CSC165H, Mathematical expression and reasoning for computer science
week 7

6th July 2005

Gary Baumgartner and Danny Heap
heap@cs.toronto.edu
SF4306A
416-978-5899
http://www.cs.toronto.edu/~heap/165/S2005/index.shtml

Proof structure

Today we'll discuss various flavours of proof, and how to present them in our structured proof format. After lecture I'll post Gary Baumgartner's notes summarizing proof structure on the web page as a reference.

Multiple quantifier example

Suppose we have a mystery function f and the following statement (I have added parentheses to indicate the conventional parsing)

$$\forall e \in \mathbf{R},\ e > 0 \Rightarrow (\exists d \in \mathbf{R}, d > 0 \wedge (\forall x \in \mathbf{R},\ 0 < |x-a| < d \Rightarrow (|f(x) - l| < e)))$$

If we want to prove this TRUE, structure the proof as follows:[1]

If we want to prove the statement FALSE, we first negate it, and then use one of our proof formats (I use the equivalences $\neg(p \Rightarrow q) \Leftrightarrow (p \wedge \neg q)$ and $\neg(p \wedge q) \Leftrightarrow (p \Rightarrow \neg q)$):

$$\exists e \in \mathbf{R},\ e > 0 \wedge \forall d \in \mathbf{R},\ d > 0 \Rightarrow \exists x \in \mathbf{R},\ 0 < |x-a| < d \wedge |f(x) - l| \geq e$$

Of course, this negation involved several applications of rules we already know, and now its proof may be written step-by-step. In the middle of that proof we had a "$\wedge$" to prove.

Proving $\wedge$

The $\wedge$ subproof has the following form:

So, $d_e > 0$

Let $x \in \mathbf{R}$

$\vdots$

Since x is an arbitrary real number, $\forall x \in \mathbf{R}, 0 < |x-a| < d \Rightarrow |f(x) - l| < e$.

So $d_e > 0 \wedge \forall x \in \mathbf{R}, 0 < |x-a| < d \Rightarrow |f(x) - l| < e$...

We rolled the conclusion into the statement beginning “Therefore, $\exists d$...” The general form to prove $A \wedge B$ is:

> $\vdots$
>
> Then A.
>
> $\vdots$
>
> Then B.
>
> Thus $A \wedge B$.

Don’t let variables introduced while proving A “bleed” over into the proof of B. This tells us how to prove a bi-implication, since it is just a conjunction of implications. To prove $A \Leftrightarrow B$, start from its definition:

> Then $(A \Rightarrow B) \wedge (B \Rightarrow A)$.
>
> Thus $A \Leftrightarrow B$.

Non-boolean function example

Last time we discussed how non-boolean functions cannot take the place of predicates (which are analogous to boolean functions) in a proof. How should they be used? Define $\lfloor x \rfloor : \mathbf{R} \rightarrow \mathbf{R}$ by:

> $\lfloor x \rfloor$ is the largest integer $\leq x$.

Now we can form the statement:

Claim 1: $\forall x \in \mathbf{R}$, $\lfloor x \rfloor < x + 1$

It makes sense to apply $\lfloor x \rfloor$ to elements of our domain, or variables that we have introduced, and to evaluate it in predicates such as “$<$” but $\lfloor x \rfloor$ it self is not a variable, a sentence, nor a predicate. We can’t (sensibly) say $\forall \lfloor x \rfloor \in \mathbf{R}$ or $\forall x \in \mathbf{R}$, $\lfloor x \rfloor \vee \lfloor x+1 \rfloor$. The structure of Claim 1 is a direct proof of a universally-quantified predicate:[2]

> Since x is an arbitrary element of $\mathbf{R}$, $\forall x \in \mathbf{R}$, $\lfloor x \rfloor < x + 1$

Of course, we need to fill in the “meat” of the “$\vdots$”[3]

In some cases you need to break down a statement such as “y is the largest integer $\leq x$”:

$$y \in \mathbf{Z} \wedge y \leq x \wedge (\forall z \in \mathbf{Z}, z \leq x \Rightarrow z \leq y)$$

We didn’t need the entire definition for our proof above, and in practice we don’t always have to return to definitions when dealing with functions. For example we may have an existing result, such as:

$$\forall x \in \mathbf{R}, \lfloor x \rfloor > x - 1$$

Substituting known results

Every proof would become unmanageably long if we had to include “inline” all the results that it depended on. We inevitably refer to standard results that are either universally known (among math wonks) or can easily be looked up. Sometimes we need to prove a small technical result in order to prove something larger. You may view the smaller result as a helper method (usually returning boolean results) that you use to build a larger method (your bigger proof). To make things modular, you should be able to “call” or refer to the smaller result. An example occurs if we want to re-cycle

Theorem 1: $\forall x \in \mathbf{R}$, $x > 0 \Rightarrow 1/(x+2) < 3$.

We want to use this in proving $\forall y \in \mathbf{R}, y \neq 0 \Rightarrow 1/(y^2+2) < 3$. The template to fill in is[4]

Now we have to fill in the $\vdots$[5]

Proof by cases

To prove $A \Rightarrow B$, it can help to treat some As differently than others. For example, to prove that for all integers $x^2 + x$ is even, you might proceed by noting that $x^2 + x$ is equivalent to $x(x + 1)$. At this point our reasoning has to branch: at least one of the factors x or $x + 1$ is even (for integer x), but we can't assume that a particular factor is even for every integer x. So we use proof by cases[6]

A simple two-case $\vee$ can be expressed in "if... else/otherwise..." style

> If x is even, then $x(x + 1)$ is even.
>
> Otherwise, x is odd, so $x + 1$ is even, and thus $x(x + 1)$ is even.

