csci54 – discrete math & functional programming
proofs: example, counterexample, direct, contrapositive

discrete math so far

- sets
- introductions to propositional and predicate logic
- reflections on what it means to prove something

- this week:
  - proof techniques
  - group meeting Thursday/Friday
  - problem set due this Sunday
    - can discuss ideas, but must not look at anyone else's written up solution (in latex, on a whiteboard, etc)

Negating nested quantifiers

- Consider the following statement:

$$\forall i \in \{1, 2, \ldots, n\} : [\exists j \in \{1, 2, \ldots, n\} : (i \neq j) \wedge (A[i] = A[j])]$$

- Simplify the negation:

$$\neg \; \forall i \in \{1, 2, \ldots, n\} : [\exists j \in \{1, 2, \ldots, n\} : (i \neq j) \wedge (A[i] = A[j])]$$

Example from csci101

Theorem: If L is a context-free language, then:

$$\exists k \geq 1\ (\forall \text{ strings } w \in L, \text{ where } |w| \geq k\ (\exists u, v, x, y, z\ \ (w = uvxyz,$$
$$vy \neq \varepsilon,$$
$$|vxy| \leq k, \text{ and}$$
$$\forall q \geq 0\ (uv^q xy^q z \text{ is in } L)))).$$

"Automata, Computability and Complexity", Elaine

$$\forall x \in S : [P(x) \lor \neg P(x)]$$

$$\neg[\forall x \in S : P(x)] \Leftrightarrow [\exists x \in S : \neg P(x)]$$ De Morgan's Laws (quantified form)

$$\neg[\exists x \in S : P(x)] \Leftrightarrow [\forall x \in S : \neg P(x)]$$

$$[\forall x \in S : P(x)] \Rightarrow [\exists x \in S : P(x)]$$ *if the set S is nonempty*

$$\forall x \in \varnothing : P(x)$$ Vacuous quantification

$$\neg\exists x \in \varnothing : P(x)$$

$$[\exists x \in S : P(x) \lor Q(x)] \quad \Leftrightarrow \quad [\exists x \in S : P(x)] \lor [\exists x \in S : Q(x)]$$

$$[\forall x \in S : P(x) \land Q(x)] \quad \Leftrightarrow \quad [\forall x \in S : P(x)] \land [\forall x \in S : Q(x)]$$

$$[\exists x \in S : P(x) \land Q(x)] \quad \Rightarrow \quad [\exists x \in S : P(x)] \land [\exists x \in S : Q(x)]$$

$$[\forall x \in S : P(x) \lor Q(x)] \quad \Leftarrow \quad [\forall x \in S : P(x)] \lor [\forall x \in S : Q(x)]$$

$$[\forall x \in S : P(x) \Rightarrow Q(x)] \land [\forall x \in S : P(x)] \Rightarrow [\forall x \in S : Q(x)]$$

$$[\forall x \in \{y \in S : P(y)\} : Q(x)] \quad \Leftrightarrow \quad [\forall x \in S : P(x) \Rightarrow Q(x)]$$

$$[\exists x \in \{y \in S : P(y)\} : Q(x)] \quad \Leftrightarrow \quad [\exists x \in S : P(x) \land Q(x)]$$

from Figure 3.21 in CDMCS

On proofs

- A proof of a proposition is a convincing argument that the proposition is true.

- Assumes that you are trying to convince a particular audience
  - For this class assume you are writing for a classmate

some definitions

- an integer k is even if and only if there exists an integer r such that $k=2r$
- an integer k is odd if and only if there exists an integer r such that $k=2r+1$
- $k|m$ if and only if there exists an integer r such that $m=kr$. This is equivalent to saying that "m mod k = 0" or that "k evenly divides m".
- an integer $k>1$ is prime if the only positive integers that evenly divide k are 1 and k itself.
- an integer $k>1$ is composite if it is not prime.
- an integer k is a perfect square if and only if there exists an integer r such that $k=r^2$

proof techniques (by giving an example)

- proof by construction / proof by example:
  - given a claim that there exists x such that P(x) is true, can prove by constructing such an x

there exists a prime number larger than 20

- disproof by counterexample:
  - given a claim that some P(x) is true for all x, can disprove by showing there exists an element y where P(y) is not true.

