Let f and g be functions and let C and D be propositions. By definition,

$$\begin{array}{l} \quad y \\ = \quad \langle \quad f : C \quad \rangle \\ \quad z \\ = \quad \langle \quad g : D \quad \rangle \\ \quad x \end{array} \quad : \quad C \wedge D \;\Rightarrow\; y = (f \cdot g).x$$

If we let

$$\begin{array}{l} \quad y \\ = \quad \langle \quad f : C \quad \rangle \\ \quad x \end{array} \quad = \quad \begin{array}{l} \quad y \\ = \quad \langle \quad f : C \quad \rangle \\ \quad z \\ = \quad \langle \quad id : \textbf{true} \quad \rangle \\ \quad x \end{array}$$

we can see that

$$\begin{array}{l} \quad y \\ = \quad \langle \quad f : C \quad \rangle \\ \quad x \end{array} \quad \in \quad C \;\Rightarrow\; y = f.x$$

We will use this proof format attain the following:

Objective

The design of a demultiplexor chip together with a proof of its correctness.

NTT5 Introduction

We wish to construct *dmux*, a so-called *demultiplexor*.

dmux inputs a pair of booleans and outputs a pair of booleans i.e.

$$dmux : 2 \to 2$$

and is specified by

$$[\![dmux]\!].[s, in] \triangleq [s \wedge in, \neg s \wedge in]$$

In order to construct *dmux*, we have the following chips at our disposal:

- nand $\bar{\wedge}\mathbb{C}$, not $\neg\mathbb{C}$, and $\wedge\mathbb{C}$, or $\vee\mathbb{C}$, xor $\not\equiv\mathbb{C}$
- *mux*.

Hence we calculate:

$$
\begin{array}{ll}
 & [s \wedge in, \neg s \wedge in] \\
= & \quad \langle \quad [\![second\ \neg\mathbb{C}]\!] : [\![second\ f]\!].[a,b] = [a, [\![f]\!].b] \quad \rangle \\
 & [s \wedge in, s \wedge in] \\
= & \quad \langle \quad [\![fork\nwarrow\!\!\searrow]\!] : [\![fork\nwarrow\!\!\searrow\ f]\!].[a] = [a,a] \quad \rangle \\
 & [s \wedge in] \\
= & \quad \langle \quad [\![\wedge\mathbb{C}]\!] : [\![\wedge\mathbb{C}]\!].[a,b] = [a \wedge b] \quad \rangle \\
 & [s, in]
\end{array}
$$

Recalling that

$$\left[\ [\![f\ \rangle\!\rangle\ g]\!] = [\![g]\!] \cdot [\![f]\!]\ \right]$$

we arrive at our final program:

$$dmux \triangleq \wedge\mathbb{C}\ \rangle\!\rangle\ fork\nwarrow\!\!\searrow\ \rangle\!\rangle\ second\ \neg\mathbb{C}$$