



# Kent Academic Repository

**Stepney, Susan, Cooper, David and Woodcock, Jim (2000) *An Electronic Purse: Specification, Refinement and Proof*. Technical report. Oxford University**

## Downloaded from

<https://kar.kent.ac.uk/22009/> The University of Kent's Academic Repository KAR

## The version of record is available from

## This document version

UNSPECIFIED

## DOI for this version

## Licence for this version

UNSPECIFIED

## Additional information

Technical Monograph PRG-126 ISBN 0-902928-41-4 July 2000 Oxford University Computing Laboratory Programming Research Group Wolfson Building Parks Road Oxford OX1 3QD England

## Versions of research works

### Versions of Record

If this version is the version of record, it is the same as the published version available on the publisher's web site. Cite as the published version.

### Author Accepted Manuscripts

If this document is identified as the Author Accepted Manuscript it is the version after peer review but before type setting, copy editing or publisher branding. Cite as Surname, Initial. (Year) 'Title of article'. To be published in *Title of Journal*, Volume and issue numbers [peer-reviewed accepted version]. Available at: DOI or URL (Accessed: date).

## Enquiries

If you have questions about this document contact [ResearchSupport@kent.ac.uk](mailto:ResearchSupport@kent.ac.uk). Please include the URL of the record in KAR. If you believe that your, or a third party's rights have been compromised through this document please see our [Take Down policy](https://www.kent.ac.uk/guides/kar-the-kent-academic-repository#policies) (available from <https://www.kent.ac.uk/guides/kar-the-kent-academic-repository#policies>).

**AN ELECTRONIC PURSE**  
**Specification, Refinement, and Proof**

by

Susan Stepney  
David Cooper  
Jim Woodcock



Oxford University Computing Laboratory  
Programming Research Group

**AN ELECTRONIC PURSE**  
**Specification, Refinement, and Proof**

by

Susan Stepney  
David Cooper  
Jim Woodcock

Technical Monograph PRG-126  
ISBN 0-902928-41-4

July 2000

Oxford University Computing Laboratory  
Programming Research Group  
Wolfson Building  
Parks Road  
Oxford OX1 3QD  
England

Copyright © 2000 Logica UK Ltd

Oxford University Computing Laboratory  
Software Engineering Centre  
Wolfson Building  
Parks Road  
Oxford OX1 3QD  
England

email: stepneys@logica.com  
cooperd@praxis-cs.co.uk  
Jim.Woodcock@comlab.ox.ac.uk

---

## Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	The application	1
1.2	Overview of model and proof structure	3
1.3	Rationale for model structure	5
1.4	Rationale for proof structure	6
1.5	Status	7
<b>I</b>	<b>Models</b>	<b>9</b>
<b>2</b>	<b>SPs</b>	<b>11</b>
2.1	Introduction	11
2.2	Abstract model SPs	11
2.3	Concrete model SPs	13
2.4	SPs and the models	13
<b>3</b>	<b><math>\mathcal{A}</math> model</b>	<b>17</b>
3.1	Introduction	17
3.2	The abstract state	17
3.3	Secure operations	18
3.4	Abstract initial state	21
3.5	Abstract finalisation	22
<b>4</b>	<b><math>\mathcal{B}</math> model, purse</b>	<b>23</b>
4.1	Overview	23
4.2	Status	23

4.3	Message Details	23
4.4	Clear Exception Log Validation	25
4.5	Messages	26
4.6	A concrete purse	26
4.7	Single Purse operations	28
4.8	Invisible operations	28
4.9	Value transfer operations	30
4.10	Exception logging operations	35
<b>5</b>	<b><math>\mathcal{B}</math> model, world</b>	<b>39</b>
5.1	The world	39
5.2	Auxiliary definitions	40
5.3	Constraints on the ether	44
5.4	Framing schema	47
5.5	Ignore, Increase and Abort	49
5.6	Promoted operations	49
5.7	Operations at the world level only	50
5.8	Forging messages	52
5.9	The complete protocol	53
<b>6</b>	<b><math>\mathcal{B}</math> initial, final</b>	<b>55</b>
6.1	Initialisation	55
6.2	Finalisation	56
<b>7</b>	<b><math>\mathcal{C}</math> model</b>	<b>59</b>
7.1	Concrete World State	59
7.2	Framing Schema	59
7.3	Ignore, Increase and Abort	60
7.4	Promoted operations	60
7.5	Operations at the world level only	61
7.6	Initial state	62
7.7	Finalisation	63
<b>8</b>	<b>Consistency</b>	<b>65</b>
8.1	Introduction	65
8.2	Abstract model consistency proofs	65
8.3	Between model consistency proofs	67
8.4	Concrete model consistency proofs	68

