Proofs

And why not to reason backwards

CS 2800: Discrete Structures, Spring 2015

Sid Chaudhuri
Thought for the Day #1

Identify all the logical flaws in this “proof”

http://youtu.be/X2xlQaimsGg
Faulty Logic

• How do you known she is a witch?
• She looks like one!

Beware of results that “look right”!
A picture is **not** a proof
Logical Implication

- “$x$ is a witch” $\Rightarrow$ “$x$ looks like a witch”
- This does **not** mean “$x$ looks like a witch” $\Rightarrow$ “$x$ is a witch”

- Circumstantial evidence is not proof!
- Circumstantial evidence is not proof!!
- **Circumstantial evidence is not proof!!!**
Logical Implication

• Another example:
  – “It's sunny” ⇒ “I will go for a run”

• This does not mean
  – “I will go for a run” ⇒ “It's sunny”
    (i.e. if I'm out running, then it must be sunny)
  – I might also go for a run on a cloudy day!

• However, it is true that
  – If I'm not out running, it cannot be sunny
Logical Implication

- More generally, if $P \implies Q$
  - It need not be the case that $Q \implies P$
  - However, it is always the case that $\neg Q \implies \neg P$

If there's one thing you take away from this course, let this be it
Outline of a correct proof

- We need to prove statement $S$
- Start with a statement $S_0$ known to be true
- Show that it logically implies $S_1$
- Show that $S_1$ logically implies $S_2$
- ... and so on until you end up implying $S$
- The proof looks like

$$S_0 \Rightarrow S_1 \Rightarrow S_2 \Rightarrow \ldots \Rightarrow S_n \Rightarrow S$$

Note the direction of the chain of implications!
Beware of reasoning backwards!

- This is **not** a proof of statement $S$

  $$S \Rightarrow S_n \Rightarrow \ldots \Rightarrow S_2 \Rightarrow S_1 \Rightarrow S_0$$

- A very common error in this course!
- We *will* treat backwards proofs as incorrect
A backwards proof

• Prove that \( a + b = a \), whenever \( a = b \neq 0 \)

• “Proof”:

\[
\begin{align*}
   a + b &= a \\
   (a + b)(a - b) &= a(a - b) \\
   a^2 - b^2 &= a^2 - ab \\
   b^2 &= ab \\
   b &= a \quad (\text{dividing by } b \neq 0)
\end{align*}
\]

... which is true (given), hence “proved”
What went wrong?

we need implications in this direction

... but that doesn't work (division by zero going from second line to first)

\[
\begin{align*}
  a + b &= a \\
  \iff (a + b)(a - b) &= a(a - b) \\
  \iff a^2 - b^2 &= a^2 - ab \\
  \iff b^2 &= ab \\
  \iff b &= a
\end{align*}
\]
A backwards proof of a true result

- If $x$ and $y$ are positive real numbers, then 
  \[
  \frac{x + y}{2} \geq \sqrt{xy}
  \]
- “Proof”:
  \[
  \frac{x + y}{2} \geq \sqrt{xy} \\
  \frac{(x + y)^2}{4} \geq xy \\
  x^2 + 2xy + y^2 \geq 4xy \\
  x^2 - 2xy + y^2 \geq 0 \\
  (x - y)^2 \geq 0
  \]
  ... which is true, hence “proved”

If the direction of implications is not specified, the proof is assumed to be “forward”

This proves that
- if \((x + y)/2 > \sqrt{xy}\),
- then \((x - y)^2 > 0\),
not the other way round

You may lose points for writing the proof exactly like this
A correct proof

- If $x$ and $y$ are positive real numbers, then $(x + y)/2 \geq \sqrt{xy}$

**Proof:**

\[(x - y)^2 \geq 0 \quad \text{(square of a real number is } \geq 0)\]

\[\Rightarrow x^2 - 2xy + y^2 \geq 0\]

\[\Rightarrow x^2 + 2xy + y^2 \geq 4xy\]

\[\Rightarrow (x + y)^2/4 \geq xy\]

\[\Rightarrow (x + y)/2 \geq \sqrt{xy}\]

Hence proved
It's ok to figure out the proof “backwards” (often easier, else you're searching for that “magic” place to start), as long as your final chain of reasoning works “forwards”!
Thought for the Day #2

If the statement $S$ to be proved is actually true, can I really construct a chain that works backwards (from $S$) but not forwards (to $S$)?
Yes!

- Prove that \( a + b \geq a - b \) for \( a \geq b > 0 \)

- "Proof":
  \[
  a + b \geq a - b
  \]
  \[
  (a + b)(a - b) \geq (a - b)(a - b) \quad (a - b \geq 0)
  \]
  \[
  a^2 - b^2 \geq a^2 - 2ab + b^2
  \]
  \[
  -2b^2 \geq -2ab
  \]
  \[
  b \leq a \quad (\text{dividing by } -2b < 0)
  \]
  ... which is true (given)

- Division by zero when \( a = b \), going in the direction we actually want (upwards)
Life Lesson #0

Avoid backwards proofs. Always write out the direction of implications using ⇒ ("implies"), ⇐ ("is implied by") and ⇔ ("if and only if") symbols, and ensure they point the right way.
It's not just for math and CS...
It's not just for math and CS...
Observation

- A man is discovered lying dead in his country house with a kitchen knife stuck in his side
Hypothesis

The Butler Did It
Proposed Proof

- Let's assume the butler did it!
Proposed Proof

- Let's assume the butler did it!
- He needed to get the weapon, and have a motive
Proposed Proof

- Let's assume the butler did it!
- He needed to get the weapon, and have a motive
- The cook didn't see a kitchen knife missing during day, so the butler must have obtained it at night
Proposed Proof (cont'd)

• (Let's assume the butler did it!)
Proposed Proof (contd)

● (Let's assume the butler did it!)

● The parlormaid, who was sneaking back into the house after a liaison with the gardener, saw the butler walking towards the kitchen at 2am.
Proposed Proof (contd)

• (Let's assume the butler did it!)

• The parlormaid, who was sneaking back into the house after a liaison with the gardener, saw the butler walking towards the kitchen at 2am

• The chauffeur testified the late master overruled the butler's preference to serve red wine instead of white. The butler took it as a mortal insult.
Does this prove the butler did it?

- No, the proof is backwards
- It shows that if the butler did it, then two things would be highly probable
  - He would go towards the kitchen at night
  - He would have a motive
- But it does not show that the observations conclusively incriminate the butler
- He could have been going to the restroom, and someone else could have had a stronger motive!
Remember

- A solid understanding of logical implications can save innocent lives
- We will revisit this topic in the context of conditional probability
  - Instead of “if $A$, then definitely $B$” ($A \Rightarrow B$)
  - … we have “if $A$, then probably $B$” ($P(B \mid A) = …$)