CSC165H, Mathematical expression and reasoning for computer science
week 6

23rd June 2005

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

Midterm preparation

- The midterm (next Thursday from 6:10–7:00) will be 3 questions, worth 5 points each, lasting 50 minutes, during tutorial.
- Midterm material is based on Lectures 1–6 (see web page) and Assignments 1 and 2 (see solutions on web page). You should review the lecture summaries, the assignment solutions, and quiz solutions (to be posted soon).
- I aim to have the marked midterms back to you less than 10 days, and a summary of your term marks thus far in the course will be available at that time.

More proof structure

We continue to develop a structured format for presenting proofs in this course. The intention is to provide you with an example of proof structure that can guide your future work either (a) writing proofs of your own, or (b) evaluating proofs written by others. The structure presented here isn't meant to restrict you to a particular way of writing and presenting proofs, but rather to provide a framework to decide whether a given proof has all its working parts intact.

negation (contrapositive)

Last time we described the search for a chain of implications of the form $p(x) \Rightarrow r_1(x) \Rightarrow r_2(x) \Rightarrow \cdots$, in order to eventually prove $\forall x \in D, p(x) \Rightarrow q(x)$. To help form promising links in this chain, consider whether implications such as $\forall x \in D, t(x) \Rightarrow \neg r_k(x)$. You recognize this as the contrapositive of $\forall x \in D, r_k(x) \Rightarrow \neg t(x)$, so if you have $r_k(x)$ on your list, you can now add $\neg t(x)$.

Symmetrically, we were looking (from the other end) for a chain of the form $s_n(x) \Rightarrow \cdots \Rightarrow s_1(x) \Rightarrow q(x)$. It helps to consider implications of the form $\forall x \in D, \neg s_k(x) \Rightarrow t(x)$, since this is the contrapositive of $\forall x \in D, \neg t(x) \Rightarrow s_k(x)$, adding another link to the chain.

BI-IMPLICATION

Even when searching for an implication, adding bi-implication links is useful. Consider

$$\forall x \in D, r_k(x) \Leftrightarrow r_{k+1}(x)$$

This is the conjunction of two implications, so that if $r_k(x) \Rightarrow q(x)$ then $r_{k+1}(x) \Rightarrow q(x)$, which means that r_{k+1} is a "dead end" if and only if r_k is. This helps trim down the search tree by leading to fewer dead ends.

AN ODD EXAMPLE REVISITED

Last week we considered the implication "$\forall n \in \mathbf{N}$, n odd $\Rightarrow n^2$ odd," and its converse. We developed a direct proof of the implication[1], and found that the same template could not be applied to prove the converse (even though the converse is true). This asymmetry shows that the search through the implication trees from p to q does not necessarily follow the same path as from q to p, even when both paths exist and $p \Leftrightarrow q$.

However, it seems aesthetically disturbing that when $p \Leftrightarrow q$ we don't find a doubly-linked list of implications connecting them. One of your classmates came up with an approach that allows this symmetry (I've modified it slightly)

CLAIM: $\forall n \in \mathbf{N}$, n odd $\Leftrightarrow n^2$ odd.

PROOF:

> Let $n \in \mathbf{N}$.
>
> > Then
> > n^2 is odd
> > is equivalent to
> > $\exists k \in \mathbf{N}$ such that $n^2 = 2k + 1$ (definition of odd natural numbers);
> > is equivalent to
> > $n^2 - 1 = 2k$ is even (definition of even integer),
> > is equivalent to
> > $(n-1)(n+1)$ is even (complete the square);
> > is equivalent to
> > $(n-1)$ is even or $(n+1)$ is even ($\Rightarrow$ if prime number 2 divides a product, it divides some factor) ($\Leftarrow$ definition of even);
> > is equivalent to
> > $(n-1)$ is even or $(n+1) - 2 = (n-1)$ is even (integer i is even if and only if $i - 2$ is even);
> > is equivalent to
> > $(n-1)$ is even (idempotent law);
> > is equivalent to
> > $n - 1 = 2j$ for some integer j (definition of even)
> > is equivalent to
> > $n = 2j + 1$ for some integer j;
> > is equivalent to
> > n is odd
>
> Thus n^2 is odd $\Leftrightarrow n$ is odd.
>
> Since n is an arbitrary natural number,
>
> $\forall n \in \mathbf{N}$, n^2 odd $\Leftrightarrow n$ odd.

