

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 ↔ Data

Initialisation

FileInit —————
File' —————

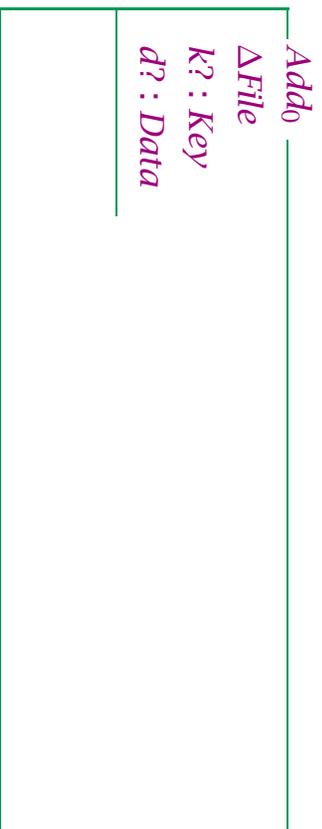
read

$Read_0$
 $EFile$
 $k? : Key$
 $d! : Data$
 $k? \in \text{dom contents}$
 $d! = \text{contents } k?$

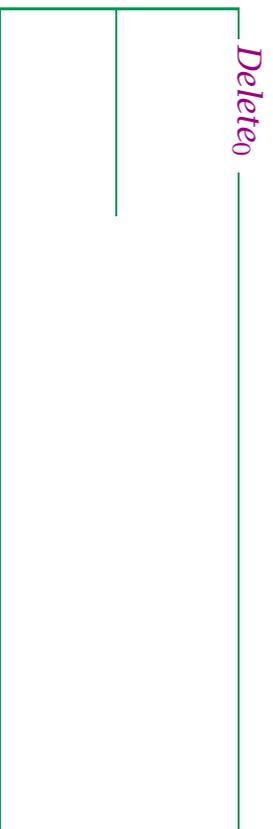
write

$Write_0$
 $\Delta File$
 $k? : Key$
 $d? : Data$
 $k? \in \text{dom contents}$
 $\text{contents}' = \text{contents} \oplus \{k? \mapsto d?\}$

add



delete



Key errors

Report ::= keyInUse | keyNotInUse | okay

KeyError
EFile
k? : Key
r! : Report

KeyNotInUse
KeyError
k? ∉ dom contents
r! = keyNotInUse

KeyInUse
KeyError
k? ∈ dom contents
r! = keyInUse

Success*Success**r1 : Report**r1 = okay**Read* $\hat{=}$ (*Read*₀ \wedge *Success*) \vee *KeyNotInUse**Write* $\hat{=}$ (*Write*₀ \wedge *Success*) \vee *KeyNotInUse**Add* $\hat{=}$ (*Add*₀ \wedge *Success*) \vee *KeyInUse**Delete* $\hat{=}$ (*Delete*₀ \wedge *Success*) \vee *KeyNotInUse***Otherwise***contents, contents' : Key \leftrightarrow Data**k? : Key**d! : Data**r1 : Report* $(k? \in \text{dom } \textit{contents} \wedge$ $d! = \textit{contents } k? \wedge$ $\textit{contents}' = \textit{contents} \wedge$ $r1 = \textit{okay})$ \vee $(k? \notin \text{dom } \textit{contents} \wedge$ $\textit{contents}' = \textit{contents} \wedge$ $r1 = \textit{keyNotInUse})$

File system

[Name]

System

file : Name \leftrightarrow File

open : \mathbb{P} Name

open \subseteq dom *file*

Initialisation

SystemInit

System'

file' = \emptyset

Promotion

$Promote$ $\Delta System$ $\Delta File$ $n? : Name$ $n? \in open$ $File\ n? = \emptyset File$ $file' = file \oplus \{n? \mapsto \emptyset File'\}$ $open' = open$

File operations

$$KeyRead_0 \cong \exists \Delta File \bullet Read \wedge Promote$$

$$KeyWrite_0 \cong \exists \Delta File \bullet Write \wedge Promote$$

$$KeyAdd_0 \cong \exists \Delta File \bullet Add \wedge Promote$$

$$KeyDelete_0 \cong \exists \Delta File \bullet Delete \wedge Promote$$

File access

<i>FileAccess</i>
Δ System
$n? : \text{Name}$
$n? \in \text{dom file}$
$\text{file}' = \text{file}$

