352 (building 1/2) Suppose we can flip a coin, but we suspect that the coin may be biased. Let us say that the probability of landing on its head is p . What we want is a coin with probability 1/2 of landing on its head. Here's one way to create what we want. Flip the coin twice. If the outcomes differ, use the first outcome. If the outcomes are the same, repeat the experiment, until the two outcomes differ, and then use the first outcome of the first pair that differed. Prove that this procedure works, and find out how long it takes.

After trying the question, scroll down to the solution.

§ Formally, we want the result

$\textbf{if } 1/2 \textbf{ then } x'=\mathit{head} \textbf{ else } x'=\mathit{tail} \textbf{ fi}$

The procedure apparently achieves slightly more:

$\textbf{if } 1/2 \textbf{ then } x'=\mathit{head} \wedge y'=\mathit{tail} \textbf{ else } x'=\mathit{tail} \wedge y'=\mathit{head} \textbf{ fi}$

which can be simplified to

$(x'\neq y')/2$

If we call that result R , then one understanding of the procedure is the program

```
$R \;=\;$ $\textbf{if } p \textbf{ then } x{:=}\ \mathit{head} \textbf{ else } x{:=}\ \mathit{tail} \textbf{ fi}.$
          $\textbf{if } p \textbf{ then } y{:=}\ \mathit{head} \textbf{ else } y{:=}\ \mathit{tail} \textbf{ fi}.$
          $\textbf{if } x{=}y \textbf{ then } R \textbf{ else } \mathit{ok} \textbf{ fi}$
```

Another understanding of the procedure is the program

```
$R \;=\;$ $\textbf{if } p \textbf{ then } x{:=}\ \mathit{head} \textbf{ else } x{:=}\ \mathit{tail} \textbf{ fi}.\ \ S$
$S \;=\;$ $\textbf{if } p \textbf{ then } y{:=}\ \mathit{head} \textbf{ else } y{:=}\ \mathit{tail} \textbf{ fi}.$
          $\textbf{if } x{=}y \textbf{ then } x{:=}\ y;\ \ S \textbf{ else } \mathit{ok} \textbf{ fi}$
```

The informal description could reasonably be understood either way; it is ambiguous. If two people with different understandings of the informal description of the procedure ask each other whether it is clear and understood, they will each say yes, and a long argument about whether the procedure produces the desired result will ensue. In contrast to that, the programs are unambiguous. With them we don't need to argue; we just calculate. Let me begin with the first one.

$$
\begin{aligned}
& \textbf{if } p \textbf{ then } x{:=}\ \mathit{head} \textbf{ else } x{:=}\ \mathit{tail} \textbf{ fi}.\\
& \textbf{if } p \textbf{ then } y{:=}\ \mathit{head} \textbf{ else } y{:=}\ \mathit{tail} \textbf{ fi}.\\
& \textbf{if } x{=}y \textbf{ then } R \textbf{ else } \mathit{ok} \textbf{ fi}\\
= \quad & \Sigma x'', y''\cdot\ \ (p\times(x''{=}\mathit{head}) + (1{-}p)\times(x''{=}\mathit{tail})) \times (p\times(y''{=}\mathit{head}) + (1{-}p)\times(y''{=}\mathit{tail}))\\
& \qquad\qquad \times ((x''{=}y'')\times(x'\neq y')/2 + (x''\neq y'')\times(x'{=}x'')\times(y'{=}y''))\\
= \quad & \ \ p^2\times(x'\neq y')/2\\
& +\ p\times(1{-}p)\times(x'{=}\mathit{head})\times(y'{=}\mathit{tail})\\
& +\ (1{-}p)\times p\times(x'{=}\mathit{tail})\times(y'{=}\mathit{head})\\
& +\ (1{-}p)^2\times(x'\neq y')/2\\
= \quad & (p^2 + 2\times p\times(1{-}p)\ \ +\ \ (1{-}p)^2) \times (x'\neq y')\ /\ 2\\
= \quad & (x'\neq y')\ /\ 2\\
= \quad & R
\end{aligned}
$$

For the timing, just put $t{:=}\ t{+}1$ before the recursive call, and add timing to specification R :

$$R \;=\; (x'\neq y') \times (t'{\ge}t) \times (p^2 + (1{-}p)^2)^{t'-t} \times p \times (1{-}p)$$

Here's the calculation.

