On mathematical induction and the invariance theorem

Introduction

Roughly speaking, two kinds of mathematical theorems exist. Theorems of the first kind serve to record the results of mathematical labour. Such theorems may represent deep insights and their proofs may be difficult. They are the theorems theories are made of. Theorems of the second kind are used as building blocks in proofs of other theorems or in derivations of programs. They need not be deep nor need their proofs be difficult. What counts is whether they embody a meaningful separation of concerns: in order to be useful they must contribute to the disentanglement of the mathematical reasoning in which they are used.

In this paper we present a theorem of the second kind, a generalisation of the principle of Mathematical Induction. It is not deep and it is probably not new either. The idea behind it is used implicitly in many designs of proofs and programs. We believe that this theorem indeed embodies a meaningful separation of concerns and that its explicit formulation contributes to a better disentanglement of the designs in which it is used. To provide some support for this opinion we show an application of the theorem. Besides, this paper is an exercise in proof construction.

Mathematical induction

V and C are sets. Dummies u and v range over V, whereas x and y range over C. Predicates on V are denoted by P, and Q and R denote predicates on C. Furthermore, $<$ is a binary relation on C.

theorem: $(0) \wedge (1) \Rightarrow (2)$, with:

(0) $t : V \rightarrow C$

(1) $(\mathbf{A}R :: (\mathbf{A}x :: R{\cdot}x) \Leftarrow (\mathbf{A}x :: R{\cdot}x \Leftarrow (\mathbf{A}y : y < x : R{\cdot}y)))$

(2) $(\mathbf{A}P :: (\mathbf{A}u :: P{\cdot}u) \Leftarrow (\mathbf{A}u :: P{\cdot}u \Leftarrow (\mathbf{A}v : t{\cdot}v < t{\cdot}u : P{\cdot}v)))$

□

Formula (1) expresses that (the universal truth of) predicates on C may be proved by mathematical induction; this is a property of C together with $<$. In most applications $<$ is (the non-reflexive part of) a partial order; partially ordered sets $(C,<)$ satisfying (1) are also called *well-founded* sets. The theorem states that, for well-founded sets C , predicates on V may be proved by *mathematical induction on (the values of) t* , so to speak, for any function t of type $V \rightarrow C$.

proof of theorem: Assuming $(0) \wedge (1)$, we prove, for predicate P (on V), the term of (2) by transforming it into an instance of (1) . For this purpose, we need a predicate R (on C) coupled to P in such a way that this transformation is possible; postponing the choice of R , we derive:

$$
\begin{array}{ll}
 & (\mathbf{A}u :: P{\cdot}u) \\
= & \quad \{ \text{ lemma about } P \text{ and } C \text{ (see below), with } Q{\cdot}x \leftarrow \text{true } \} \\
 & (\mathbf{A}x :: R{\cdot}x) \\
\Leftarrow & \quad \{ \ (1) \ \} \\
 & (\mathbf{A}x :: R{\cdot}x \Leftarrow (\mathbf{A}y : y < x : R{\cdot}y)\,) \\
= & \quad \{ \text{ the same lemma, with } Q{\cdot}x \leftarrow (\mathbf{A}y : y < x : R{\cdot}y) \ \} \\
 & (\mathbf{A}u :: P{\cdot}u \Leftarrow (\mathbf{A}y : y < t{\cdot}u : R{\cdot}y)\,) \\
= & \quad \{ \text{ trading (preparing for application of the lemma to } R{\cdot}y) \ \} \\
 & (\mathbf{A}u :: P{\cdot}u \Leftarrow (\mathbf{A}y :: R{\cdot}y \Leftarrow y < t{\cdot}u)\,) \\
= & \quad \{ \text{ again the lemma, with } Q{\cdot}y \leftarrow y{<}t{\cdot}u \text{ and dummy renaming } u \leftarrow v \ \} \\
 & (\mathbf{A}u :: P{\cdot}u \Leftarrow (\mathbf{A}v :: P{\cdot}v \Leftarrow t{\cdot}v < t{\cdot}u)\,) \\
= & \quad \{ \text{ trading } \} \\
 & (\mathbf{A}u :: P{\cdot}u \Leftarrow (\mathbf{A}v : t{\cdot}v < t{\cdot}u : P{\cdot}v)\,) \quad .
\end{array}
$$

This concludes the proof of (2) . The lemma is a generalisation of the first step of this derivation. The lemma represents the coupling of P and R as we need it above. By proving the lemma we construct a suitable R .

lemma: For all predicates Q (on C):

$$(\mathbf{A}x :: R{\cdot}x \Leftarrow Q{\cdot}x) \equiv (\mathbf{A}u :: P{\cdot}u \Leftarrow Q{\cdot}(t{\cdot}u))$$

proof: The lemma must hold for all predicates Q . For the special case that Q is the point-predicate $(=y)$, we derive:

$$
\begin{array}{ll}
 & (\mathbf{A}x::R{\cdot}x \Leftarrow x=y) \;\equiv\; (\mathbf{A}u::P{\cdot}u \Leftarrow t{\cdot}u=y) \\
= & \quad \{\ \text{trading}\ \} \\
 & (\mathbf{A}x:x=y:R{\cdot}x) \;\equiv\; (\mathbf{A}u:t{\cdot}u=y:P{\cdot}u) \\
= & \quad \{\ \text{one-point rule}\ \} \\
 & R{\cdot}y \;\equiv\; (\mathbf{A}u:t{\cdot}u=y:P{\cdot}u) \quad .
\end{array}
$$

Using this as definition of R we now prove the lemma for arbitrary Q :

$$
\begin{array}{ll}
 & (\mathbf{A}x::R{\cdot}x \Leftarrow Q{\cdot}x) \\
= & \quad \{\ \text{definition of } R\ \} \\
 & (\mathbf{A}x::(\mathbf{A}u:t{\cdot}u=x:P{\cdot}u) \Leftarrow Q{\cdot}x) \\
= & \quad \{\ (\Leftarrow Q{\cdot}x) \text{ distributes over } \mathbf{A}\ \} \\
 & (\mathbf{A}x::(\mathbf{A}u:t{\cdot}u=x:P{\cdot}u \Leftarrow Q{\cdot}x)) \\
= & \quad \{\ \text{shuffling dummies}\ \} \\
 & (\mathbf{A}u::(\mathbf{A}x:t{\cdot}u=x:P{\cdot}u \Leftarrow Q{\cdot}x)) \\
= & \quad \{\ (0) : \text{one-point rule}\ \} \\
 & (\mathbf{A}u::P{\cdot}u \Leftarrow Q{\cdot}(t{\cdot}u))
\end{array}
$$

□

□

The main calculation in the above proof consists of four steps; one step is a (necessary) appeal to (1) , the other three steps are applications of the lemma, needed to replace P by R or vice versa. Because (2) contains three occurrences of P , three applications of the lemma are not surprising. The lemma itself captures what these three replacements have in common. It is the interface between the definition of R and its use in the proof of the theorem. So, the lemma is a theorem of the second kind too: it is introduced for the modularisation of the proof. Finally, we note that the theorem is independent of the properties of $<$.

The invariance theorem

In her Ph.D. thesis [0], A.J.M. van Gasteren presents a formal derivation of a proof of (an abstract version of) the invariance theorem. After a minor simplification, the theorem is, in the nomenclature of [0]:

theorem: For

P,Q : predicates on a set V ,
t : a function of type $V \to C$, where $(C,<)$ is partially ordered ,
f : a predicate transformer (for predicates on V) ,

we have that $[P \Rightarrow Q]$ follows from the conjunction of

(0) $(C,<)$ is well-founded
(2) $(\mathbf{A}x :: [P \wedge t=x \Rightarrow f.(P \wedge t<x)])$
(3) $[f.Q \Rightarrow Q]$
(4) f is monotonic, i.e. for all predicates X,Y on V: $[X \Rightarrow Y] \Rightarrow [f.X \Rightarrow f.Y]$

□

In this theorem square brackets denote universal quantification over V . In (2) and in what follows dummies u and v range over V , and x and y range over C .

The presence of function t and premiss (0) are indications that we could try to prove this theorem by mathematical induction on t . This even seems to be the only way to exploit (0) . Before doing so, however, we simplify premiss (2) -- the most complicated one -- :

$(\mathbf{A}x :: [P \wedge t=x \Rightarrow f.(P \wedge t<x)])$
$=$ { definition of $[\cdots]$ }
$(\mathbf{A}x :: (\mathbf{A}u :: P.u \wedge t.u=x \Rightarrow f.(P \wedge t<x).u))$
$=$ { shuffling dummies }
$(\mathbf{A}u :: (\mathbf{A}x :: P.u \wedge t.u=x \Rightarrow f.(P \wedge t<x).u))$
$=$ { trading }
$(\mathbf{A}u :: (\mathbf{A}x : t.u=x : P.u \Rightarrow f.(P \wedge t<x).u))$
$=$ { one-point rule }

$(\mathbf{A}u :: P\cdot u \Rightarrow f\cdot(P \wedge t < t\cdot u)\cdot u)$

= { introduction of predicate R_u , see below }

$(\mathbf{A}u :: P\cdot u \Rightarrow f\cdot R_u\cdot u)$.