<b>II</b>	<b>First Refinement: <math>\mathcal{A}</math> to <math>\mathcal{B}</math></b>	<b>69</b>
<b>9</b>	<b><math>\mathcal{A}</math> to <math>\mathcal{B}</math> rules</b>	<b>71</b>
9.1	Security of the implementation	71
9.2	Backwards rules proof obligations	72
<b>10</b>	<b><math>Rab</math></b>	<b>75</b>
10.1	Retrieve state	75
10.2	Retrieve inputs	84
10.3	Retrieve outputs	84
<b>11</b>	<b><math>\mathcal{A}</math> to <math>\mathcal{B}</math> initialisation</b>	<b>85</b>
11.1	Proof obligations	85
11.2	Proof of initial state	85
11.3	Proof of initial inputs	85
<b>12</b>	<b><math>\mathcal{A}</math> to <math>\mathcal{B}</math> finalisation</b>	<b>87</b>
12.1	Proof obligations	87
12.2	Output proof	88
12.3	State proof	88
<b>13</b>	<b><math>\mathcal{A}</math> to <math>\mathcal{B}</math> applicability</b>	<b>91</b>
13.1	Proof obligation	91
13.2	Proof	91
<b>14</b>	<b><math>\mathcal{A}</math> to <math>\mathcal{B}</math> lemmas</b>	<b>93</b>
14.1	Introduction	93
14.2	Lemma 'multiple refinement'	94
14.3	Lemma 'ignore': separating the branches	95
14.4	Lemma 'deterministic': simplifying the <i>Okay</i> branch	95
14.5	Lemma 'lost unchanged'	102
14.6	Lemma ' <i>AbIgnore</i> ': Operations that refine <i>AbIgnore</i>	103
14.7	<i>Ignore</i> refines <i>AbIgnore</i>	106
14.8	<i>Abort</i> refines <i>AbIgnore</i>	107
14.9	Lemma 'abort backward': operations that first abort	115
14.10	Summary of lemmas	116
<b>15</b>	<b><i>Increase</i></b>	<b>119</b>
15.1	Proof obligation	119
15.2	Invoking lemma 'lost unchanged'	119
15.3	check-operation-ignore	120

<b>16</b>	<b><i>StartFrom</i></b>	<b>121</b>
16.1	Proof obligation	121
16.2	Instantiating lemma 'deterministic'	122
16.3	Behaviour of <i>maybeLost</i> and <i>definitelyLost</i>	122
16.4	exists-pd	123
16.5	exists-chosenLost	123
16.6	check-operation	124
<b>17</b>	<b><i>StartTo</i></b>	<b>125</b>
17.1	Proof obligation	125
17.2	Instantiating lemma 'deterministic'	126
17.3	Behaviour of <i>maybeLost</i> and <i>definitelyLost</i>	126
17.4	exists-pd	127
17.5	exists-chosenLost	127
17.6	check-operation	128
<b>18</b>	<b><i>Req</i></b>	<b>129</b>
18.1	Proof obligation	129
18.2	Instantiating lemma 'deterministic'	129
18.3	Discussion	130
18.4	exists-pd	131
18.5	exists-chosenlost	131
18.6	check-operation	131
18.7	case 1: <i>ReqOkay</i> and <i>RabOkayCIPd'</i>	133
18.8	case 2: <i>ReqOkay</i> and <i>RabWillBeLostPd'</i>	138
18.9	case 3: <i>ReqOkay</i> and <i>RabHasBeenLostPd'</i>	142
18.10	case 4: <i>ReqOkay</i> and <i>RabEndPd'</i>	146
<b>19</b>	<b><i>Val</i></b>	<b>149</b>
19.1	Proof obligation	149
19.2	Instantiating lemma 'deterministic'	149
19.3	exists-pd	150
19.4	exists-chosenlost	150
19.5	check-operation	150
19.6	Behaviour of <i>maybeLost</i> and <i>definitelyLost</i>	151
19.7	Clarifying the hypothesis	153
<b>20</b>	<b><i>Ack</i></b>	<b>157</b>
20.1	Proof obligation	157
20.2	Instantiating lemma 'deterministic'	157
20.3	exists-pd	158

20.4	exists-chosenlost	158
20.5	check-operation	159
20.6	Behaviour of <i>maybeLost</i> and <i>definitelyLost</i>	159
20.7	Finishing proof of check-operation	162
<b>21</b>	<b><i>ReadExceptionLog</i></b>	<b>163</b>
21.1	Proof obligation	163
21.2	Invoking lemma 'lost unchanged'	164
21.3	check-operation-ignore	164
<b>22</b>	<b><i>ClearExceptionLog</i></b>	<b>165</b>
22.1	Proof obligation	165
22.2	Invoking lemma 'Lost unchanged'	166
22.3	check-operation-ignore	166
<b>23</b>	<b><i>AuthoriseExLogClear</i></b>	<b>167</b>
23.1	Proof obligation	167
23.2	Proof	167
<b>24</b>	<b><i>Archive</i></b>	<b>169</b>
24.1	Proof obligation	169
24.2	Proof	169
<b>III</b>	<b>Second Refinement: <math>B</math> to <math>C</math></b>	<b>171</b>
<b>25</b>	<b><math>B</math> to <math>C</math> rules</b>	<b>173</b>
25.1	Security of the implementation	173
25.2	Forwards rules proof obligations	174
<b>26</b>	<b><i>Rbc</i></b>	<b>177</b>
26.1	Retrieve state	177
<b>27</b>	<b>Initialisation, Finalisation, and Applicability</b>	<b>179</b>
27.1	Initialisation proof	179
27.2	Finalisation proof	179
27.3	Applicability proofs	180
<b>28</b>	<b><math>B</math> to <math>C</math> lemmas</b>	<b>181</b>
28.1	Specialising the proof rules	181
28.2	Correctness of <i>CIgnore</i>	182

