A File System

Using Z

Woodcock & Davies

A programming interface

We will model the programming interface to a file system. This is a list of operations upon the file system, complete with a description of their intended effects.

We will divide the operations into two groups: those that affect the data within a single file, and those that affect the file system as a whole.

File operations

- `read`: used to read a piece of data from a file
- `write`: used to write a piece of data to a file
- `add`: used to add a new piece of data to a file
- `delete`: used to delete a piece of data from a file

File system operations

- `create`: used to create a new file
- `destroy`: used to destroy an existing file
- `open`: used to make a file available for the reading and writing of data
- `close`: used to make a file unavailable for reading and writing

Files

$[Key, Data]$

File

$contents : Key \rightarrowtail Data$

Initialisation

FileInit

$File'$

read

$$
\begin{array}{l}
\textit{Read}_0 \\
\hline
\Xi \textit{File} \\
k? : \textit{Key} \\
d! : \textit{Data} \\
\hline
k? \in \operatorname{dom} \textit{contents} \\
d! = \textit{contents}\, k?
\end{array}
$$

write

$$
\begin{array}{l}
\textit{Write}_0 \\
\hline
\Delta \textit{File} \\
k? : \textit{Key} \\
d? : \textit{Data} \\
\hline
k? \in \operatorname{dom} \textit{contents} \\
\textit{contents}' = \textit{contents} \oplus \{k? \mapsto d?\}
\end{array}
$$

add

Add_0

$\Delta File$

$k? : Key$

$d? : Data$

delete

$Delete_0$

Key errors

$Report ::= \mathsf{keyInUse} \mid \mathsf{keyNotInUse} \mid \mathsf{okay}$

KeyError

$\Xi File$
$k? : Key$
$r! : Report$

KeyNotInUse

$KeyError$

$k? \notin \operatorname{dom} contents$
$r! = \mathsf{keyNotInUse}$

KeyInUse

$KeyError$

$k? \in \operatorname{dom} contents$
$r! = \mathsf{keyInUse}$

Success

Success

$r! : Report$

$r! = \mathsf{okay}$

$$Read \mathrel{\widehat{=}} (Read_0 \land Success) \lor KeyNotInUse$$
$$Write \mathrel{\widehat{=}} (Write_0 \land Success) \lor KeyNotInUse$$
$$Add \mathrel{\widehat{=}} (Add_0 \land Success) \lor KeyInUse$$
$$Delete \mathrel{\widehat{=}} (Delete_0 \land Success) \lor KeyNotInUse$$

Otherwise

$contents, contents' : Key \rightarrowtail\!\!\!\!\!\rightarrow Data$
$k? : Key$
$d! : Data$
$r! : Report$

$$
\begin{aligned}
&(\, k? \in \operatorname{dom} contents \land \\
&\quad d! = contents\, k? \land \\
&\quad contents' = contents \land \\
&\quad r! = \mathsf{okay}\,) \\
&\lor \\
&(\, k? \notin \operatorname{dom} contents \land \\
&\quad contents' = contents \land \\
&\quad r! = \mathsf{keyNotInUse}\,)
\end{aligned}
$$

File system

$[Name]$

System

$file : Name \rightarrowtail File$
$open : \mathbb{P}\, Name$

$open \subseteq \operatorname{dom} file$

Initialisation

SystemInit

$System'$

$file' = \varnothing$

Promotion

$$
\begin{array}{l}
\textit{Promote} \\
\hline
\Delta System \\
\Delta File \\
n? : Name \\
\hline
n? \in open \\
file\, n? = \theta File \\
file' = file \oplus \{n? \mapsto \theta File'\} \\
open' = open \\
\hline
\end{array}
$$

File operations

$$
\begin{aligned}
KeyRead_0 &\mathrel{\widehat{=}} \exists\, \Delta File \bullet Read \wedge Promote \\
KeyWrite_0 &\mathrel{\widehat{=}} \exists\, \Delta File \bullet Write \wedge Promote \\
KeyAdd_0 &\mathrel{\widehat{=}} \exists\, \Delta File \bullet Add \wedge Promote \\
KeyDelete_0 &\mathrel{\widehat{=}} \exists\, \Delta File \bullet Delete \wedge Promote
\end{aligned}
$$