Direct proof structure of the universal

Our general form of a direct proof of the implication $\forall x \in D,\ p(x) \Rightarrow q(x)$ is:

Let $x \in D$. (introduce variable x with scope indicated by indentation).

Suppose $p(x)$ (indentation indicates where $p(x)$ is assumed true)

(fill in the proof of $q(x)$)

Hence $p(x) \Rightarrow q(x)$.

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

Here's an example.

Let $\mathbf{R}$ be the set of real numbers. $\forall x \in \mathbf{R}, x > 0 \Rightarrow 1/(x+2) < 3$.

Structure the proof as above:

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

Suppose $x > 0$

(prove $1/(x+2) < 3$)
Therefore $1/(x+2) < 3$.

Hence $x > 0 \Rightarrow 1/(x+2) < 3$.

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

Of course, you should unwrap the sub-proof that $1/(x+2) < 3$.

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

Suppose $x > 0$

so $x + 2 > 2$ (since $x > 0$)
so $1/(x+2) < 1/2$ (since $x + 2 > 2$ and $2 > 0$)
so $1/(x+2) < 3$ (since $1/(x+2) < 1/2$ and $1/2 < 3$)
Therefore $1/(x+2) < 3$.

Hence $x > 0 \Rightarrow 1/(x+2) < 3$.

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

Is the converse true (what is the converse)?[2]

When no implication is stated, then we don't assume (suppose) anything about x other than membership in the domain. For example, $\forall x \in D, p(x)$ has this proof structure:

Let $x \in D$

(prove $q(x)$)
Hence $q(x)$.

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

Direct proof structure of the existential

Consider the example $\exists x \in \mathbf{R}, x^3 + 2x^2 + 3x + 4 = 2$. Since this is the existential, we need only find a single example, and structure the proof as follows:

> Let $x = -1$.
>
> > Then $x \in \mathbf{R}$.
> > Also, $x^3 + 2x^2 + 3x + 4 = (-1)^3 + 2(-1)^2 + 3(-1) + 4 = -1 + 2 - 3 + 4 = 2$.
>
> Since $x \in \mathbf{R}$, $\exists x \in \mathbf{R},\ x^3 + 2x^2 + 3x + 4 = 2$.

The general form for a direct proof of $\exists x \in D, p(x)$ is:

> Let $x =$ [pick a specific value, unlike the universal]
>
> > Then $x \in D$ [this may be obvious from choice of x].
> > prove $p(x)$.
> > Hence $p(x)$
>
> Since $x \in D$, $\exists x \in D, p(x)$.

Multiple quantifiers

Multiple quantifiers cause multiple nesting. Consider $\forall x \in D, \exists y \in D, p(x, y)$. The corresponding proof structure is:

> Let $x \in D$
>
> > Let $y_x =$(select something that helps prove $p(x, y)$)
> >
> > > Then $y_x \in D$.
> > > Also $p(x, y_x)$
> >
> > Since $y_x \in D$, $\exists y, p(x, y)$
>
> Since x is an arbitrary element of D, $\forall x \in D, \exists y \in D, p(x, y)$.

Notes

[1]Let $n \in \mathbf{N}$, and n is odd.

Then, for some $j \in \mathbf{N}$, $n = 2j + 1$ (definition of odd number).

So $n^2 = 4j^2 + 2j + 1$ (definition of squaring a number)
So $n^2 = 2(2j^2 + j) + 1$ (distributive law)
So there exists a natural number $k = 2j^2 + j$ such that $n^2 = 2k + 1$. ($\mathbf{N}$ is closed under addition and multiplication)
So n^2 is odd.

Thus $\forall n \in \mathbf{N}$, n odd $\Rightarrow n^2$ odd.

[2]$\forall x \in \mathbf{R},\ 1/(x + 2) < 3 \Rightarrow x > 0$. False, for example let $x = -4$ (Alex's suggestion), then $1/(-4 + 2) = -1/2 < 3$ but $-4 \not> 0$. Indeed, every $x < -2$ is a counter-example.