28.3	Correctness of a branch of the operation	182
28.4	Correctness of <i>CIncrease</i>	185
28.5	Correctness of <i>CAbort</i>	185
28.6	Lemma 'logs unchanged'	187
28.7	Lemma 'abort forward': operations that first abort	188
<b>29</b>	<b>Correctness proofs</b>	<b>191</b>
29.1	Introduction	191
29.2	Correctness of <i>CStartFrom</i>	191
29.3	Correctness of <i>CStartTo</i>	193
29.4	Correctness of <i>CReq</i>	196
29.5	Correctness of <i>CVal</i>	197
29.6	Correctness of <i>CAck</i>	198
29.7	Correctness of <i>CReadExceptionLog</i>	200
29.8	Correctness of <i>CClearExceptionLog</i>	201
29.9	Correctness of <i>CAuthoriseExLogClear</i>	201
29.10	Correctness of <i>CArchive</i>	202
<b>30</b>	<b>Summary</b>	<b>203</b>
<b>IV</b>	<b>Appendices</b>	<b>209</b>
<b>A</b>	<b>Proof Layout</b>	<b>211</b>
A.1	Notation	211
A.2	Labelling proof steps	211
<b>B</b>	<b>Inference rules</b>	<b>213</b>
B.1	Universal quantifier becomes hypothesis	213
B.2	Disjunction in the hypothesis	214
B.3	Disjunction in the consequent	214
B.4	Conjunction in the consequent	214
B.5	Cut for lemmas	215
B.6	Thin	215
B.7	Universal Quantification	215
B.8	Negation	215
B.9	Contradiction	216
B.10	One Point Rule	216
B.11	Derived Rules	216
B.12	Proof of the Derived Rules	217

<b>C</b>	<b>Lemmas</b>	<b>219</b>
C.1	Lemma 'deterministic'	219
C.2	Lemma 'lost unchanged'	220
C.3	Lemma ' <i>AbIgnore</i> '	220
C.4	Lemma ' <i>Abort</i> refines <i>AbIgnore</i> '	221
C.5	Lemma 'abort backward'	221
C.6	Lemma 'constraint'	222
C.7	Lemma 'logs unchanged'	222
C.8	Lemma 'abort forward'	223
C.9	Lemma 'compose backward'	224
C.10	Lemma 'compose forward'	225
C.11	Lemma 'promoted composition'	226
C.12	Lemma 'notLoggedAndIn'	229
C.13	Lemma 'lost'	230
C.14	Lemma 'not lost before'	231
C.15	Lemma ' <i>AbWorld</i> unique'	232
<b>D</b>	<b>Toolkit</b>	<b>235</b>
D.1	Total abstract balance	235
D.2	Total lost value	235
D.3	Summing values	236

---

## Acknowledgments

The work described in this monograph took place as part of a development funded by the NatWest Development Team (now *platform seven*).

Part of the refinement work was carried out by Eoin MacDonnell.



## Introduction

### 1.1 The application

This case study is a reduced version of a real development by the NatWest Development Team (now *platform seven*) of a Smartcard product for electronic commerce. This development was deeply security critical: it was vital to ensure that these cards would not contain any bugs in implementation or design that would allow them to be subverted once in the field.

The system consists of a number of *electronic purses* that carry financial value, each hosted on a Smartcard. The purses interact with each other via a communications device to exchange value. Once released into the field, each purse is on its own: it has to ensure the security of all its transactions without recourse to a central controller. All security measures have to be implemented on the card, with no real-time external audit logging or monitoring.

#### 1.1.1 Models

We develop two key models in this case study. The first is an *abstract* model, describing the world of purses and the exchange of value through atomic transactions, expressing the security properties that the cards must preserve. The second is a *concrete* model, reflecting the design of the purses which exchange value using a message protocol. Both models are described in the Z notation [Spivey 1992b] [Woodcock & Davies 1996] [Barden *et al.* 1994], and we prove that the concrete model is a *refinement* of the abstract.

#### Abstract model

The abstract model is small, simple, and easy to understand. The key operation

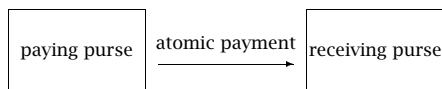


Figure 1.1: An atomic transaction in the abstract model

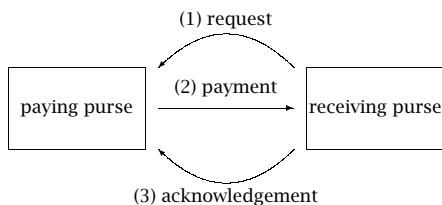


Figure 1.2: Part of the  $n$ -step protocol used to implement the atomic transaction in the concrete model.

transfers a chosen amount of value from one purse to another; the operation is modelled as an atomic action that simultaneously decrements the value in the paying purse and increments the value in the receiving purse (figure 1.1). Two key system security properties are maintained by this and other operations:

- no value may be created in the system; and
- all value is accounted in the system (no value is lost).