<i>Open₀</i>
<i>FileAccess</i>
$n? \notin \text{open}$
$\text{open}' = \text{open} \cup \{n?\}$

Closing a file

<i>Close₀</i>
<i>FileAccess</i>
$n? \in \text{open}$
$\text{open}' = \text{open} \setminus \{n?\}$

File management

FileManage

Δ System

$n? : \text{Name}$

$\text{open}' = \text{open}$

*Create*₀

FileManage

$\exists \text{FileInit}' \bullet$

$n? \notin \text{dom } \text{file} \wedge$

$\text{file}' = \text{file} \cup \{n? \mapsto \emptyset \text{File}'\}$

Destroying a file

*Destroy*₀

More reports

Report ::= keyInUse | keyNotInUse | okay |
fileExists | fileDoesNotExist |
fileIsOpen | fileIsNotOpen

File errors

FileError
ESystem
n? : Name
r! : Report

FileExists
FileError
n? ∈ dom *file*
r! = fileExists

File system operations

$KeyRead \hat{=} KeyRead_0 \vee FileIsNotOpen \vee$
 $FileDoesNotExist$
 $KeyWrite \hat{=} KeyWrite_0 \vee FileIsNotOpen \vee$
 $FileDoesNotExist$
 $KeyAdd \hat{=} KeyAdd_0 \vee FileIsNotOpen \vee$
 $FileDoesNotExist$
 $KeyDelete \hat{=} KeyDelete_0 \vee FileIsNotOpen \vee$
 $FileDoesNotExist$

$Open \hat{=} (Open_0 \wedge Success) \vee FileIsOpen \vee$
 $FileDoesNotExist$
 $Close \hat{=} (Close_0 \wedge Success) \vee FileIsNotOpen \vee$
 $FileDoesNotExist$
 $Create \hat{=} (Create_0 \wedge Success) \vee$
 $FileExists$
 $Destroy \hat{=} (Destroy_0 \wedge Success) \vee FileDoesNotExist \vee$
 $FileIsOpen$

Formal analysis

- consistency of requirements
- operation preconditions

Initialisation theorem

\exists *System'* • *SystemInit*

Proof

$$\begin{array}{c}
 \frac{\frac{\frac{\emptyset \in \mathbb{P} \text{ Name} \quad \emptyset \subseteq \text{dom } \emptyset}{\exists \text{ open}' : \mathbb{P} \text{ Name} \bullet}}{\emptyset \in \text{Name} \leftrightarrow \text{File}} \quad \text{open}' \subseteq \text{dom } \emptyset}{\exists \text{ file}' : \text{Name} \leftrightarrow \text{File}; \text{open}' : \mathbb{P} \text{ Name} \mid} \\
 \text{open}' \subseteq \text{dom file}' \bullet \text{file}' = \emptyset \\
 \frac{}{\exists \text{ System}' \bullet \text{SystemInit}} \quad \text{[definition]}
 \end{array}$$

[∃-intro] [one-point]

Precondition

$$\begin{array}{l}
 \text{KeyRead} \hat{=} \text{KeyRead}_0 \vee \text{FileDoesNotExist} \vee \text{FileIsNotOpen} \\
 \text{pre KeyRead} = \\
 \text{pre KeyRead}_0 \vee \text{pre FileDoesNotExist} \vee \text{pre FileIsNotOpen}
 \end{array}$$

pre FileIsNotOpen

<i>System</i> <i>n?</i> : Name <hr/> $\exists r^! : \text{Report} \bullet$ $n? \notin \text{open} \wedge$ $n? \in \text{dom } \textit{file} \wedge$ $r^! = \text{fileIsNotOpen}$

pre KeyRead

$$\textit{KeyRead}_0 \hat{=} \exists \Delta \textit{File} \bullet \textit{Read} \wedge \textit{Promote}$$

$$\textit{pre KeyRead}_0 = \exists \textit{Local} \bullet \textit{pre Read} \wedge \textit{pre Promote}$$

$$\textit{pre KeyRead} \Leftrightarrow \textit{true}$$

Result

Operation	Precondition
<i>KeyRead</i>	$n? \in \textit{open}$
<i>KeyRead₀</i>	$n? \in (\textit{dom file}) \setminus \textit{open}$
<i>FileIsNotOpen</i>	$n? \notin \textit{dom file}$
<i>FileDoesNotExist</i>	<i>true</i>
<i>KeyRead</i>	<i>true</i>