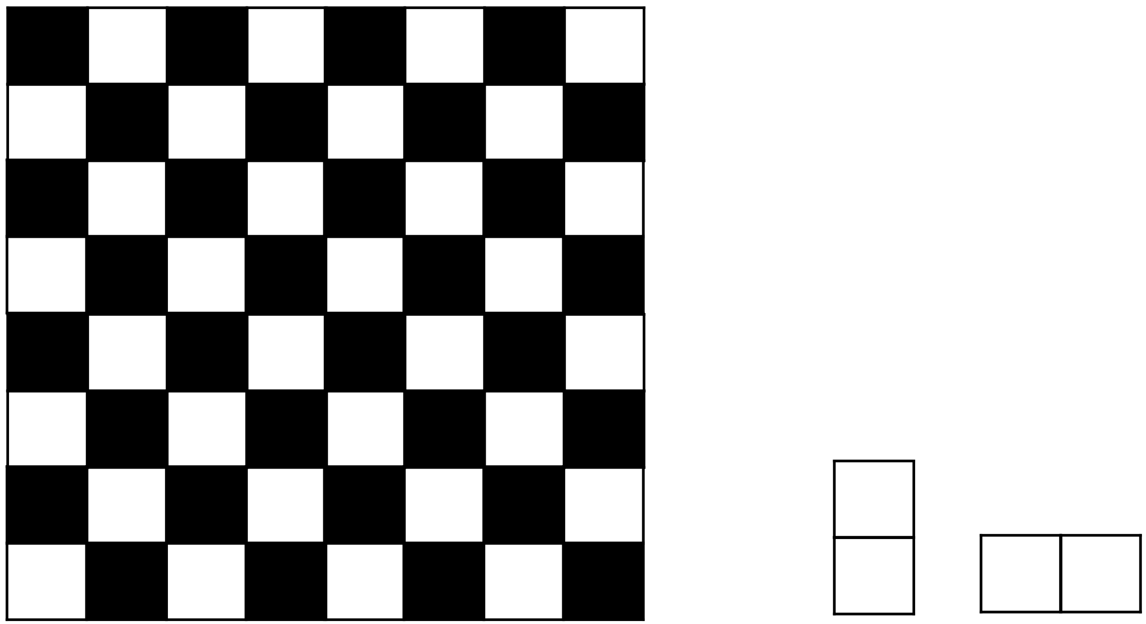
$$0.5\,(x + y) > (x\,y)^{0.5}$$

- Proof: By backward reasoning strategy, we find that

1. $0.25\,(x + y)^2 > x\,y \rightarrow 0.5\,(x + y) > (x\,y)^{0.5}$
2. $(x + y)^2 > 4\,x\,y \rightarrow 0.25\,(x + y)^2 > x\,y$
3. $x^2 + 2\,x\,y + y^2 > 4\,x\,y \rightarrow (x + y)^2 > 4\,x\,y$
4. $x^2 - 2\,x\,y + y^2 > 0 \rightarrow x^2 + 2\,x\,y + y^2 > 4\,x\,y$
5. $(x - y)^2 > 0 \rightarrow x^2 - 2\,x\,y + y^2 > 0$
6. $(x - y)^2 > 0$ is true, since x and y are distinct.

