Designing a Calculational Proof of Cantor's Theorem

Edsger W. Dijkstra and Jayadev Misra

0 Cantor's Diagonalization

The one purpose of this little Note is to show that formal arguments need not be lengthy at all; on the contrary, they are often the most compact rendering of the argument. Its other purpose is to show the strong heuristic guidance that is available to us when we design such calculational proofs in sufficiently small, explicit steps. We illustrate our approach on Georg Cantor's classic diagonalization argument [chosen because, at the time, it created a sensation].

Cantor's purpose was to show that any set S is *strictly* smaller than its powerset $\wp S$ (i.e., the set of all subsets of S). Because of the 1-1 correspondence between the elements of S and its singleton subsets, which are elements of $\wp S$, S is not larger than $\wp S$, and our proof can now be focussed on the "strictly", i.e., we have to show that there is no 1-1 correspondence between S and $\wp S$. We can confine ourselves to non-empty S.

1 Proof Format and Notation

Eventually we present our proof in a format, due to W.H.J. Feijen, in which consecutive proof stages are separated by a connective and a justification. Thus,

$$\begin{array}{ll} & p \\ \Rightarrow & \{\mathrm{J}\} \\ & q \\ \equiv & \{\mathrm{M}\} \\ & r \end{array}$$

would show a proof of $p \Rightarrow r$ in which J justifies the conclusion q from p, while M explains why q and r are equivalent. In our proof we use $\equiv$ and $\Leftarrow$, the latter connective being the converse of $\Rightarrow$, i.e., $(p \Rightarrow q) \equiv (q \Leftarrow p)$.

In writing quantified formulae, we use the angle brackets, $\langle\rangle$, to delineate the scope of the dummy, and the double colon, ::, to separate the dummy from the quantified term, as in $\langle \forall x :: p.x \rangle$. Function application, as in the preceding "$p.x$", is denoted explicitly by an infix dot.

Besides "substituting equals for equals", we use the Rule of Instantiation, viz., that for any expression y in the range of the dummy x

$$\langle \forall x :: p.x \rangle \Rightarrow p.y \ .$$

Twice we use it in its contrapositive form

$$\langle \exists x :: q.x \rangle \Leftarrow q.y \ .$$

In the context of the latter rule, expression y is often referred to as the *witness* for x. We write "$x := y$" in a justification to denote that x is to be instantiated by y.

Type declarations consist of identifier and type (expression), separated by a colon. In what follows, x, Y, F, g are of the types

$$x\colon S,\ Y\colon \wp S,\ F\colon S \to \wp S,\ g\colon \wp S \to S \ ,$$

while the constants $id\colon S \to S$ and $ID\colon \wp S \to \wp S$ denote the identity functions on S and $\wp S$ respectively. When x or Y are used as dummies, the range of the quantification is understood to extend over all elements of their type. Examples of well-typed boolean expressions are: $F.x = Y,\ g.Y = x,\ F.(g.Y) = Y,\ g.(F.x) = x,\ x \in Y,\ g.Y \in Y,\ x \in F.x,\ g.Y \in F.x$, etc.

2 The Design of the Proof

We propose to prove the absence of a 1-1 correspondence between S and $\wp S$ by showing that for any F, g of the appropriate types

$$(0) \quad ID \neq F \circ g \ .$$

Remark We have already made a choice, since $id \neq g \circ F$ would have implied the absence of a 1-1 correspondence as well, but the trouble with the latter is that it is not a theorem, because F, g satisfying $F.x = \{x\}$ and $g.\{x\} = x$ provide a counterexample.

Our proof displays a sequence of boolean expressions, starting with (0) and ending with *true*, such that each expression implies its predecessor in the sequence. To construct the successor of (0) we propose to apply the definition of function (in)equality and record that (0) is equivalent to

$$(1) \quad \langle \exists Y :: ID.Y \neq (F \circ g).Y \rangle \ .$$

This wasn't the only choice possible, since $(p \neq q) \Leftarrow (h.p \neq h.q)$ for *any* function h, but the point is that, on our way from (0) to *true*, we must get rid of the constants ID and $\circ$, and we usually eliminate constants by appealing to their defining properties. Since both ID and $\circ$ are defined in terms of function application, it stands to reason to apply both sides of (0) to some Y. Our remaining task is now to come up with a set-valued expression that can serve as a witness for Y.