The simplicity of the abstract model allows these properties to be expressed in a way that is easily understood by the client.

### Concrete model

The concrete model is rather more complicated, reflecting the details of the real system design. The key changes from the abstract are:

- transactions are no longer atomic, but instead follow an  $n$ -step protocol (figure 1.2);
- the communications medium is insecure and unreliable;
- transaction logging is added to handle lost messages; and

- there are no global properties—each purse has to be implemented in isolation.

The basic protocol is:

1. the communications device ascertains the transaction to perform;
2. the receiving purse requests the transfer of an amount from the paying purse;
3. the paying purse sends that amount to the receiving purse; and
4. the receiving purse sends an acknowledgement of receipt to the paying purse.

The protocol, although simple in principle, is complicated by several facts: the protocol can be stopped at any point by removing the power from a card; the communications medium could lose a message; and a wire tapper could record a message and play it back to the same or different card later. In the face of all these possible actions, the protocol must implement the atomic transfer of value correctly, as specified in the abstract model.

### 1.1.2 Proofs

All the security properties of the abstract model are *functional*, and so are preserved by refinement.

The purpose of performing the proof is to give a very high assurance that the chosen design (the protocol) does, indeed, behave just like the abstract, atomic transfers. We choose to do rigorous proofs by hand: our experience is that current proof tools are not yet appropriate for a task of this size. We did, however, type-check the statements of the proof obligations and many of the proof steps using a combination of *fuzz* [Spivey 1992a] and Formaliser [Flynn *et al.* 1990] [Stepney]. As part of the development process, all proofs were also independently checked by external evaluators.

## 1.2 Overview of model and proof structure

The specification and security proof have the following structure (summarised in figure 1.3):

- Security Properties, SPs:
  - The *Security Properties* are defined in terms of constraints on secure operations; they are *formalised* in terms of the appropriate model concepts (see later).

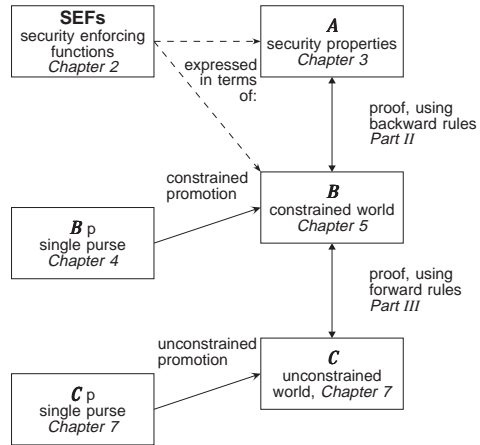


Figure 1.3: Overview of document organisation, with model and proof structure

- In some cases, where it may not be evident that a model captures a particular constraint, the desired property is recast as a *theorem* and proved.
- Abstract model,  $\mathcal{A}$ : We define an *abstract model* (Chapter 3), which forms the *Formal Security Policy Model*; it consists of a global model in terms of a simple *state and operations*:
  - the state is a world of (abstract) purses; and
  - the operations are defined on this state.
- Between model,  $\mathcal{B}$ : Next we build a *'between' levels model*. This is the first refinement towards the implementation of purses consisting of local state information only. This model,  $\mathcal{B}$ , is structured as a promoted state-and-operations model:
  - The state of a single (concrete) purse, and the corresponding single-purse operations, are defined (Chapter 4).
  - The purses and operations are *promoted* to a global state and operations (Chapter 5). Constraints are put on this promotion to enable the correctness proofs to be performed.

- Concrete model,  $\mathcal{C}$ : Our final model is the *concrete level model*, which forms the *Formal Architectural Design*. This model,  $\mathcal{C}$ , is structured as a promoted state-and-operations model, very similar to  $\mathcal{B}$ , except it has no constraints on the promotion:
  - The state of a single (concrete) purse, and the corresponding single-purse operations, are defined (Chapter 7).
  - The purses and operations are *promoted* to a global state and operations, with *no* constraints (Chapter 7).
- Security proof  $\mathcal{A}$ - $\mathcal{B}$ : The *security policy* is proved to hold for  $\mathcal{B}$  by proving that  $\mathcal{B}$  is a *refinement* of  $\mathcal{A}$ . This forms the first part of *Explanation of Consistency*.
  - The retrieve relation  $R_{ab}$ , relating the  $\mathcal{B}$  and  $\mathcal{A}$  worlds, is defined (Chapter 10).
  - The *security policy* is shown to hold for  $\mathcal{B}$  by proof that  $\mathcal{B}$  refines  $\mathcal{A}$ , using the 'backward' proof rules (Part II). This proof comprises the bulk of the proof work.
- Security proof  $\mathcal{B}$ - $\mathcal{C}$ : The *security policy* is proved to hold for  $\mathcal{C}$  by proving that  $\mathcal{C}$  is a *refinement* of  $\mathcal{B}$  (and hence of  $\mathcal{A}$ , by transitivity of refinement). This forms the remaining part of *Explanation of Consistency*.
  - The retrieve relation  $R_{bc}$ , relating the  $\mathcal{C}$  and  $\mathcal{B}$  worlds, is defined (Chapter 26).
  - The *security policy* is shown to hold for  $\mathcal{C}$  by proof that  $\mathcal{C}$  refines  $\mathcal{B}$ , using the 'forward' proof rules (Part III). These two levels are relatively close, so this proof is relatively straightforward.

