CSCE 222

Discrete Structures for Computing

Proofs

Dr. Hyunyoung Lee

Based on slides by Andreas Klappenecker

What is a Proof?

A proof is a sequence of statements, each of which is either assumed, or follows from preceding statements by a rule of inference.

We already learned many rules of inference (and essentially all of them are common sense rules).

Use Plain English!

In predicate logic, we already learned how to do formal proofs. In mathematical arguments, we essentially use the same method. However, formal proofs are not very appealing to humans (the intended readership of our proofs), so we should try to formulate our proofs in plain English!

Example

Instead of writing an implication in the form

p -> q

we will write

If p, then q.

For instance:

If 2x=5, then x=5/2.

Styles of Proofs

We have essentially three basic styles of proof:

- Direct proof

- Proof by contradiction

- Proof by induction

In addition, we have some variations of these basic styles of proofs.

Direct Proof (1)

Definition: An integer n is called even if and only if there exists an integer k such that n=2k.

An integer n is called odd if and only if there exists an integer k such that n=2k+1.

Theorem: If n is an odd integer, then n^2 is an odd integer.

How can we prove it?

Direct Proof (2)

Theorem: If n is an odd integer, then n^2 is an odd integer.

Proof: Since n is an odd integer, there exists an integer k such that n=2k+1.

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

Thus, by definition of an odd integer, we can conclude that n^2 is an odd integer (as it is one more than twice the integer $2k^2+2k$).

Contrapositive

The contrapositive of an implication p -> q is given by ¬q -> ¬p. We have (p -> q) ≡ (¬q -> ¬p).

p	q	p->q	¬q	¬p	¬q-> ¬p
F	F	T	T	T	T
F	T	T	F	T	T
T	F	F	T	F	F
T	T	T	F	F	T

Proof by Contrapositive

In a proof of contraposition of p->q, one assumes ¬q and shows that ¬p must follow.

This is of course a variation on the direct proof.

Proof by Contrapositive

Theorem: For all integers n, if n^2 is even then n is even.

We prove the contrapositive.

Suppose that n is not even, that is, n is odd. Then n = 2k + 1 for some integer k. So $n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$ which is odd.Thus we have proved: if n is not even, then n^2 is not even.

So by the contrapositive, we can conclude that if n^2 is even, then n is even.

Proof by Contradiction (1)

Theorem: For all integers n, if n^2 is even then n is even.

Seeking a contradiction, assume that the theorem is false. That is, assume that for some integers n, n^2 is even but n is not even, that is, n is odd. Then n = 2k + 1 for some integer k. So

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1,$$

which is odd. Contradiction.

Therefore, the theorem holds true.

Prime Numbers

A prime number is a natural number p>=2 whose only positive divisors are 1 and p.

A natural number m >= 2 that is not prime is called composite.

Examples of prime numbers: 2, 3, 5, 7, 11, ...

Fundamental Theorem of Arithmetic

Theorem: Every natural number m >=2 can be factored into a product of primes

$$m = p_1 p_2 \ldots p_n$$

in exactly one way.

Proof by Contradiction (2)

Theorem. There are infinitely many prime numbers.

Proof. Seeking a contradiction, suppose that there are only finitely many prime numbers, say $p_1 < p_2 < \ldots < p_n$. Consider the number $q = p_1 p_2 \ldots p_n + 1$. Now, q is either prime or it is not. If it is a prime, it is not contained in the set $\{p_1, p_2 \ldots, p_n\}$. If it is not a prime, it is divisible by some prime p, and p cannot be any of $p_1, p_2 \ldots, p_n$ otherwise p would divide 1.

Thus, the number q is divisible by a prime not contained in the set $\{p_1, p_2 \ldots, p_n\}$, which proves the theorem.

Proof by Induction

Suppose we wish to prove a certain assertion concerning positive integers.

Let A(n) be the assertion concerning the integer n.

To prove it for all natural numbers n>=1, we can do the following:

Basis: Prove that the assertion A(1) is true.

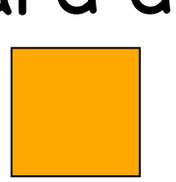
Inductive Step: For all n, show that A(n) implies A(n+1).

We can conclude that A(n) is true for all n>=1.

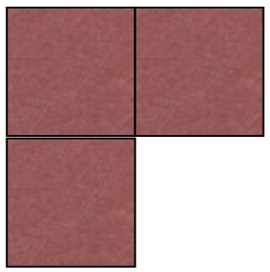
A Tiling Problem

We want to consider tiling problems.

Consider a chessboard of side length $2^n \times 2^n$.

We call the chessboard defective if and only if it has precisely one square  missing.

We want to cover the nondefective part with triominos, where turning the triominos is allowed.

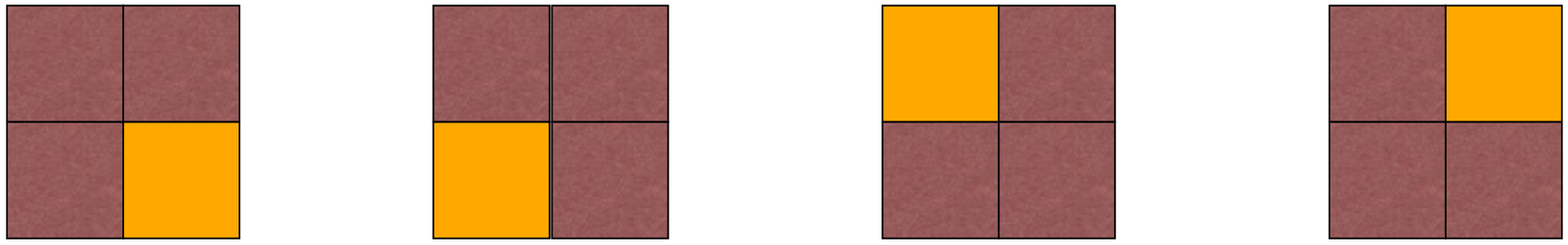


Triomino Tiling

Theorem: Any defective 2^n x 2^n chessboard can be covered by triominos.

Proof by Mathematical Induction

Basis: n = 1



Induction step: