Some notes on DMI and DMII material

Thomas Forster

May 11, 2014

COMPUTER SCIENCE TRIPOS Part IA 2013 Paper 2 Q 5(b)

Suppose there is a surjection $f : D \twoheadrightarrow (D \to D)$. Show that this happens if and only if D has precisely one element.

If D has one element then $D \to D$ is the singleton of the identity function $\mathbb{1}_D$ and both D and $D \to D$ are singletons so there is a surjection as desired.

If D is empty then $D \to D$ is the singleton of the empty function. There can be no surjection from the empty set to a nonempty set, so again, we get the result we want.

Now suppose D is a set with at least two members. Let us name two of them 'a' and 'b'. Suppose further that $f : D \to (D \to D)$. We will show that f is not surjective.

The challenge is to cook up a function $\delta : D \to D$ which is not in the range of f. And we have to cook up such a function using only f, a and b. ...

Observe that we *have* to use *both* a and b. After all, we saw above that if f has only one member there *is* a surjection. We should expect a diagonal construction to appear, so tinkering with $f(x)$ applied to x would be a good thing to start with. And of course we have to alter the thing on the diagonal, so something like the following would be worth trying.

Define a function $\delta : D \to D$ by

$$\texttt{if } (f(x))(x) = a \texttt{ then } b \texttt{ else } a$$

The chief effect of this definition is that

$$(\forall d \in D)(\delta(d) \neq (f(d))(d)) \tag{1}$$

We now claim that δ is not in the range of f. For suppose δ were $f(d_0)$; we obtain a contradiction by considering $\delta(d_o)$.

$\underline{\delta}(d_o) = \underline{f(d_0)}(d_0)$ (the underlined parts are identical by definition).

But we also have

$\delta(d_o) = (f(d_0))(d_0)$ by (1)

giving us the contradiction we sought.

Observe that we used only the fact that D has two distinct elements. We had not assumed that D was finite. You can try [tho' you shouldn't] to prove this result by induction on the size of D, but that only proves it for D that are finite.

For the *cognoscenti*... we have also used excluded middle on $x = a$, in the definition of δ.

A question on the last example sheet of DM I 2013

RTP

$$x^{m+n} = x^n \cdot x^m$$

That's what it sez on the example sheet, and of course it's true for any kind of number—but the example sheet is on induction!

Observe that all these three variables could be variables ranging over $\mathbb{N}$. So any of these variables could become embroiled in an induction. It looks fairly clear that induction on 'x' is not going to be much use to us. Pretty obviously we want to do a UG on 'x'. But what do we do with the other two variables? I can't see an easy way to find the correct approach, and this is typical of this kind of problem. I just wrestled with it until it came out.

We fix x and prove by induction on 'm' that, for each m,

$$(\forall n)(x^{n+m} = x^n \cdot x^m)$$

Start with $m = 0$.

$$(\forall n)(x^{n+0} = x^n \cdot x^0)$$

That was easy. Now for the induction step.

For the induction assume

$$(\forall n)(x^{n+m} = x^n \cdot x^m)$$

So certainly

$$(\forall n)(x^{(n+1)+m} = x^{n+1} \cdot x^m)$$

whence

$$(\forall n)(x^{(n+1)+m} = x^n \cdot x \cdot x^m)$$

Then we do lots of rearrangement using associativity and commutativity of addition.

$$(\forall n)(x^{(n+1)+m} = x^n \cdot x^{1+m})$$

$$(\forall n)(x^{(n+1)+m} = x^n \cdot x^{m+1})$$

$$(\forall n)(x^{n+(1+m)} = x^n \cdot x^{m+1})$$

$$(\forall n)(x^{n+(m+1)} = x^n \cdot x^{m+1})$$

which is the same statement for $m + 1$.

You have to chose your induction carefully in order to not get into a tangle.

Observe that these three variables are treated in three different ways! UG on 'z', induction on 'm', and the 'n' is carried around and not inducted on.

Exercise 1.3 in DM II

"Suppose 99 passengers are assigned to one of two flights, one to Almeria and one to Barcelona. Show one of the flights has at least 50 passengers assigned to it. (Which flight is it?)"