The mathematical operators and schemas defined in this document are included in the index at the end of the document.

### 1.3 Rationale for model structure

As noted above, this case study has been adapted from a larger, real development. In order to produce a case study of a size appropriate for public presentation, much of the real functionality has had to be removed. Some of the structure of the larger specification has remained present in the smaller one, although it might not have been used had the smaller specification been written from scratch. This omitted functionality, whilst important from a business perspective, is peripheral to the central security requirements.

## 1.4 Rationale for proof structure

Imagine two specifications  $\mathcal{A}$  and  $C$ , which describe executable machines. Imagine that, on every step, each machine consumes an input and produces an output. Finally, imagine that every execution of  $C$ , viewed solely in terms of inputs and outputs, could equally well have been an execution of  $\mathcal{A}$ . In this sense,  $\mathcal{A}$  can *simulate* any behaviour of  $C$ . If this is the case, then we say that  $C$  is a *refinement* of  $\mathcal{A}$ .

This is exactly what we want to prove in our case study: that the concrete model is a refinement of the abstract one.

Refinement is an ordering between specifications that captures an intuitive notion of when a concrete specification implements an abstract one. This allows us to postpone implementation detail in writing our top-level specification, focussing only on essential properties. The cost of this abstraction is the need to refine the specification, reifying data structures and algorithms; refinement is a formal technique for ensuring that essential properties are present in a more concrete specification.

Nondeterminism is used in an abstract specification to describe alternative acceptable behaviours; in choosing a concrete refinement of an abstract specification, some of these nondeterministic choices may be resolved. Since we view  $\mathcal{A}$  and  $C$  only in terms of inputs and outputs, nondeterminism present in  $\mathcal{A}$  may be resolved at a different point in  $C$ .

Our abstract model, chosen to represent the difference between secure and insecure transactions very clearly, has nondeterminism in a different place from the implementation. In fact, it has it in a place that precludes proof using the forward rules of [Spivey 1992b, section 5.6]. For this reason we use the backward rules to prove against the abstract model.

At the concrete level, we must describe the purse behaviour in a way that closely mirrors the actual design. An important (and obvious) property of the design is that the purses are *independent*, that is, each purse acts on the basis of its own, local knowledge, and we have no control over the communications medium between purses. This can be expressed cleanly in Z by building a model of an individual purse in isolation, and then *promoting* [Barden *et al.* 1994, chapter 19] this model to a world with many purses. To express the fact that we have no global control over the purses nor over the communications medium, we must use an unconstrained promotion. This we do in the  $C$  model.

Why do we not, then, do a single backward proof step from the  $\mathcal{A}$  model to the  $C$  model?

For technical reasons, the backward proof rules need the more concrete specification to be tightly constrained in its state space. The form of the proofs forces the description of the state space to include explicit predicates excluding

all but valid states. However, these predicates are not expressible locally to purses, and hence cannot be included in specification derived by unconstrained promotion. That is, we cannot express the predicates needed for the proof in the  $C$  model.

We therefore introduce an intermediate model, the  $B$  model, which is a *constrained* promotion, and hence can contain the predicates needed for the backward proofs. We then prove a refinement from  $\mathcal{A}$  to  $B$  using the backward rules. But now the constrained promotion  $B$  is very close to the unconstrained promotion  $C$ , and in particular the nondeterminism is resolved in the same place in both models, allowing the forward rules to be used. This we do in our proof of refinement from  $B$  to  $C$ .

## 1.5 Status

The specification and theorems have been parsed and type-checked using `fuzz` [Spivey 1992a]. There is no use of the `%unchecked` parser directive in the specification, in the statement of theorems, or in the statement of most of the intermediate goals; however, some reasoning steps have hidden declarations to make them type-check and some do not conform to `fuzz`'s syntax at all.

**Part I**  
**Models**

---

## Security Properties

### 2.1 Introduction

This chapter gathers together the Security Properties (SPs) definitions, for reference. The SPs are formalised in terms of the abstract and concrete models, making use of definitions in Chapters 3 and 4. (The index can be used to find the definitions of these terms.) The full meaning and effect of a SP can be seen only in the context of the model that includes it.

### 2.2 Abstract model SPs

The following SPs are expressed in terms of the abstract model  $\mathcal{A}$ , defined in chapter 3.

#### 2.2.1 No value creation

**Security Property 1.** *No value may be created in the system: the sum of all the purses' balances does not increase.*<sup>1</sup>

$$\frac{\text{NoValueCreation}}{\Delta \text{AbWorld}} \frac{}{totalAbBalance \text{ abAuthPurse}' \leq totalAbBalance \text{ abAuthPurse}}$$

<sup>1</sup>Proved to hold for the model, section 2.4. *NoValueCreation* requires that the sum of the before balances is greater or equal to the sum of the after balances. The abstract model enforces a stronger condition: that transfers change only the purses involved in the transfer and only by the amount stated in the transfer.