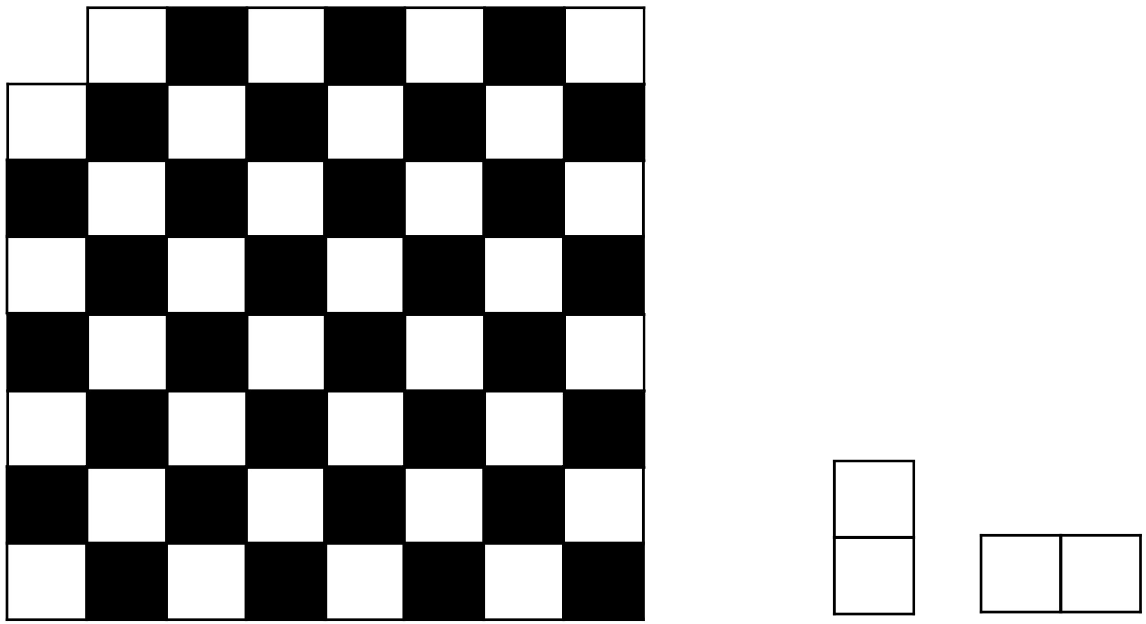
Thus, the original statement is true.

Interesting Examples



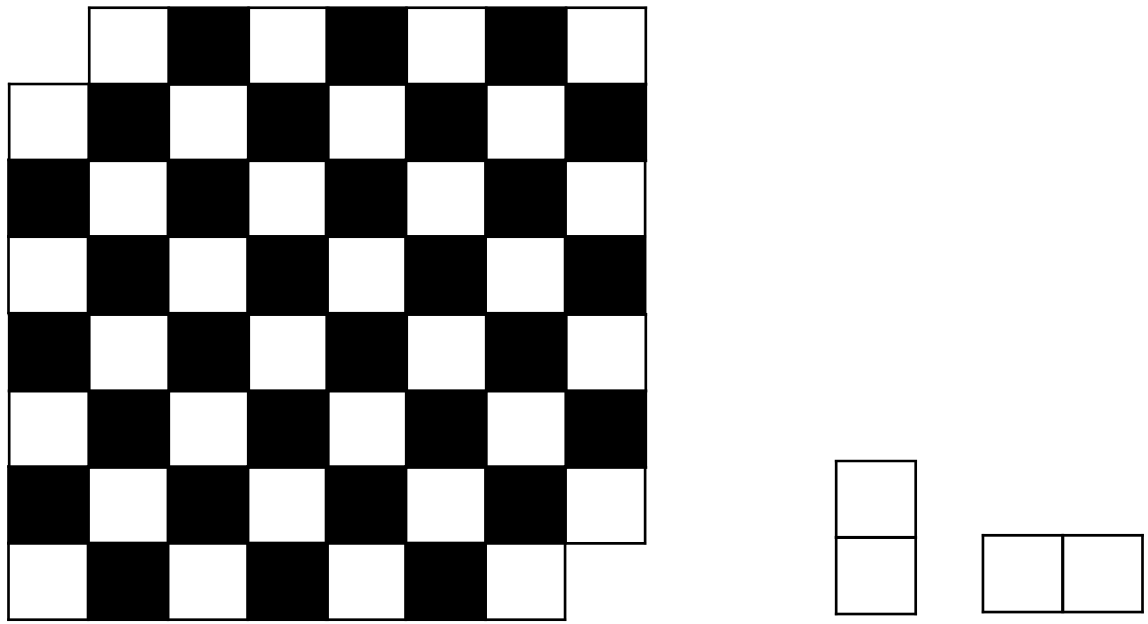
Can a checkerboard be tiled by 1×2 dominoes?

Interesting Examples



What if the top left corner is removed ?

Interesting Examples



What if the lower right corner is also removed ?