Courtesy Georg Cantor and Jayadev Misra

The purpose of Cantor's "Diagonalverfahren" was to show that any set S is strictly 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 "strictly", i.e. we have to show that there exists no 1-1 correspondence between S and $\mathcal{P}S$. We can confine ourselves to the case of non-empty S.

This note is devoted to two calculational proofs designed by Jayadev Misra, each interesting for its own reason. We shall use lower case letters to denote elements of S and functions with such values, and upper case letters for elements of $\mathcal{P}S$ and functions with such values. Consequently we distinguish between two identity functions, viz. id and ID. Functions F, g are of the types

(0) $F:\ S \to \mathcal{P}S$ and $g: \mathcal{P}S \to S$.

Misra's first proof. We assume g to be a 1-1 function and derive a contradiction.

For function g being 1-1 we use in this proof the characterization

(1) $\langle \forall Y, Z :: Y = Z \equiv g.Y = g.Z \rangle$,

and in order to formulate the contradiction we define set X by

(2) $\langle \forall y :: y \in X \equiv \langle \exists Z : y = g.Z : y \notin Z \rangle\rangle$;

and now we calculate

$$
\begin{array}{ll}
 & g.X \in X \\
\equiv & \quad \{ (2) \text{ with } y := g.X \} \\
 & \langle \exists Z : g.X = g.Z : g.X \notin Z \rangle \\
\equiv & \quad \{ (1) \text{ with } Y, Z := X, Z \} \\
 & \langle \exists Z : X = Z : g.X \notin Z \rangle \\
\equiv & \quad \{ \text{1-point rule} \} \\
 & g.X \notin X
\end{array}
$$,

which yields the contradiction promised. (End of Misra's first proof.)

The disappointing thing about the above presentation is that the introduction of X by (2) comes as a great, big rabbit. (Misra's second proof admits a heuristically nicer presentation.) It is an interesting proof because in more than one way it shows the power of well-designed calculations. Firstly I ask you to envisage the complications if we hadn't had the equivalence at our disposal, and had to rewrite it á la Gentzen as mutual implication. Secondly I would like to point out that we could have replaced the existential quantifier $\exists$ in (2) by the universal quantifier $\forall$, for the 1-point rule works equally well for both: for someone used to the manipulation of uninterpreted formulae, the change is irrelevant, for someone who insists on an awareness of what the formulae he manipulates "mean", the change would result in a totally new proof.

* * *

<u>Misra's second proof</u>. We shall show the absence of a 1-1 correspondence between $\mathcal{S}$ and $\mathcal{PS}$ by showing the absence of a pair of functions F, g typed as in (0) and such that F and g are the inverses of each other, and we shall do so by showing $F \circ g \neq ID$ for any F, g of such types.

We calculate for any F, g typed as in (0)

$$
\begin{array}{ll}
 & F \circ g \neq ID \\
\equiv & \quad \{\text{definition of (in)equality of functions}\} \\
 & \langle \exists X :: \ (F \circ g).X \neq ID.X \rangle \\
\equiv & \quad \{\text{definition of } \circ \text{ and of } ID\} \\
 & \langle \exists X :: \ F.(g.X) \neq X \rangle \\
\Leftarrow & \quad \{\text{Leibniz, see Note below}\} \\
 & \langle \exists X :: \ g.X \in F.(g.X) \not\equiv g.X \in X \rangle
\end{array}
$$

$$\langle \exists X :: g.X \in F.(g.X) \not\equiv g.X \in X \rangle$$
$\Leftarrow$ { instantiation $z := g.X$ }
$$\langle \exists X :: \langle \forall z :: z \in F.z \not\equiv z \in X \rangle \rangle$$
$\Leftarrow$ { with $X := \{z \mid z \notin F.z\}$ as witness }
true

<u>Note</u> The usual form of Leibniz's Principle — "substituting equals for equals" — is

$$x = y \Rightarrow f.x = f.y \quad ,$$

but its contra-positive

$$f.x \neq f.y \Rightarrow x \neq y$$

— "different values implies different arguments" — should be known as well, as it is a standard way of concluding difference. Applying for some z $(z \in S)$ to both sides the operator "$z \in$" should not come as a surprise because somewhere in the argument we <u>have</u> to take into account that the elements of $\mathcal{P}S$ are the subsets of S. That in this case we have chosen $g.X$ for z should not come as a surprise either because in the terminology available, $g.X$ is the only element of S we can identify.

It could very well be this step that is responsible for the "surprise value" of Cantor's argument. If we wish to view the expression $(z \in A)$ as result of a function application, the usual way of doing so is as $(\_ \in A).z$, i.e. applying A's membership function to z , but here we do it as $(z\in \_).A$, i.e. applying z's "containership function" to A , and the membership function is (for good reasons) much better known than the containership function. (End of Note.)

One can try to prove $g \circ F \neq id$ instead, but than one gets stuck.

Austin, 17 October 1999

prof. dr Edsger W. Dijkstra
Department of Computer Sciences
The University of Texas at Austin
Austin, TX 78712-1188
USA