### 2.2.2 All value accounted

**Security Property 2.1.** All value must be accounted for in the system: the sum of all purses' balances and lost components does not change.<sup>2</sup>

$$\frac{\text{AllValueAccounted} \quad \Delta \text{AbWorld}}{\text{totalAbBalance } abAuthPurse' + \text{totalLost } abAuthPurse' = \text{totalAbBalance } abAuthPurse + \text{totalLost } abAuthPurse}$$

### 2.2.3 Authentic purses

**Security Property 3.** A transfer can occur only between authentic purses.<sup>3</sup>

$$\frac{\text{Authentic} \quad \text{AbWorld} \quad \text{name?} : \text{NAME}}{\text{name?} \in \text{dom } abAuthPurse}$$

### 2.2.4 Sufficient funds

**Security Property 4.** A transfer can occur only if there are sufficient funds in the from-purse.<sup>4</sup>

$$\frac{\text{SufficientFundsProperty} \quad \text{AbWorld} \quad \text{TransferDetails?}}{\text{value?} \leq (\text{abAuthPurse } from?).\text{balance}}$$

## 2.3 Concrete model SPs

The following SPs are expressed in terms of the between (and concrete) model  $\mathcal{B}$ , defined in chapter 4.

<sup>2</sup>Proved to hold for the model, section 2.4. The concrete level SP 2.2 uses logging to support this SP.

<sup>3</sup>Used in the definition of:  $AbTransferOkay$  and  $AbTransferLost$ , section 3.3.3.

<sup>4</sup>Used in the definition of:  $AbTransferOkay$  and  $AbTransferLost$ , section 3.3.3. Used in the proof of: SP1, section 2.4.1, section 2.4.3; SP2, section 2.4.2, section 2.4.4. Note that the model also ensures that the  $balance$  and  $value?$  are non-negative.

### 2.3.1 Exception logging

**Security Property 2.2.** If a purse aborts a transfer at a point where value could be lost, then the purse logs the details.<sup>5</sup>

$$\frac{\text{LogIfNecessary} \quad \Delta \text{ConPurse}}{\text{exLog}' = \text{exLog} \cup (\text{if } status \in \{epv, epa\} \text{ then } \{pdAuth\} \text{ else } \emptyset)}$$

The only times the log need be updated are if the purse is in  $epv$  (having sent the  $req$  message) or in  $epa$  (having sent the  $val$  but not yet received the  $ack$ ). In all other cases the transfer has not yet got far enough for the purse to be worried that the transfer has failed, or has got far enough that the purse is happy that the transfer has succeeded.

## 2.4 SPs and the models

All the SPs hold in the appropriate models.

In most cases, this is obviously true, by construction: the SPs appear as explicit predicates in the relevant definitions. However,  $NoValueCreation$  and  $AllValueAccounted$  are not explicitly included in the operation that changes the relevant components:  $AbTransfer$ . In this section, we demonstrate that the abstract model indeed satisfies these SPs. That is:

$$AbTransferOkay \vdash NoValueCreation \wedge AllValueAccounted$$

$$AbTransferLost \vdash NoValueCreation \wedge AllValueAccounted$$

$$AbIgnore \vdash NoValueCreation \wedge AllValueAccounted$$

In the proofs below, we use the  $TD$  form of the definitions, by [cut]ting in the appropriate  $TransferDetails$ .

### 2.4.1 Transfer okay, no value creation

$$AbTransferOkayTD \vdash NoValueCreation$$

<sup>5</sup>Used in the definition of:  $AbortPurse$ , section 4.8.2.

**Proof:**

$$\begin{aligned}
& totalAbBalance\ abAuthPurse' \\
&= totalAbBalance(\{from?, to?\} \triangleleft abAuthPurse') \\
&\quad + (abAuthPurse'\ from?).balance \\
&\quad + (abAuthPurse'\ to?).balance \quad [totalAbBalance] \\
&= totalAbBalance(\{from?, to?\} \triangleleft abAuthPurse) \\
&\quad + ((abAuthPurse\ from?).balance - value?) \\
&\quad + ((abAuthPurse\ to?).balance + value?) \quad [AbTransferOkay] \\
&= totalAbBalance\ abAuthPurse \\
&\leq totalAbBalance\ abAuthPurse
\end{aligned}$$

■ 2.4.1

**2.4.2 Transfer okay, all value accounted** $AbTransferOkayTD \vdash AllValueAccounted$ **Proof:**

$$\begin{aligned}
& totalAbBalance\ abAuthPurse' + totalLost\ abAuthPurse' \\
&= totalAbBalance(\{from?, to?\} \triangleleft abAuthPurse') \\
&\quad + (abAuthPurse'\ from?).balance \\
&\quad + (abAuthPurse'\ to?).balance \quad [totalAbBalance] \\
&\quad + totalLost(\{from?, to?\} \triangleleft abAuthPurse') \\
&\quad + (abAuthPurse'\ from?).lost \\
&\quad + (abAuthPurse'\ to?).lost \quad [totalLost] \\
&= totalAbBalance(\{from?, to?\} \triangleleft abAuthPurse) \\
&\quad + ((abAuthPurse\ from?).balance - value?) \\
&\quad + ((abAuthPurse\ to?).balance + value?) \\
&\quad + totalLost(\{from?, to?\} \triangleleft abAuthPurse) \\
&\quad + (abAuthPurse\ from?).lost \\
&\quad + (abAuthPurse\ to?).lost \quad [AbTransferOkay] \\
&= totalAbBalance\ abAuthPurse + totalLost\ abAuthPurse
\end{aligned}$$