File access

FileAccess

$\Delta System$

$n? : Name$

$n? \in \mathrm{dom}\, file$

$file' = file$

Open$_0$

FileAccess

$n? \notin open$

$open' = open \cup \{n?\}$

Closing a file

Close$_0$

FileAccess

$n? \in open$

$open' = open \setminus \{n?\}$

File management

FileManage

$\Delta System$

$n? : Name$

$open' = open$

Create$_0$

$FileManage$

$\exists\, FileInit' \bullet$

$\quad n? \notin \operatorname{dom} file \wedge$

$\quad file' = file \cup \{n? \mapsto \theta File'\}$

Destroying a file

Destroy$_0$

More reports

$$Report ::= \mathsf{keyInUse} \mid \mathsf{keyNotInUse} \mid \mathsf{okay} \mid \mathsf{fileExists} \mid \mathsf{fileDoesNotExist} \mid \mathsf{fileIsOpen} \mid \mathsf{fileIsNotOpen}$$

File errors

FileError

$\Xi System$
$n? : Name$
$r! : Report$

FileExists

$FileError$

$n? \in \mathrm{dom}\, file$
$r! = \mathsf{fileExists}$

File system operations

$$KeyRead \mathrel{\widehat{=}} KeyRead_0 \lor FileIsNotOpen \lor FileDoesNotExist$$

$$KeyWrite \mathrel{\widehat{=}} KeyWrite_0 \lor FileIsNotOpen \lor FileDoesNotExist$$

$$KeyAdd \mathrel{\widehat{=}} KeyAdd_0 \lor FileIsNotOpen \lor FileDoesNotExist$$

$$KeyDelete \mathrel{\widehat{=}} KeyDelete_0 \lor FileIsNotOpen \lor FileDoesNotExist$$

$$Open \mathrel{\widehat{=}} (Open_0 \land Success) \lor FileIsOpen \lor FileDoesNotExist$$

$$Close \mathrel{\widehat{=}} (Close_0 \land Success) \lor FileIsNotOpen \lor FileDoesNotExist$$

$$Create \mathrel{\widehat{=}} (Create_0 \land Success) \lor FileExists$$

$$Destroy \mathrel{\widehat{=}} (Destroy_0 \land Success) \lor FileDoesNotExist \lor FileIsOpen$$

Formal analysis

- consistency of requirements
- operation preconditions

Initialisation theorem

$$\exists\, System' \bullet SystemInit$$

Proof

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\varnothing \in \mathbb{P}\, Name} \quad \dfrac{}{\varnothing \subseteq \operatorname{dom} \varnothing}}{\exists\, open' : \mathbb{P}\, Name \bullet open' \subseteq \operatorname{dom} \varnothing}\,[\exists\text{–intro}] \quad \dfrac{}{\varnothing \in Name \rightarrowtail\!\!\!\!\!\rightarrow File}}{\exists\, file' : Name \rightarrowtail\!\!\!\!\!\rightarrow File;\ open' : \mathbb{P}\, Name \mid open' \subseteq \operatorname{dom} file' \bullet file' = \varnothing}\,[\text{one-point}]}{\exists\, System' \bullet SystemInit}\,[\text{definition}]$$

Precondition

$$KeyRead \mathrel{\widehat{=}} KeyRead_0 \lor FileDoesNotExist \lor FileIsNotOpen$$

$$\begin{aligned} &\operatorname{pre} KeyRead = \\ &\qquad \operatorname{pre} KeyRead_0 \lor \operatorname{pre} FileDoesNotExist \lor \operatorname{pre} FileIsNotOpen \end{aligned}$$

pre *FileIsNotOpen*

$$
\begin{array}{l}
\mathit{System} \\
n? : \mathit{Name} \\
\hline
\exists\, r! : \mathit{Report} \bullet \\
\quad n? \notin \mathit{open} \land \\
\quad n? \in \operatorname{dom} \mathit{file} \land \\
\quad r! = \mathsf{fileIsNotOpen}
\end{array}
$$

pre *KeyRead*

$$\mathit{KeyRead}_0 \mathrel{\widehat{=}} \exists\, \Delta \mathit{File} \bullet \mathit{Read} \land \mathit{Promote}$$

$$\operatorname{pre} \mathit{KeyRead}_0 = \exists\, \mathit{Local} \bullet \operatorname{pre} \mathit{Read} \land \operatorname{pre} \mathit{Promote}$$

$$\operatorname{pre} \mathit{KeyRead} \Leftrightarrow \mathit{true}$$

Result

Operation		Precondition
KeyRead	$KeyRead_0$	$n? \in open$
	FileIsNotOpen	$n? \in (\mathrm{dom}\, file) \setminus open$
	FileDoesNotExist	$n? \notin \mathrm{dom}\, file$
	KeyRead	*true*