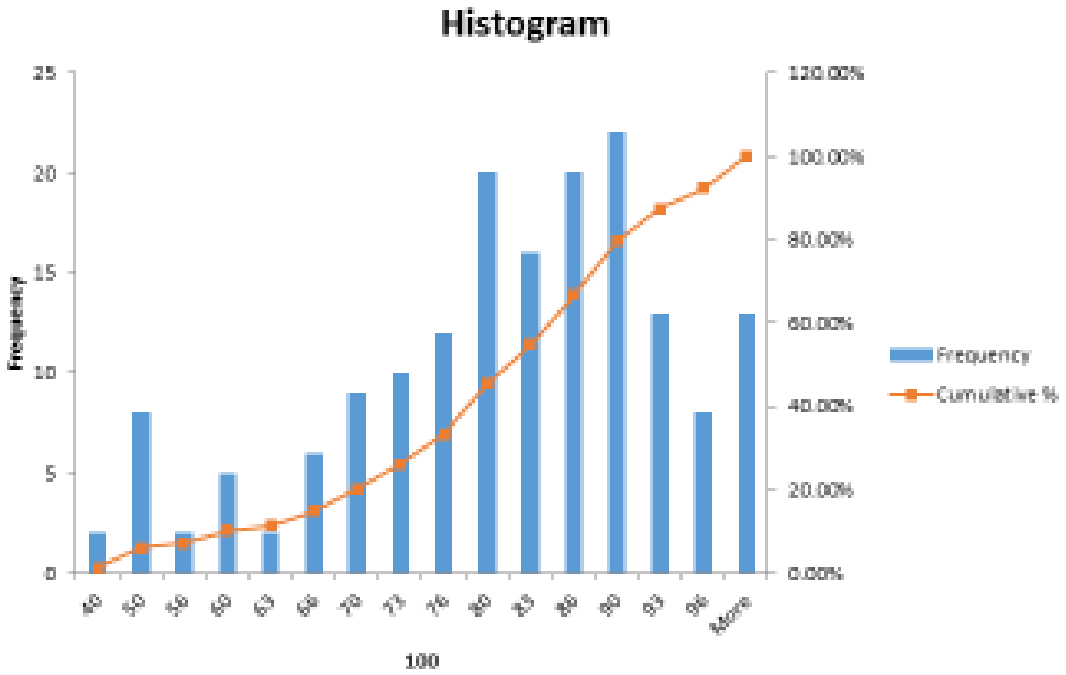
Proof by Contradiction

Discrete Structures (CS 173)

Gul Agha

Based on slides by Derek Hoiem, University of Illinois

Grades to Exam 4 (52.5%)



Final Exam

- Date and Time posted by Registrar: Thursday December 16 7-10pm. No room assignment yet.
- Accounts for 15% of total grade in grading schedule
- Will be 1 hour 45 minutes long
- Will cover last 2 weeks of class (topics not covered by Examlet 6) *but as usual will assume knowledge of topics previously covered.*

About conflict exams for final

- Look for posted conflict exams. These are from courses with combined exams. CS 173 is not a combined exam--it doesn't have a posted conflict exam.
- Two exams at the same time?
  - *The course with the combined exam handles it*.
  - If there's more than one non-combined exam, the largest such course handles it.
  - Really large combined exams often have an unposted "conflict conflict" time already set up, that you'll only find out about after you report a conflict to their course staff.
- Three exams in a row? The largest course handles it.
- Conflicts must be reported to instructors by the last day of classes. Earlier is better.
  - If you aren't 100% sure which course is handling it, notify all the instructors involved, so we can help make sure you end up with a solution.
- More details are on the student code exams page

- Last class
  - Analysis of running time of code
  - P vs. NP: Problems in NP can be verified in polynomial time. Problems in P can also be solved in polynomial time. $P \subseteq NP$
  - We *don't know* if *NP* problems necessarily require exponential time. (That would imply $P \neq NP$)

This class

- Proof by contradiction
- When to use different types of proofs

Proof by Contradiction

- Sometimes you want to show that something is impossible
  - $\sqrt{2}$ cannot be written as a ratio of integers
  - There is no compression algorithm that reduces the size of all files
  - A cycle with an odd number of nodes can't be colored with two colors
- Difficult to prove non-existence directly, and can't prove by example
- Solution: show that the negation of the claim leads to a contradiction

Basic form of proof by contradiction

1. We need to show proposition p
2. Suppose, instead, that p is false.
3. Then, we can see that both q and $\neg q$ follow, which is a contradiction.
4. Therefore, p must be true.

