Copyright Notice

The manuscript

EWD 1294: Designing a calculational proof of Cantor's theorem

has been accepted for publication in

Amercan Mathemarical Monthly

Copyright © The Mathematical Association of America, 2000. All rights reserved.

Designing a calculational proof of Cantor's Theorem

Edsger W. Dijkstra and Jayadev Misra
Department of Computer Sciences
The University of Texas at Austin
Austin, TX 78712-1188
USA

0 Cantor's Diagonalization

The one purpose of this little note is to show that formal proofs 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 <u>strictly</u> smaller than its powerset $\mathcal{P}S$ (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 $\mathcal{P}S$, S is not larger than $\mathcal{P}S$, 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 $\mathcal{P}S$. We can confine ourselves to non-empty S.

1 Proof Format and Notation

Eventually we shall 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. For instance,

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

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 shall use $\equiv$ and $\Leftarrow$, the latter connective being the converse of $\Rightarrow$, i.e., $(p \Leftarrow q) \equiv (q \Rightarrow p)$.

In writing quantified formulae, we use the angle brackets $\langle\rangle$ to delineate the scope of the dummy, 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

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

Twice we will use it in its contrapositive form

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

[In the context of the latter rule, expression y is often referred to as "the witness" for x .]

In what follows, x, Y, F, g are of the types

$$x : \mathcal{S} \;,\quad Y : \mathcal{PS} \;,\quad F : \mathcal{S} \rightarrow \mathcal{PS} \;,\quad g : \mathcal{PS} \rightarrow \mathcal{S} \;,$$

while the constants $id : \mathcal{S} \rightarrow \mathcal{S}$ and $ID : \mathcal{PS} \rightarrow \mathcal{PS}$ denote the identity functions on $\mathcal{S}$ and on $\mathcal{PS}$ 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 $\mathcal{S}$ and $\mathcal{PS}$ 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. [Any F, g satisfying $F.x = \{x\}$ and $g.\{x\} = x$ provide a counterexample.] (End of Remark.)

Our proof will display a sequence of boolean expressions, starting with (0), ending with *true*, and such that each next 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) $\quad \langle \exists Y :: ID.Y \neq (F\circ g).Y \rangle$.

Note that this wasn't our only choice as $p \neq q \Leftarrow h.p \neq h.q$ for *any* h, but the point is that, on our way from (0) to *true*, we have to 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 stood 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.

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

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

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

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

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. (End of Remark.)

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

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

[Note that 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 <u>only</u> element of $\mathcal{S}$ we can identify (and which 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

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

[In passing we have moved the negation to the right-hand side.]

Note that 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 us 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

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

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

$$(7) \qquad \{x \mid x \notin F.x\} = \{x \mid x \notin F.x\} \quad ,$$

which, because of the reflexity of = , equivales

(8) $\underline{\text{true}}$.

3 A summary of the calculation

In the above we have included the heuristics 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.

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

The above 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" $\{x \mid x \notin F.x\}$.

* * *

There are several reasons for liking the calculational proof style. It provides heuristic guidance –as shown above in the 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.

Biographical Information Dr. Edsger W. Dijkstra is Professor Emeritus in the Department of Computer Sciences at the University of Texas at Austin. Dr. J. Misra is Professor in the same department.