Students find this question disconcerting, co's it's so bloody obvious: what on earth is one supposed to say? The answer is that you are supposed to say the following: suppose neither of the planes had as many as 50 passengers on it. Then the largest number of passengers in aggregate that there could be is 98. But there are 99. So it isn't true that neither of the planes has as many as 50 passengers on it. So at least one does.

The point of the question (easy to miss, in the midst of one's puzzlement about how to prove the obvious) is that the conclusion is obtained by means of a *proof by contradiction*. Generally, if one is trying to prove the existence of something—a solution to an equation perhaps—then one prefers direct proofs to proofs-by-contradiction. Typically a proof that does *not* use proof-by-contradiction can be unpicked to reveal a construction of the object whose existence one is trying to prove. In contrast we find that existence proofs that use proof-by-contradiction cannot be unpicked in this way, and this is strikingly illustrated by the question before you. You are trying to prove that there is a plane with ≥ 50 passengers on it. You assume that there isn't, obtain a contradiction, and conclude that there is. It's a proof all right, but it doesn't tell you which plane is the answer.

The best advice is to avoid proof-by-contradiction whenever possible, for precisely that reason. Sometimes, however—as this example illustrates—it is the only proof available. How can i assert this so confidently? Beco's information about the planes is symmetric: anything you can prove about one you can prove

about the other, and you clearly can't prove that they *both* have ≥ 50 people on them co's there are only 99 passengers all told. A proof that didn't use proof-by-contradiction would tell you which of the two planes it was that had ≥ 50 passengers on it, and there can clearly be no such proof. The proof that we have—using proof-by-contradiction—is the only show in town.

A discussion of Question B11 in Glynn Winskel's DMII notes

The Question

"Define the length of a Boolean proposition by structural induction as follows:

$|a| = 1$,
$|\top| = 1$,
$|\bot| = 1$,
$|A \wedge B| = |A| + |B| + 1$,
$|A \vee B| = |A| + |B| + 1$,
$|\neg A| = |A| + 1$.

Define a translation which eliminates disjunction from Boolean expressions by the following structural induction:

$tr(a) = a$, $tr(\top) = \top$, $tr(\bot) = \bot$,
$tr(A \wedge B) = tr(A) \wedge tr(B)$,
$tr(A \vee B) = \neg(\neg tr(A) \wedge \neg tr(B))$,
$tr(\neg A) = \neg tr(A)$.

Prove by structural induction on Boolean propositions that

$$|tr(A)| \leq 3|A| - 1,$$

for all Boolean propositions A."

Discussion

This is a beautiful question, co's it touches several important points. It tests your understanding of structural induction; it tests your ability to do the fiddly manipulation necessary to perform the inductive step; it underlines the importance of having a sufficiently strong induction hypothesis, and finally it makes a point about dereferencing.

So: we have a propositional language—a recursive datatype of formulæ—which starts off with three propositional letters ("literals") 'a', '$\top$' and '$\bot$'. We then build up compound formulæ by means of the constructors '$\wedge$', '$\vee$' and '$\neg$'. We have a *length* function defined on objects in the datatype of formulæ, written

with two vertical bars as in the question, which is roughly what you think it is—so that the length of a literal is 1, and the length of a conjunction (or a disjunction) of two formulæ is one plus the sum of their lengths, and the length of the negation of a formula is one plus the length of the formula. Evidently the question-designer thought that the length of a '(' or a ')' is zero!

One tends naturally to write the second half of the preceding paragraph with expressions like

$$|A \wedge B| = |A| + |B| + 1.$$

This looks fair enough, and in some sense it is, but we need to be clear about the conventions we are using. The letter 'A' by itself is a single symbol, so a pedant might insist that $|A| = 1$. This is wrong of course: the letter 'A' is not a formula, but a variable ranging over formulæ... when looking for the length $|A|$ of A we have to *see through* the variable all the way to the value it takes—and that value is a formula. All this is well and good, but it can cause some confusion when we start thinking about expressions like: $|A \vee B|$. The constructor '$\vee$' is something we put between two formulæ to make a new formula; we don't put it between two *names* of formulæ or between two *pointers* to formulæ! Until we have a convention to make our practice OK, writing things like '$|A \vee B|$' should generate a `syntax error` warning. If you look back to the first page you will find that i wrote

> "... length of a literal is 1, and the length of a conjunction (or a disjunction) of two formulæ is one plus the sum of their lengths..."

