CSC165H, Mathematical expression and reasoning for computer science
week 5

16th 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

Proliferating domains

Multiple quantification taxes our picture-drawing skills. For example, we started last lecture with domains E (for employees) and $\mathbf{N}$ (natural number), and we had predicates $f(e)$ (employee is female), $s(e, k)$ (employee makes salary k) and $k > 25,000$. If we wanted to guide our thinking with a detailed drawing, we would have to think of our predicates as being in the domain $E \times \mathbf{N}$ — the Cartesian product of E and $\mathbf{N}$, defined as the set of ordered pairs (e, n), where $e \in E$ and $n \in \mathbf{N}$. A trivial change to our predicate can make them artificially take pairs as arguments: $f(e, k)$ means e is female, regardless of k, and $(e, k) > 25,000$ means. So now the sentence $\exists e, \exists k, f(e, k) \wedge s(e, k) \wedge (e, k) > 25,000$ simply means that the intersection of the three sets in $E \times \mathbf{N}$ is non-empty.

If we take the Cartesian product of two sets, then we can think of the sets as axes of the two-dimensional plane and make another sort of drawing. From this point of view, the claim $\forall x \in D_1, \exists y \in D_2, P(x, y)$ says that there is a graph of some function in from D_1 to D_2 that is contained in the set that satisfies $P(x, y)$. On the other hand $\exists y, \forall x, P(x, y)$ says that there is a constant function from D_1 to D_2 that is contained in the set that satisfies $P(x, y)$. You may need to extend the usual conventions of diagrams to guide your thinking when reasoning about domains.

Transitivity of implication

Consider $(P(x) \Rightarrow Q(x)) \wedge (Q(x) \Rightarrow R(x))$ (I have put the parentheses to make it explicit that the implications are considered before the $\wedge$). What does this statement imply if considered in terms of sets P, Q, and R?[1] We can also work this out using the logical arithmetic we introduced last week: write $\neg(((P(x) \Rightarrow Q(x)) \wedge (Q(x) \Rightarrow R(x))) \Rightarrow (Q(x) \Rightarrow R(x)))$ using only $\vee, \wedge$, and $\neg$, and show that it is a contradiction (never true). Use DeMorgan's law, the distributive laws, and anything else that comes to mind. Thus, implication is transitive.

A similar transformation is that $P(x) \Rightarrow (Q(x) \Rightarrow R(x))$ is equivalent to $(P(x) \wedge Q(x)) \Rightarrow R(x)$. Notice this is stronger than the previous result (an equivalence rather than an implication).

Proofs

We want to make convincing arguments that a statement is true. We're allowed (forced, actually) to use previously proven statements and axioms (things that are defined to be true, or assumed to be true, for the domain). For example, if D is the real numbers, then we have plenty of rules about arithmetic and inequalities.

Setting up direct proof of implication

Consider implications of the form

c1: $\forall x \in D, p(x) \Rightarrow q(x)$

Many already-known-to-be-true statements are universally quantified implications like c1. We'd like to find among them a chain:

c2.0: $\forall x \in D, p(x) \Rightarrow r_1(x)$

c2.1: $\forall x \in D, r_1(x) \Rightarrow r_2(x)$

$\vdots$

c2.n: $\forall x \in D, r_n(x) \Rightarrow q(x)$

This, in n steps, proves c1, using the transitivity of implication. A more flexible way to summarize that the chain c2.0…c2.n prove c1 is to cite the intermediate implications that justify each intermediate step. Here you write the proof that $p(x) \Rightarrow q(x)$ as

Let $x \in D$ be such that $p(x)$

> Then $r_1(x)$ (by c2.0)
>
> So $r_2(x)$ (by c2.1)
>
> $\vdots$
>
> So $q(x)$ (by c2.n)

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

This form emphasizes what each existing result adds to our understanding. And when it's obvious which result was used, we can just avoid mentioning it (but be careful, one person's obvious is another's mystery).

Although this form seems to talk about just one particular x, by not assuming anything more than $x \in D$ and $p(x)$, it applies to every $x \in D$ with $p(x)$.

