A Proof Primer

Class 2

Administrative

- video on
- "Hello" in chat tool
- preferred first name and last name in zoom profile

- questions about anything in Monday's material?
- questions about the assignment due tomorrow?

Submission

- you can re-submit as many times as you wish
- until the due date and time

- if you submit after it's due
  1. I may not see it unless you let me know
  2. it may get a late penalty

1.1 A Proof Primer

- introduces some terminology
- introduces four "informal" proof techniques
  - exhaustive checking
  - direct proof of implication
  - indirect proof by contrapositive
  - indirect proof by contradiction

Truth Tables

- much of this course is about Boolean algebra
- a Boolean expression has exactly one of two possible values, usually denoted true and false
- simple declarative English statements are Boolean statements: it is raining

- the values of a Boolean expression can be tabulated with a truth table

- a truth table is table that lists all possible values for a set of Boolean variables (inputs)
- and a set of the corresponding values of Boolean expressions (outputs)

Boolean Operations

- there are a number of operations that exist in Boolean algebra
- some of the most important are:
  - unary negation (not)
  - binary conjunction (and)
  - binary disjunction (or)
  - binary implication (if-then, also called the conditional)

Not's Truth Table

- consider the declaration "it is raining"
- we normally represent statements with upper-case math letters:

$$A = \text{it is raining}$$

- the negation of this statement is "not A" or $\neg A$: "it is not raining"
- we can use a truth table to show the possible input values of A
- along with the corresponding output values of $\neg A$

A	$\neg A$
T	F
F	T

Binary Operator Truth Tables

- let A be a declaration (e.g., "it is raining")
- let B be a declaration (e.g., "my name is Xerxes")
- we use a truth table to show the possible input values of A and B
- along with the corresponding output values of A and B, A or B, and A implies B

A	B	$A \wedge B$	$A \vee B$	$A \rightarrow B$
T	T	T	T	T
T	F	F	T	F
F	T	F	T	T
F	F	F	F	T

Proof by Exhaustive Checking

- the simplest proof technique
- typically used for Boolean expressions
- small, finite number of cases

example: prove $\neg(A \wedge B)$ is equivalent to $(\neg A) \vee (\neg B)$

			3			6
A	B	$A \wedge B$	$\neg(A \wedge B)$	$\neg A$	$\neg B$	$\neg A \vee \neg B$
T	T	T	F	F	F	F
T	F	F	T	F	T	T
F	T	F	T	T	F	T
F	F	F	T	T	T	T

since columns 3 and 6 are identical, their expressions are equivalent

Proof by Exhaustive Checking Example 2

- prove $A \rightarrow B$ is equivalent to $\neg A \vee B$

Proof by Exhaustive Checking Example 2

- prove $A \rightarrow B$ is equivalent to $\neg A \vee B$

		2		4
A	B	$A \rightarrow B$	$\neg A$	$\neg A \vee B$
T	T	T	F	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

since columns 2 and 4 are identical, their expressions are equivalent

Exhaustive Checking

- exhaustive checking is often used for Boolean expressions because the number of possible cases is relatively small
- sometimes for integer problems we can also use exhaustive checking

example: prove that for n between 2 and 7 inclusive, $n^2 + 2$ is not divisible by 4

- we set up a table similar to a truth table:

n	$n^2 + 2$	$4 \mid n^2 + 2$
2	6	F
3	11	F
4	18	F
5	27	F
6	38	F
7	51	F

- by exhaustively checking all possibilities, the proof is demonstrated

Exhaustive Checking

example: prove that for n between 2 and 500 inclusive, $n^2 + 2$ is not divisible by 4

- manually building a table for this is possible but quite tedious
- instead we write a program to do the exhaustive checking for us

```
1  int main()
2  {
3    bool proved = true;
4    unsigned n = 2;
5    while (proved && n <= 500)
6    {
7      if ((n * n + 2) % 4 == 0)
8      {
9        proved = false;
10     }
11     else
12     {
13       n++;
14     }
15   }
16   if (proved)
17   {
18     cout << "Proved by exhaustive checking" << endl;
19   }
20   else
21   {
22     cout << "Disproved by counterexample n = " << n << endl;
23   }
24   return 0;
25 }
```

Exhaustive Checking

- prove that for all non-negative integers n, $n^2 + 2$ is not divisible by 4
- this cannot be done by exhaustive checking because there are infinitely many non-negative integers

- if there are infinitely many input values, exhaustive checking can sometimes disprove an assertion by finding even a single counterexample
- but exhaustive checking can never be used to prove an assertion when there are infinitely many input values

Contrapositive

- if A then B is implication
- if $\neg B$ then $\neg A$ is the implication's contrapositive
- let's examine the truth table

		2			5
A	B	$A \to B$	$\neg B$	$\neg A$	$\neg B \to \neg A$
T	T	T	F	F	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	T	T	T

since columns 2 and 5 are identical, an implication and its contrapositive are equivalent

- we can prove an implication by proving its contrapositive
- this is called indirect proof by contrapositive
- or, simply proof by contrapositive

Proof by Contrapositive

- to prove an implication, we assume the antecedent is true
- and then see if that leads us to the consequent

- sometimes this is straightforward
- but sometimes it's not

- the contrapositive of an implication is also an implication
- again, assume the antecedent, reason to the consequent
- if we prove the contrapositive implication, then we have also proved the original implication indirectly

- sometimes this is easier than proving the original implication directly

Proof by Contradiction

- a contradiction is a statement that is false
- proof by contradiction has the following steps:
  1. assume the original statement to be proved is false
  2. use direct proof techniques to show the assumption leads to a contradiction
  3. conclude that the original statement must not have been false, so it is proved true

Proof by Contradiction Example

- prove that the square root of 2 is irrational

Step 1 assume the square root of 2 is rational, i.e., $\sqrt{2} = \frac{a}{b}$ where $\frac{a}{b}$ is in lowest terms.

Step 2 at least one of a or b is odd; if they were both even, $\frac{a}{b}$ is not in lowest terms
since $\frac{a}{b} = \sqrt{2}$, square both sides and rearrange to get $a^2 = 2b^2$
therefore a^2 must be even, and since the square of an odd number is also odd, then a must be even
since a is even, then b must be odd
however, if a is even, then a^2 must be a multiple of 4
since $a^2 = 2b^2$, then $2b^2$ must also be a multiple of 4, and so b^2 must be even, which means that b must be even

Step 3 since b must be both odd and even, which is impossible, we have reached a contradiction; therefore the original statement is proved true