... and this is syntactically correct. When we wrote '$|A \wedge B|$' we should really have written '| the conjunction of A and B|'.

There are two ways of dealing with this. One is to have explicit names for the constructors, as it might be 'conjunction of ...' and 'disjunction of ...' and 'negation of ...' This makes huge demands on our supply of alphanumerics. The other solution is to have a kind of `environment` command that creates an environment within which [deep breath]

> *contructors applied to* **pointers** *to objects construct* **pointers** *to the objects thereby constructed.*

Inside such a context things like '$|A \vee B|$' have the meaning we intend here. There is a culture within which this environment is created by the '$\ulcorner$' symbol (LaTeX: `\ulcorner`) and closed by the '$\urcorner$' symbol (LaTeX: `\urcorner`). In fact people tend to leave things out.

Thus we should/should have posed the question as:

"Define the length of a Boolean proposition by structural induction as follows:

$|a| = 1,$
$|\top| = 1,$

$|\bot| = 1$,
$|\ulcorner A \wedge B \urcorner| = |A| + |B| + 1$,
$|\ulcorner A \vee B \urcorner| = |A| + |B| + 1$,
$|\ulcorner \neg A \urcorner| = |A| + 1$.

Define a translation which eliminates disjunction from Boolean expressions by the following structural induction:

$tr(a) = a$, $tr(\top) = \top$, $tr(\bot) = \bot$,
$\ulcorner tr(A \wedge B) = tr(A) \wedge tr(B)$,
$tr(A \vee B) = \neg(\neg tr(A) \wedge \neg tr(B))$,
$tr(\neg A) = \neg tr(A) \urcorner$.

Prove by structural induction on Boolean propositions that

$$|tr(A)| \leq 3|A| - 1,$$

for all Boolean propositions A."

The above use of corner quotes illustrates how there is no restriction that says that the scope of the corner quotes has to live entirely inside a single formula. I use corner quotes in what follows, but (although—i *think*–i have put them in correctly) they can be inserted correctly in more than one way.

The Proof by Structural Induction

We aspire to prove by structural induction on the recursive datatype of formulæ that

$$(\forall A)(|tr(A)| \ \leq \ 3 \cdot |A| - 1)$$

The base case we verify easily. The induction step has three cases

$\neg$ If $|tr(A)| \ \leq \ 3 \cdot |A|$ what is $|\ulcorner tr(\neg A) \urcorner|$? $\ulcorner tr(\neg A) = \neg tr(A) \urcorner$ so $\ulcorner |tr(\neg A)| = |\neg tr(A)| \urcorner$, and $|\ulcorner \neg tr(A) \urcorner|$ is $|tr(A)| + 1$ which is certainly $\ \leq \ 3 \cdot |\ulcorner \neg A \urcorner|$.

$\wedge$ If $|tr(A)| \ \leq \ 3 \cdot |A|$ and $|tr(B)| \ \leq \ 3 \cdot |B|$ what is $|\ulcorner tr(A \wedge B) \urcorner|$?

$\ulcorner tr(A \wedge B) \urcorner$ is $\ulcorner tr(A) \wedge tr(B) \urcorner$. By induction hypothesis $|tr(A)| \ \leq \ 3 \cdot |A| - 1$ and $|tr(B)| \ \leq \ 3 \cdot |B| - 1$ so $\ulcorner |tr(A) \wedge tr(B)| \urcorner \ \leq \ (3 \cdot |A| - 1) + (3 \cdot |B| - 1) + 1$. The final '+1' is for the '$\wedge$'. This rearranges to

$|\ulcorner tr(A) \wedge tr(B) \urcorner| \ \leq \ 3 \cdot (|A| + |B|) - 1$

but $|A| + |B| \ \leq \ |\ulcorner A \wedge B \urcorner|$ whence

$\ulcorner |tr(A) \wedge tr(B)| \ \leq \ 3 \cdot (|A \wedge B|) - 1 \urcorner$ and finally

$\ulcorner |tr(A \wedge B)| \ \leq \ 3 \cdot (|A \wedge B|) - 1 \urcorner$.