■ 2.4.2

**2.4.3 Transfer lost, no value creation** $AbTransferLostTD \vdash NoValueCreation$ **Proof:**

$$\begin{aligned}
& totalAbBalance\ abAuthPurse' \\
&= totalAbBalance(\{from?, to?\} \triangleleft abAuthPurse') \\
&\quad + (abAuthPurse'\ from?).balance \\
&\quad + (abAuthPurse'\ to?).balance \quad [totalAbBalance] \\
&= totalAbBalance(\{from?, to?\} \triangleleft abAuthPurse) \\
&\quad + ((abAuthPurse\ from?).balance - value?) \\
&\quad + (abAuthPurse\ to?).balance \quad [AbTransferLost] \\
&= totalAbBalance\ abAuthPurse - value? \quad [totalAbBalance] \\
&\leq totalAbBalance\ abAuthPurse
\end{aligned}$$

■ 2.4.3

**2.4.4 Transfer lost, all value accounted** $AbTransferLostTD \vdash AllValueAccounted$ **Proof:**

$$\begin{aligned}
& totalAbBalance\ abAuthPurse' + totalLost\ abAuthPurse' \\
&= totalAbBalance(\{from?, to?\} \triangleleft abAuthPurse') \\
&\quad + (abAuthPurse'\ from?).balance \\
&\quad + (abAuthPurse'\ to?).balance \quad [totalAbBalance] \\
&\quad + totalLost(\{from?, to?\} \triangleleft abAuthPurse') \\
&\quad + (abAuthPurse'\ from?).lost \\
&\quad + (abAuthPurse'\ to?).lost \quad [totalLost] \\
&= totalAbBalance(\{from?, to?\} \triangleleft abAuthPurse) \\
&\quad + ((abAuthPurse\ from?).balance - value?) \\
&\quad + (abAuthPurse\ to?).balance \\
&\quad + totalLost(\{from?, to?\} \triangleleft abAuthPurse) \\
&\quad + ((abAuthPurse\ from?).lost + value?) \\
&\quad + (abAuthPurse\ to?).lost \quad [AbTransferLost] \\
&= totalAbBalance\ abAuthPurse + totalLost\ abAuthPurse
\end{aligned}$$



- 2.4.4

### 2.4.5 Transfer ignore

$AbIgnore \vdash NoValueCreation \wedge AllValueAccounted$

**Proof:**

Follows directly from the definition of  $AbIgnore$ , which changes none of the relevant values.

- 2.4.5
- 2.4
- 2

---

## Abstract model: security policy

### 3.1 Introduction

The abstract model specification has the following parts:

- State: the abstract world of purses
- Operations: secure changes from one abstract state to another
- Initialisation: the abstract world starts off secure
- Finalisation: a way of observing part of the abstract world to determine that it is secure

### 3.2 The abstract state

#### 3.2.1 A purse

An abstract  $AbPurse$  consists of a *balance*, the value stored in the purse; and a *lost* component, the total value lost during unsuccessful transfers. (The unsuccessful, but still secure, transfer is defined in section 3.3.3.)

$$AbPurse \hat{=} [ balance, lost : \mathbb{N} ]$$

#### 3.2.2 Transfer details

Each purse has a distinct, unique name.

[NAME]

The details of a particular transfer include the names of the *from* and *to* purses and the value to be transferred.

$\begin{array}{l} \text{TransferDetails} \\ \text{from, to : NAME} \\ \text{value : } \mathbb{N} \end{array}$
---

Although it is not permitted to perform a transfer between a purse and itself, the constraint  $\text{from} \neq \text{to}$  is checked during  $\text{AbTransfer}$ , rather than put in  $\text{TransferDetails}$ , since it is permitted to *request* a transfer with  $\text{from} = \text{to}$ .

Transactions involving zero value are allowed.

### 3.2.3 Abstract world

The abstract world model contains a mapping from purse names to abstract purses. The domain of this function corresponds to authentic purses, those that may engage in transfers<sup>1</sup>. We allow only a finite number of authentic purses, to ensure a well-defined total value in the system.

$$\text{AbWorld} \hat{=} [ \text{abAuthPurse} : \text{NAME} \rightsquigarrow \text{AbPurse} ]$$

## 3.3 Secure operations

Having defined our abstract world,  $\text{AbWorld}$ , we now define operations on the world that respect the relevant SPs. We call these *secure operations*. They comprise:

- $\text{AbIgnore}$ : securely do nothing
- $\text{AbTransfer}$ : securely transfer balance between purses, or securely ‘lose’ the balance

### 3.3.1 Abstract inputs and outputs

We are to prove that the implementation is a refinement of the abstract security policy specification. This is made simpler if every operation has an input and an output, and if all operations’ inputs and outputs are of the same type.