The formula thus obtained is simpler than (2) : it contains quantifications over V only, whereas (2) contains quantifications over *different* ranges (C and V). Instead of (2) , we therefore use (2a) and (2b) with:

(2a) $(\mathbf{A}u :: P\cdot u \Rightarrow f\cdot R_u\cdot u)$

(2b) $(\mathbf{A}v :: R_u\cdot v \equiv P\cdot v \wedge t\cdot v < t\cdot u)$.

aside on notation: The definition of R_u contains global variable u . As an aide-mémoire, we have used subscription to indicate this: on the one hand we do not want to leave the dependence on u implicit, on the other hand u occurs as a constant in the following calculations. Omission of the subscript is not without danger: it might seduce us to rewrite (2a) to $[P \Rightarrow f\cdot R]$, which is incorrect. If so desired, name R_u can be avoided by means of λ-notation: $R_u = (\lambda v :: P\cdot v \wedge t\cdot v < t\cdot u)$.

To some extent, the notation used in formula (2) is misleading: the occurrence of $t = x$ in the antecedent of the implication could inspire us to eliminate x by replacing -- equals for equals -- its occurrence in the consequent by t , which is certainly wrong. This can be discovered by looking at the types of the variables occurring in the formula: t has type $V \rightarrow C$ whereas x has type C . Apparently, $t = x$ does not mean "t equals x" but it denotes the predicate $(\lambda u :: t\cdot u = x)$. Similarly, $\wedge$ does not denote the boolean operator but the predicate connective $\dot\wedge$ defined by $(\mathbf{A}u :: (P \mathbin{\dot\wedge} Q)\cdot u \equiv P\cdot u \wedge Q\cdot u)$. Overloading $\wedge$ with the meaning of $\dot\wedge$ is harmless, but overloading = is not: then, what does, for functions f and g of the same type, $f = g$ mean? By assigning to = a meaning that differs from equality we deny ourselves the possibility to use Leibniz's rule of substitution of equals for equals; according to [0] (p.155) "such substitution is the simplest type of manipulation one can imagine" . (In view of this, we might consider to extend the use of $\equiv$ and define $f \equiv g$ by $(\mathbf{A}x :: (f \equiv g)\cdot x \equiv (f\cdot x = g\cdot x))$, for all functions f and g of the same type, predicates or not; then, we have $(f = g) \equiv [f \equiv g]$).

Formula (2) can be rewritten in two ways: by use of an explicit dummy for the quantification implied by $[\cdots]$, as we did above, or by use of dummy-free notation designed for the purpose; for example:

$$(\mathbf{A}x::[P \wedge (=x)\circ t \Rightarrow f\cdot(P \wedge (<x)\circ t)])$$

□

proof of theorem: Having decided to use mathematical induction, we derive:

$[P \Rightarrow Q]$

$=$ { definition of $[\cdots]$ }

$(\mathbf{A}u::P\cdot u \Rightarrow Q\cdot u)$

$\Leftarrow$ { mathematical induction on t (using (0)) }

$(\mathbf{A}u::(P\cdot u \Rightarrow Q\cdot u) \Leftarrow (\mathbf{A}v:t\cdot v<t\cdot u:P\cdot v \Rightarrow Q\cdot v))$.

We prove this as follows:

$(\mathbf{A}v:t\cdot v<t\cdot u:P\cdot v \Rightarrow Q\cdot v)$

$=$ { trading (preparing for (2b)) }

$(\mathbf{A}v::P\cdot v \wedge t\cdot v<t\cdot u \Rightarrow Q\cdot v)$

$=$ { (2b) (definition of R_u) }

$(\mathbf{A}v::R_u\cdot v \Rightarrow Q\cdot v)$

$\Rightarrow$ { (4) (to introduce f's) }

$(\mathbf{A}v::f\cdot R_u\cdot v \Rightarrow f\cdot Q\cdot v)$

$\Rightarrow$ { instantiation (to eliminate the quantification) }

$f\cdot R_u\cdot u \Rightarrow f\cdot Q\cdot u$

$\Rightarrow$ { (2a), (3) (to get rid of the f's) }

$P\cdot u \Rightarrow Q\cdot u$

□

The above proof is shorter and simpler than A.J.M. van Gasteren's proof. It may very well be that formula (2) is the culprit: it is the only formula in the theorem in which (elements of) both V and C occur. By rewriting it into (2a) $\wedge$ (2b) we have uncoupled V and C : now the whole proof can be carried out in terms of V . The principle of generalised mathematical induction takes care of the coupling, via t , of V and C . Thus, it contributes to a better modularisation of the proof.

reference

[0] A.J.M. van Gasteren
On the shape of mathematical arguments
Ph.D. thesis, Eindhoven University of Technology, 1988.

□

Eindhoven, 21 september 1989
Rob Hoogerwoord
department of mathematics and computing science
Eindhoven University of Technology
P.O. Box 513
5600 MB Eindhoven