$\bigvee$ If $|tr(A)| \leq 3 \cdot |A|$ and $|tr(B)| \leq 3 \cdot |B|$ what is $|tr(A \vee B)|$? $\ulcorner tr(A \vee B) \urcorner$ is $\ulcorner \neg(\neg tr(A) \wedge \neg(tr(B))) \urcorner$. What is the length of this last expression? Clearly it's going to be $|tr(A)| + |tr(B)|$ + one for the outermost '$\neg$' + one for the '$\neg$' attached to $tr(A)$ + one for the '$\neg$' attached to $tr(B)$ + one for the '$\wedge$' ... giving $|tr(A)| + |tr(B)| + 4$. By induction hypothesis $|tr(A)| \leq 3 \cdot |A| - 1$ and $|tr(B)| \leq 3 \cdot |B| - 1$ so we have

$\ulcorner |tr(A \vee B)| \leq (3 \cdot |A| - 1) + (3 \cdot |B| - 1) + 4 \urcorner$. We can rearrange this to

$\ulcorner |tr(A \vee B)| \leq 3 \cdot (|A| + |B|) - 1 - 1) + 4 \urcorner$ and further to

$\ulcorner |tr(A \vee B)| \leq 3 \cdot (|A| + |B|) + 2 \urcorner$.

Now $|A| + |B| = \ulcorner |A \vee B| \urcorner - 1$ so we can substitute getting

$\ulcorner |tr(A \vee B)| \leq 3 \cdot (|A \vee B| - 1)) + 2 \urcorner$ and rearrange again to get

$\ulcorner |tr(A \vee B)| \leq 3 \cdot |A \vee B| - 1 \urcorner$ as desired.

A final thought ... I wouldn't mind betting that quite a lot of thought went into this question. We've proved $|tr(A)| \leq 3 \cdot |A| - 1$ so we've certainly also proved the weaker claim $|tr(A)| \leq 3 \cdot |A|$. However wouldn't stake my life on our ability to prove the weaker claim by induction. You might like to try ... i'm not going to!

Exercise C.1 in DM II

Part (i). If you think of A, B, C and D as intervals in $\mathbb{R}$, then the LHS is an intersection of two rectangles in the plane and the RHS is a rectangle in the plane.

Exercise 3.34 in DM II

The set of rationals is countable, so if the set of *ir*rationals is countable, so too would be the set of reals, and it ain't. You all got that.

Observe however that this proof does not prove that the set of irrationals is of size $2^{\aleph_0}$ (tho', as a matter of fact, it is).... After all—for all you know—it might be possible to chop the reals into two smaller pieces, both of them uncountable. Finding a bijection between the reals and the irrationals requires a bit of work. Fiddly. If you want to try, you might like to think about continued fractions. But you probably have enough on your plate as it is.

Find a bijection between $\mathcal{P}(X \times Y)$ and $\mathcal{P}(X) \to Y$

Need a picture here. (**Hint!**)

Left-to-right

Given $A \subseteq \mathcal{P}(X \times Y)$ we want a function $f : \mathcal{P}(X) \to Y$.
Evidently we want

$$L : \quad \lambda x_X.\{y \in Y : \langle x, y\rangle \in A\}.$$

Right-to-left

$$R : \quad \lambda f.\{\langle x, y\rangle : y \in f(x)\}.$$

Finally we want to check that these two functions are inverse to each other. (That's the best way to check that each is injective and surjective)

$$\begin{aligned} L(R(f)) &= L(\{\langle x, y\rangle : y \in f(x)\}) \\ &= \lambda x.\{y : \langle x, y\rangle \in \{\langle x, y\rangle : y \in f(x)\}\} \\ &= \lambda x.\{y : y \in f(x)\} \\ &= \lambda x.f(x) \\ &= f \end{aligned}$$

$$\begin{aligned} R(L(A)) &= R(\lambda x.\{y : \langle x, y\rangle \in A\}) \\ &= \{\langle x, y\rangle : y \in \lambda z.\{y : \langle x, y\rangle \in A\}(x)\} \\ &= \{\langle x, y\rangle : \langle x, y\rangle \in A\} \\ &= A \end{aligned}$$