Why proof by contradiction works

1. We need to prove proposition p
2. Instead, we show $\neg p \rightarrow F$, i.e., that we can conclude a contradiction from not p
3. By contrapositive, $\neg p \rightarrow F \equiv T \rightarrow p \equiv p$

Another explanation

We need to prove proposition $p = T$

Instead, we show $\neg p \rightarrow F$, i.e., that we can conclude a contradiction from $\neg p$

But $\neg p \rightarrow F$ means that $\neg p = F$, so $p = T$

Contradiction

A set of propositions is a **contradiction** if their conjunction is always false

Contradiction?

1. $p \wedge \neg p$
2. $p \vee \neg p$
3. $(x > 5) \wedge (x > 21)$
4. $x = 20$ and x is odd
5. $(x > 5) \wedge (x < 21)$
6. $(x < 5) \wedge (x > 21)$
7. x is negative number and $\sqrt{x}$ is real

Example 1: Non-Divisibility

Let x and y be integers.

Claim: If p is even and q is odd, then p does not divide q

$$p \text{ is even } \wedge q \text{ is odd } \Rightarrow p \nmid q$$

Proof: Assume that the claim is false. Then the premise is true but the conclusion is false.

Consider some $p|q$. Then $q = pk$ for some integer k. Now p is even, so $p = 2n$, for some n. Thus $q = 2nk$. This means q is even which means the premise (q is odd) cannot be true thus contradicting the statement that the claim is false.

Example 2: Non-Divisibility

Claim: If n is an integer, then $n^2 + 2$ is not divisible by 4

Proof. Assume statement is false.

Then there is some integer k, $4|(k^2+2)$,

i.e. $k^2 + 2 = 4j$ for some j

Case 1: k is even. Let $k = 2m$. Now $(2m)^2+2 = 4j$

i.e, $4m^2 + 2 = 4j$

or $2j = 2m^2 + 1$

Case 2: k is odd. Let $k = 2m + 1$. Now $(2m + 1)^2+2 = 4j$

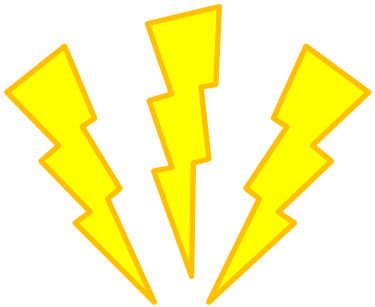
i.e., $4m^2 + 4m + 3 = 4j$

…

Example 4: Infinitely many primes

Claim: There are infinitely many prime numbers

Equivalent claim: The set of prime numbers is not finite.



Danger of proof by contradiction: a mistake in the proof might also lead to a contradiction

See this blog post about P=NP problem

http://rjlipton.wordpress.com/2011/01/08/proofs-by-contradiction-and-other-dangers/

Proof by contradiction

Claim: $\sqrt{2}$ is irrational

Equivalent claim: There does not exist a pair of integers p, q without common factors such that $p/q = \sqrt{2}$

Example 5: Well-foundedness and Infinite Descending Chains

Proposition. The set S with partial order $<$ has no infinite descending chains if and only if every nonempty subset of S has a minimal element.

Recall $x \in S$ is a minimal element of S, if $\forall y \in S, y \not< x$

An infinite descending chain of elements of S is a sequence consisting of (some) elements $a_1, a_2, \ldots, a_n, \ldots$ such that $a_{i+1} < a_i$

(Example negative integers $-1, -2, -3, \ldots$ under the < relation).

Proof: **if:** Suppose some nonempty subset of S has no minimal element (call it B) but there are no infinite descending chains of elements in S. Pick an element $x_1 \in B$. There must be an element $x_2 \in B, x_2 < x_1$ (otherwise x_1 would be minimal). The argument can be repeated continuously to construct an infinite descending change. Contradiction.

Only if: Suppose every nonempty set $A \subseteq S$ has a minimal element but there is an infinite descending chain consisting of (a subset of) elements of S. Call the set of elements in the infinite descending chain B. B has no minimal element thus contradicting the assumption.