$$
\begin{aligned}
& \textbf{if } p \textbf{ then } x{:=}\ \mathit{head} \textbf{ else } x{:=}\ \mathit{tail} \textbf{ fi}.\\
& \textbf{if } p \textbf{ then } y{:=}\ \mathit{head} \textbf{ else } y{:=}\ \mathit{tail} \textbf{ fi}.\\
& \textbf{if } x{=}y \textbf{ then } t{:=}\ t{+}1.\ \ (x'\neq y') \times (t'{\ge}t) \times (p^2 + (1{-}p)^2)^{t'-t} \times p \times (1{-}p) \textbf{ else } \mathit{ok} \textbf{ fi}\\
= \quad & \Sigma x'', y'', t''\cdot\\
& \qquad (p\times(x''{=}\mathit{head}) + (1{-}p)\times(x''{=}\mathit{tail})) \times (p\times(y''{=}\mathit{head}) + (1{-}p)\times(y''{=}\mathit{tail})) \times (t''{=}t)\\
& \quad \times\ (\ \ (x''{=}y'')\times(x'\neq y')\times(t'{\ge}t''{+}1)\times(p^2 + (1{-}p)^2)^{t'-t''-1}\times p\times(1{-}p)\\
& \qquad +\ (x''\neq y'')\times(x'{=}x'')\times(y'{=}y'')\times(t'{=}t'')\ )\\
= \quad & \ \ p^2\times(x'\neq y')\times(t'{\ge}t{+}1)\times(p^2 + (1{-}p)^2)^{t'-t-1}\times p\times(1{-}p)\\
& +\ p\times(1{-}p)\times(x'{=}\mathit{head})\times(y'{=}\mathit{tail})\times(t'{=}t)\\
& +\ (1{-}p)\times p\times(x'{=}\mathit{tail})\times(y'{=}\mathit{head})\times(t'{=}t)\\
& +\ (1{-}p)^2\times(x'\neq y')\times(t'{\ge}t{+}1)\times(p^2 + (1{-}p)^2)^{t'-t-1}\times p\times(1{-}p)\\
= \quad & \ \ \ (p^2 + (1{-}p)^2)\times(x'\neq y')\times(t'{\ge}t{+}1)\times(p^2 + (1{-}p)^2)^{t'-t-1}\times p\times(1{-}p)\\
& +\ p\times(1{-}p)\times(x'\neq y')\times(t'{=}t)\\
= \quad & (x'\neq y')\times(t'{\ge}t{+}1)\times(p^2 + (1{-}p)^2)^{t'-t}\times p\times(1{-}p)\ \ +\ \ p\times(1{-}p)\times(x'\neq y')\times(t'{=}t)\\
= \quad & (x'\neq y') \times (t'{\ge}t) \times (p^2 + (1{-}p)^2)^{t'-t} \times p \times (1{-}p)
\end{aligned}
$$

There was no need for an assumption that p differs from both 0 and 1 in either proof. But if p is either 0 or 1, the timing expression gives probability 0 to any finite value of t'. And if p is either 0 or 1 we can easily prove $t'=\infty$ (but we don't bother).

So the first program works. But the second program doesn't; it gives exactly the same result as a single flip of the coin. Here's the calculation. This time define

$$\begin{aligned} R \;&=\; \textbf{if } p \textbf{ then } x'=head \wedge y'=tail \textbf{ else } x'=tail \wedge y'=head \textbf{ fi} \\ &=\; p\times(x'=head)\times(y'=tail) + (1-p)\times(x'=tail)\times(y'=head) \end{aligned}$$

which is a single flip, and define

$$S \;=\; x'=x\neq y'$$

then the first equation is proved as follows:

$$\begin{aligned} & \textbf{if } p \textbf{ then } x{:=}\ head \textbf{ else } x{:=}\ tail \textbf{ fi}.\ \ S \\ = \quad & \textbf{if } p \textbf{ then } x{:=}\ head \textbf{ else } x{:=}\ tail \textbf{ fi}.\ \ x'=x\neq y' \\ = \quad & \textbf{if } p \textbf{ then } x{:=}\ head.\ \ x'=x\neq y' \textbf{ else } x{:=}\ tail.\ \ x'=x\neq y' \textbf{ fi} \\ = \quad & \textbf{if } p \textbf{ then } x'=head\neq y' \textbf{ else } x'=tail\neq y' \textbf{ fi} \\ = \quad & R \end{aligned}$$

and the second equation is proved as follows:

$$\begin{aligned} & \textbf{if } p \textbf{ then } y{:=}\ head \textbf{ else } y{:=}\ tail \textbf{ fi}. \\ & \textbf{if } x=y \textbf{ then } x{:=}\ y.\ \ S \textbf{ else } ok \textbf{ fi} \\ = \quad & \Sigma x'', y''\cdot \quad (p\times(x''=x)\times(y''=head) + (1-p)\times(x''=x)\times(y''=tail)) \\ & \qquad\qquad \times ((x''=y'')\times(x'=x'')\times(y'\neq y'') + (x''\neq y'')\times(x'=x'')\times(y'=y'')) \\ = \quad & \quad\ p \times ((x=head)\times(x'=x)\times(y'\neq head) + (x\neq head)\times(x'=x)\times(y'=head)) \\ & +\ \ (1-p) \times ((x=tail)\times(x'=x)\times(y'\neq tail) + (x\neq tail)\times(x'=x)\times(y'=tail)) \\ = \quad & \quad\ p \times ((x=head)\times(x'=x)\times(y'\neq x) + (x\neq head)\times(x'=x)\times(y'\neq x)) \\ & +\ \ (1-p) \times ((x=tail)\times(x'=x)\times(y'\neq x) + (x\neq tail)\times(x'=x)\times(y'\neq x)) \\ = \quad & (x'=x) \times (y'\neq x) \times (p\times((x=head) + (x\neq head)) \ \ + \ \ (1-p)\times((x=tail) + (x\neq tail))) \\ = \quad & (x'=x) \times (y'\neq x) \\ = \quad & S \end{aligned}$$