for all positive integers n, $2n=n^2$

practice

- Claim: no positive integer is expressible in two different ways as the sum of two perfect squares.
  - Reminder: an integer k is a <u>perfect square</u> if and only if there exists an integer r such that $k=r^2$

proof techniques

- direct proof:
  - start with known facts. repeatedly infer additional new facts until can conclude what you want to show.
  - may divide work into cases
- proof of the contrapositive
  - if trying to prove an implication, prove the contrapositive instead
- proof by contradiction
  - if trying to prove a statement, assume the statement is not true and prove something that is clearly false. From this conclude that the original statement must be true.

proof techniques

- direct proof:
  - start with known facts. repeatedly infer additional new facts until can conclude what you want to show.
  - may divide work into cases

- proof of the contrapositive:
  - if trying to prove an implication, prove the contrapositive instead

- proof by contradiction
  - if trying to prove a statement, assume the statement is not true and prove something that is clearly false. From this conclude that the original statement must be true.

direct proof + cases : example

- claim: let n be any integer. Then $n(n+1)^2$ is e

state the proof technique (unless it's a direct proof)

- proof: The proof is by cases. Given an integer n, n is either even or odd.
  - If n is even, then $n=2r$ for some integer r. Then $n(n+1)^2 = 2r(2r+1)^2 = 2(r(2r+1)^2)$, which is even.
  - If n is odd, then $n=2r+1$ for some integer r. Then $n(n+1)^2 = (2r+1)(2r+2)^2 = (2r+1)(2r+2)(2r+2) = 2((2r+1)(r+1)(2r+2))$, which is even.
  - Since $n(n+1)^2$ is even regardless of whether n is eve or odd, $n(n+1)^2$ is even for all integers n.

break up the proof visually

conclude by stating what you've shown

direct proof : example

- claim: the binary representation of any odd integer ends with a 1.

representing numbers in different bases

- In base10 (decimal), every number is written as a sum of powers of 10.
  - For example, 205 = $2*10^2 + 0*10^1 + 5*10^0$
  - More generally, in base 10:

… …

- In base2 (binary), every number is written a a sum of powers of 2.
  - For example, 101 = $1*2^2 + 0*2^1 + 1*2^0$
  - More generally, in base 2:

… …

practice with decimal and binary

write in decimal

1. 1
2. 10
3. 100
4. 1011
5. 1100
6. 10101

write in binary

1. 3
2. 8
3. 10
4. 22
5. 37
6. 47

direct proof : example

- claim: If a number is odd, then its binary representation ends with a 1.

- proof:
  - Let k be an arbitrary odd integer.
  - Then there exists an integer r such that k=2r+1.
  - Now let $d_n \ldots d_2 d_1 d_0$ be the binary representation of r.
  - The binary representation of 2r is then $d_n \ldots d_2 d_1 d_0 0$, and
  - The binary representation of $k=2r+1= d_n \ldots d_2 d_1 d_0 1$.

- conclusion: Therefore the binary representation of any odd integer ends with a 1.

proof techniques

- direct proof:
  - start with known facts. repeatedly infer additional new facts until can conclude what you want to show.
  - may divide work into cases

- proof of the contrapositive:
  - if trying to prove an implication, prove the contrapositive instead

- proof by contradiction
  - if trying to prove a statement, assume the statement is not true and prove something that is clearly false. From this conclude that the original statement must be true.

proof of the contrapositive : example

- claim: If a number is odd, then its binary representation ends with a 1.

- proof: The claim states that if an integer k is odd, then its binary representation ends with a 1. We prove the contrapositive: if the binary representation of a number k ends with a 0 then k is even.

- Let k be an integer whose binary representation ends with a 0. Let $d_n \ldots d_3 d_2 d_1 0$ be the binary representation of k. Since the digits in a binary number represent powers of 2, this means

$$
\begin{aligned}
k &= d_n \cdot 2^n + d_{n-1} \cdot 2^{n-1} + \ldots + d_2 \cdot 2^2 + d_1 \cdot 2^1 + 0 \cdot 2^0 \\
&= 2(d_n \cdot 2^{n-1} + d_{n-1} \cdot 2^{n-2} + \ldots d_2 \cdot 2^1 + d_1)
\end{aligned}
$$

- Therefore k is even.
- We have proven the contrapositive and, therefore, the binary representation of any odd integer ends with a 1.

if and only if: example

- prove the following claim by proving each direction separately. Use a direct proof in one direction and a proof of the contrapositive in the other.

- claim: let n be any integer. Then n is even if and only if n^2 is even.