Minimal Counterexample

- A free variable in a conditional statement is interpreted as the statement being true for all values of the variable.
- To prove the statement:
  - we assume the statement doesn't hold for some value of the free variables.
  - We show that such a value doesn't exist.
- In case the variables are numbers, sometimes we can find a minimal value for which the statement is false.

Example 3: Divisibility by Primes

Claim: Every integer greater than 1 is divisible by a prime

Proof: Assume the statement is false. Then some integer n is not divisible by a prime.

Since a prime number divides itself, n must not be prime.

Since n is not prime, there exists a p, such that $1 < p < n$ and $p|n$. This implies there is a smallest divisor of n (why?).

Let d is the smallest divisor of n. Now d cannot be prime (otherwise, n would be divisible by a prime),

so there exists $k > 1$ such that $k|d$.

Since $k|d$ and $d|n$, it follows that $k|n$. This contradicts the fact that d is the smallest divisor of n.

Loss-less Compression

A *file compression* reduces the size of the file. A *lossless compression* allows the original file to be reconstructed exactly.

A lossless compression algorithm must perform a lossless compression on every input file.

What can be said about the function lossless compression computes?

Example 6: No Lossless Compression Algorithm

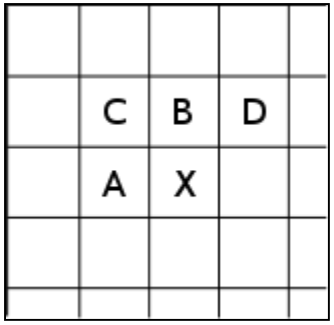
Claim: A lossless compression algorithm that makes some files smaller must make some (other) files larger.

Proof: Suppose the claim is false.

Why image compression works: images are mostly smooth

Lossless compression (PNG)

1. Predict a pixel's value based on its upper-left neighborhood
2. Store difference of predicted and actual value
3. Pkzip it (DEFLATE algorithm)



Sarah's certain death riddle (stretch time)

https://www.youtube.com/watch?v=2dgmgub8mHw

One door leads to castle, other to certain death

D2: One of us always lies, and one of us always tells the truth. D1 always lies.

D1: I do not. I tell the truth.

S to D1: Would D2 tell me that door 1 leads to the castle?

D1: Yes.

Questions:

1) Which one is the liar?
2) Which door leads to the castle?

Proof by contradiction

Claim: A cycle graph with an odd number of nodes is not 2-colorable.

Proof by contradiction or contrapositive

Claim: For all integers n, if n^2 is odd, then n is odd.

When to use each type of proof

Match the situation to the proof type

Situation

1. Can see how conclusion directly follows from hypothesis
2. Need to demonstrate claim for an unbounded set of integers
3. Easier to show that negation of hypothesis follows from negation of conclusion
4. Need to show that something doesn't exist
5. Need to show that something exists

Proof type

a) Direct proof

b) Proof by example or counter-example

c) Proof by contrapositive (or logical equivalence)

d) Induction

e) Proof by contradiction

When to use each type of proof

Match the situation to the proof type

Situation

1. Can see how conclusion directly follows from hypothesis (a)
2. Need to demonstrate claim for an unbounded set of integers (d)
3. Easier to show that negation of hypothesis follows from negation of conclusion (c)
4. Need to show that something doesn't exist (e)
5. Need to show that something exists (b)

Proof type

a) Direct proof

b) Proof by example or counter-example

c) Proof by contrapositive (or logical equivalence)

d) Induction

e) Proof by contradiction

When to use each type of proof

Match the claim to the suitable proof type

Claim

1. There is no real x, such that $x^2 < 0$.
2. If n^2 is odd, then n is odd.
3. There is an integer x, such that $x^2 = 0$.
4. If n is odd, then n^2 is odd.
5. All trees have more nodes than edges.
6. A wheel graph can't be colored with two colors.
7. Not every natural number is a square.
8. The sum of two rational numbers is rational.
9. An even number can't be created from the product of odd numbers.

Proof type

a) Direct proof

b) Proof by example or counter-example

c) Proof by contrapositive (or logical equivalence)

d) Induction

e) Proof by contradiction

Next class

- Collections of sets
  - Sets of sets
  - Powersets
  - Partitions