We now eliminate ID and $\circ$ by applying their definitions, i.e., we record that (1) is equivalent to

(2) $\langle\exists Y :: Y \neq F.(g.Y)\rangle$,

and, doing justice to the fact that we are comparing subsets of S, we record that (2) is equivalent to

(3) $\langle\exists Y :: \langle\exists x :: x \in Y \not\equiv x \in F.(g.Y)\rangle\rangle$.

Remark The last two steps—elimination of *ID*, $\circ$ and introduction of x—commute and could be done in the other order, but for the sake of brevity it is better to simplify first.

The inner existential quantification we have just introduced can be eliminated immediately by the instantiation $x := g.Y$ and we record that (3) is implied by

(4) $\langle\exists Y :: g.Y \in Y \not\equiv g.Y \in F.(g.Y)\rangle$.

This last implication depends on the monotonicity of existential quantification. This step was bold—it is our first strengthening in the sequence—and opportunistic: (i) we chose to instantiate x because at this stage we had no candidate witness for Y, and (ii) for better or for worse, we instantiated with $g.Y$ because we did not have much choice since $g.Y$ is the *only* element of S we can identify (and that is known to exist). Via the same instantiation, $x := g.Y$, we can now eliminate g and record that—again thanks to monotonicity of $\exists$—(4) is implied by

(5) $\langle\exists Y :: \langle\forall x :: x \in Y \equiv x \notin F.x\rangle\rangle$,

where we have moved the negation to the right-hand side.

We could have performed the same transformation on (2), which would have yielded

$$\langle\exists Y :: \langle\forall x :: Y \neq F.x\rangle\rangle \ ,$$

but this would not have helped in the construction of a witness for Y. With (5) we are in a much better position because thanks to set theory—which enables us to construct set-valued expressions—we can now rewrite (5) as the equivalent

(6) $\langle\exists Y :: Y = \{x|\ x \notin F.x\}\rangle$.

Now the instantiation $Y := \{x|\ x \notin F.x\}$ stares us in the face and we accordingly record that (6) is implied by

(7) $\{x|\ x \notin F.x\} = \{x|\ x \notin F.x\}$,

which, because of the reflexivity of $=$, is equivalent to

(8) *true.*

3 A Summary of the calculation

We have included the heuristics in our argument for educational reasons. In a document written for another purpose one would omit them. By way of illustration we present the proof in Feijen's format, without the heuristics and incorporating somewhat larger steps:

$$
\begin{array}{ll}
 & ID \neq F \circ g \\
\equiv & \{\text{definition of } ID,\ \neq,\ \circ\} \\
 & \langle \exists Y :: Y \neq F.(g.Y) \rangle \\
\Leftarrow & \{(p \neq q) \Leftarrow (h.p \neq h.q)\} \\
 & \langle \exists Y :: g.Y \in Y \not\equiv g.Y \in F.(g.Y) \rangle \\
\Leftarrow & \{\text{instantiation } x := g.Y\} \\
 & \langle \exists Y :: \langle \forall x :: x \in Y \equiv x \notin F.x \rangle \rangle \\
\equiv & \{\text{set theory: consider } \{x|\ x \notin F.x\} \text{ as witness for } Y\} \\
 & \mathit{true}
\end{array}
$$

This presents the calculation in a degree of detail with which we expect most mathematicians to be perfectly happy most of the time. We did not mention in our hints the monotonicity of $\exists$ because we consider it part of the predicate calculus, which we feel free to use here without mention. We would like the reader to appreciate that we have combined (i) brevity, (ii) completeness—in the sense that the hints delineate where the justification is to be found—and (iii) the constructive path that leads to the "invention" $\{x|\ x \notin F.x\}$.

Comments

There are several reasons for liking the calculational proof style. It provides heuristic guidance—as shown in our construction of the required set—and calculational proofs tend to be very compact and at the same time highly readable in the sense that they can be fully checked without pen and paper. More importantly, the design of calculational proofs is an art that seems eminently teachable.

Acknowledgement Credit for the format in which we presented our calculational proof is due to W.H.J. Feijen. This format turned out to be an essential ingredient.

The University of Texas at Austin, Austin, TX 78712-1188
dijkstra@cs.utexas.edu
misra@cs.utexas.edu