This is a special case of an "OR" clause being the antecedent of an implication. If you want to prove $(A_1 \vee A_2 \vee \cdots A_n) \Rightarrow B$, (this could happen if, along the way to proving $A \Rightarrow B$ you use the fact that $A \Rightarrow (A_1 \vee \cdots A_n)$. Now you need to prove $A_1 \Rightarrow B$, $A_2 \Rightarrow B, \cdots, A_n \Rightarrow B$. Notice that in setting this up it is not necessary that the A_i be disjoint (mutually exclusive), just that they cover A (think of A being a subset of the union of the A_i). One way to generate the cases is to break up the domain $D = D_1 \cup \cdots \cup D_n$, so $A_i = D_i \wedge A$. Now you have an equivalence, $A \Leftrightarrow A_1 \vee \cdots \vee A_n$. A very common case occurs when the domain partitions into two parts, $D = D_1 \cup \neg D_1$, so you can rewrite A as $(A \wedge D_1) \vee (A \wedge \neg D_1)$.

Indirect proof

Since $p \Rightarrow q$ is equivalent to its contrapositive, $\neg q \Rightarrow p$, proving the latter proves the former. This is called an "indirect proof." The outline format of an indirect proof of $\forall x \in D, p(x) \Rightarrow q(x)$ is[7]

As an exercise, consider $\forall x \in \mathbf{Z}$, if x^2 is odd, then x is odd.

Notes

[1] Let $e \in \mathbf{R}$.

Assume $e > 0$

Let $d_e =$(something helpful)

Then $d_e \in \mathbf{R}$.

Also $d_e > 0$.

Let $x \in \mathbf{R}$.

Assume $0 < |x - a| < d_e$

$\vdots$

So $|f(x) - l| < e$

Hence $0 < |x - a| < d_e \Rightarrow (|f(x) - l| < e)$

Since x is an arbitrary element of $\mathbf{R}$, $\forall x \in \mathbf{R},\ 0 < |x - a| < d_e \Rightarrow (|f(x) - l| < e)$

Thus $\exists d \in \mathbf{R}, d > 0 \wedge (\forall x \in \mathbf{R},\ 0 < |x - a| < d \Rightarrow (|f(x) - l| < e))$

Then, $e > 0 \Rightarrow (\exists d \in \mathbf{R}, d > 0 \wedge (\forall x \in \mathbf{R},\ 0 < |x - a| < d \Rightarrow (|f(x) - l| < e)))$

Since e is an arbitrary element of $\mathbf{R}$,

$$\forall e \in \mathbf{R},\ e > 0 \Rightarrow (\exists d \in \mathbf{R}, d > 0 \wedge (\forall x \in \mathbf{R},\ 0 < |x - a| < d \Rightarrow (|f(x) - l| < e)))$$

[2] Let $x \in \mathbf{R}$

$\vdots$

Then $\lfloor x \rfloor < x + 1$

Since x is an arbitrary element of $\mathbf{R}$, $\forall x \in \mathbf{R}$, $\lfloor x \rfloor < x + 1$.

[3] Let $x \in \mathbf{R}$

Let $y = \lfloor x \rfloor$

Then y is the largest integer $\leq x$ (definition of floor)

So $y \leq x$ and $x < x + 1$ (adding 1 to both sides of an inequality)

So $y < x + 1$

So $\lfloor x \rfloor < x + 1$

Since x was an arbitrary element of $\mathbf{R}$, $\forall x \in \mathbf{R}$, $\lfloor x \rfloor < x + 1$.

[4] Let $y \in \mathbf{R}$

Assume $y \neq 0$

$\vdots$

Hence $1/(y^2+2) < 3$.

Thus $y \neq 0 \Rightarrow 1/(y^2+2) < 3$.

Since y is an arbitrary element of $\mathbf{R}$, $\forall y \in \mathbf{R}$, $y \neq 0 \Rightarrow 1/(y^2+2) < 3$.

[5]Let $y \in \mathbf{R}$.

Assume $y \neq 0$

Then $y^2 \in \mathbf{R}$ and $y^2 \geq 0$ (true for all elements of $\mathbf{R}$).
So $y^2 > 0$, since $y^2 \neq 0$ and $y^2 \geq 0$. (Only real number whose square is 0 is 0)
So, by THEOREM 1, $1/(y^2+2) < 3$.
Hence $y \neq 0 \Rightarrow 1/(y^2+2) < 3$

Since y is an arbitrary element of R, $\forall y \in \mathbf{R}, y \neq 0 \Rightarrow 1/(y^2+2) < 3$

[6]Let $x \in \mathbf{Z}$

Case 1: x is even

Then $x(x+1)$ is even

Case 2: x is odd

Then $x+1$ is even
So $x(x+1)$ is even

Since x is either even or odd, $x(x+1)$ is even in all cases.

Since x is an arbitrary element of $\mathbf{Z}$, $\forall x \in \mathbf{Z}, x(x+1)$ is even.

[7]Let $x \in \mathbf{D}$

Suppose $\neg q(x)$

$\vdots$

Then $\neg p(x)$

Then $p(x) \Rightarrow q(x)$

Since x is an arbitrary element of D, $\forall x \in D, p(x) \Rightarrow q(x)$.