Hunting the elusive direct proof

In general, the difficulty with direct proof is there are lots of known results to consider. The fact that a result is true may not help your particular line of argument (there are many, many, true but irrelevant facts). In practice, to find a chain from $p(x)$ to $q(x)$, you gather two lists of results about x:

1. results that $p(x)$ implies, and
2. results that imply $q(x)$

Your fervent hope is that some result appears on both lists.

$$\begin{array}{l} p(x) \\ r_1(x) \\ r_2(x) \\ \vdots \\ s_2(x) \\ s_1(x) \\ q(x) \end{array}$$

Anything that one of the r_i implies can be added to the first list. Anything that implies one of the s_i can be added to the second list. What does this look like in pictures?

In Venn diagrams we can think of the r_i as sets that contain p but may not be contained in q (the ones that don't are dead ends). On the other hand, the s_i are contained in q but may not contain p (the ones that don't are dead ends). We hope to find a patch of containment from p to q. Another way to visualize this is by having the r_i represented as a tree. In one tree we have root p, with children being the r_i that p implies, and their children being results they imply. In a second tree we have root q, with children being the results that imply q, and their children being results that imply them. If the two trees have a common node, we have a chain.

Are you done when you find a chain? No, you write it up, tidying as you go. Remove the results that don't contribute to the final chain, and cite the results that take you to each intermediate link in the chain.

What do $\wedge$ and $\vee$ do?

Now your two lists have the form

$$\begin{array}{l} \forall x \in D, p(x) \Rightarrow (r_1(x) \wedge r_2(x) \cdots r_m(x)) \\ \forall x \in D, (s_k(x) \vee \cdots \vee s_1(x)) \Rightarrow q(x) \end{array}$$

Since $p(x)$ implies any "and" of the r_i, you can just collect them in your head until you find a known result, say $r_1(x) \wedge r_2(x) \Rightarrow r_k(x)$, and then add $r_k(x)$ to the list. On the other hand, if you have a result on the first list of the form $r_1(x) \wedge r_2(x)$, you can add them separately to the list. On the second list, use the same approach but substitute $\vee$ for $\wedge$. Any result on the first list can be spuriously "or'ed" with anything: $r_1(x) \Rightarrow (r_1(x) \vee l(x))$ is always true. On the second list, we can spuriously "and" anything, since $(s_1(x) \wedge l(x)) \rightarrow s_1(x)$.

If we have a disjunction $r_1(x) \vee r_2(x)$ on the first list, we can use it if we have a result that $(r_1(x) \vee r_2(x)) \Rightarrow q(x)$, or the pair of results $r_1(x) \Rightarrow q(x)$, and $r_2(x) \Rightarrow q(x)$.

An odd example

Suppose you are asked to prove that every odd natural number has a square that is odd. You can start by writing the outline of the proof you would like to have:

> Let $n \in \mathbf{N}$, and n is odd.
>
> > $\vdots$
> >
> > So n^2 is odd.

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

Start scratching away at both ends of the $\vdots$ (the bit that represents the chain of results we need to fill in). What does it mean for n^2 to be odd? Well, if there is a natural number k such that $n^2 = 2k + 1$, then n^2 is odd (by definition of odd numbers). Add that to the end of the list. Similarly, if n is odd, then there is a natural number j such that $n = 2j + 1$ (by definition of odd numbers). It seem unpromising to take the square root of $2k + 1$, so why not carry out the almost-automatic squaring of $2j + 1$? So now, on our first list, we have that, for some natural number j, $n^2 = 4j^2 + 2j + 1$. Using some algebra (distributivity of multiplication over addition), this means that for some natural number j, $n^2 = 2(2j^2 + j) + 1$. If we let k from our second list be $2j^2 + j$, then we certainly satisfy the restriction that k be a natural number (they are closed under multiplication and addition), and we have linked the first list to the second:[2]

How about the converse, $\forall n \in \mathbf{N}$, if n^2 is odd, then n is odd. If we try creating a chain, it seems a bit as though the natural direction is wrong: somehow we'd like to go from q back to p. What equivalent of an implication allows us to do this?[3]

We can set this up similarly, assuming the negation of our consequent (i.e that n is even), and trying to chain to the negation of our antecedent (i.e. that n^2 is even).

Notes

[1] It implies that P is a subset of R, since $P \subseteq Q$ and $Q \subseteq R$. It is not equivalent, since you can certainly have $P \subseteq R$ without $P \subseteq Q$ or $R \subseteq Q$.

[2] 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.

[3] The contrapositive.