So we define the inputs and outputs (some being ‘dummy’ values) using a free type construct:

$$\begin{array}{l} \text{AIN} ::= \text{aNullIn} \\ \quad | \text{transfer} \langle \langle \text{TransferDetails} \rangle \rangle \end{array}$$

<sup>1</sup>SP 3, ‘Authentic purses’, section 2.2.3.

$$\text{AOUT} ::= \text{aNullOut}$$

Every abstract operation has the following properties:

$\begin{array}{l} \text{AbOp} \\ \Delta \text{AbWorld} \\ a? : \text{AIN}; a! : \text{AOUT} \\ a! = \text{aNullOut} \end{array}$
--

The output is always  $\text{aNullOut}$  (that is, we are not interested in the abstract output).

### 3.3.2 Abstract ignore

Any operation has the option of securely doing nothing.

$\begin{array}{l} \text{AbIgnore} \\ \text{AbOp} \\ \text{abAuthPurse}' = \text{abAuthPurse} \end{array}$
---

### 3.3.3 Transfer

The transfer operation changes only the balance and lost component of the relevant purses.

$$\text{AbPurseTransfer} \hat{=} \text{AbPurse} \setminus (\text{balance}, \text{lost})$$

The secure transfer operations change at most the *from* and *to* purse states: all other purse states are unchanged.

$\begin{array}{l} \text{AbWorldSecureOp} \\ \text{AbOp} \\ \text{TransferDetails?} \\ a? \in \text{ran transfer} \\ \emptyset \text{TransferDetails?} = \text{transfer} \sim a? \\ \{ \text{from?}, \text{to?} \} \triangleleft \text{abAuthPurse}' = \{ \text{from?}, \text{to?} \} \triangleleft \text{abAuthPurse} \end{array}$
--

A transfer can securely succeed between two purses if they are distinct, both purses are authentic<sup>2</sup>, and the *from* purse has sufficient funds<sup>3</sup>.

$ \begin{array}{l} \text{AbTransferOkayTD} \\ \text{AbWorldSecureOp} \\ \text{Authentic}[from? / name?] \\ \text{Authentic}[to? / name?] \\ \text{SufficientFundsProperty} \\ to? \neq from? \\ \text{abAuthPurse}' from? = (\mu \Delta \text{AbPurse}   \\ \quad \theta \text{AbPurse} = \text{abAuthPurse } from? \\ \quad \wedge \text{balance}' = \text{balance} - \text{value?} \\ \quad \wedge \text{lost}' = \text{lost} \\ \quad \wedge \exists \text{AbPurseTransfer} \\ \quad \bullet \theta \text{AbPurse}') \\ \text{abAuthPurse}' to? = (\mu \Delta \text{AbPurse}   \\ \quad \theta \text{AbPurse} = \text{abAuthPurse } to? \\ \quad \wedge \text{balance}' = \text{balance} + \text{value?} \\ \quad \wedge \text{lost}' = \text{lost} \\ \quad \wedge \exists \text{AbPurseTransfer} \\ \quad \bullet \theta \text{AbPurse}') \end{array} $
--

The operation transfers *value?* from the *from* purse to the *to* purse<sup>4</sup>. All the other components of the *from?* and *to?* purses are unchanged, and all other purses are unchanged.

The model is more constrained than required by the SPs, and hence it represents a sufficient, but not necessary, behaviour to conform to the SPs.

Hiding the auxiliary inputs gives the *Okay* operation as:

$$\text{AbTransferOkay} \hat{=} \text{AbTransferOkayTD} \setminus (to?, from?, value?)$$

A transfer can securely lose value between two purses if they are distinct, both purses are authentic<sup>5</sup>, and the *from* purse has sufficient funds<sup>6</sup>.

<sup>2</sup>SP 3, 'Authentic purses', section 2.2.3.

<sup>3</sup>SP 4, 'Sufficient funds', section 2.2.4.

<sup>4</sup>SP 1, 'No value created', section 2.2.1.

<sup>5</sup>SP 3, 'Authentic purses', section 2.2.3.

<sup>6</sup>SP 4, 'Sufficient funds', section 2.2.4.

$ \begin{array}{l} \text{AbTransferLostTD} \\ \text{AbWorldSecureOp} \\ \text{Authentic}[from? / name?] \\ \text{Authentic}[to? / name?] \\ \text{SufficientFundsProperty} \\ to? \neq from? \\ \text{abAuthPurse}' from? \in \{ \Delta \text{AbPurse}   \\ \quad \theta \text{AbPurse} = \text{abAuthPurse } from? \\ \quad \wedge \text{balance}' = \text{balance} - \text{value?} \\ \quad \wedge \text{lost}' = \text{lost} + \text{value?} \\ \quad \wedge \exists \text{AbPurseTransfer} \\ \quad \bullet \theta \text{AbPurse}' \} \\ \text{abAuthPurse}' to? = \text{abAuthPurse } to? \end{array} $
--

The operation removes *value?* from the *from* purse's balance,<sup>7</sup> and adds it to the *from* purse's *lost* component.<sup>8</sup> All the other components of the *from?* purse are unchanged, The *to* purse and all other purses are unchanged.

Hiding the auxiliary inputs gives the *Okay* operation as:

$$\text{AbTransferLost} \hat{=} \text{AbTransferLostTD} \setminus (to?, from?, value?)$$

The full transfer operation can also securely do nothing, *AbIgnore*. The full transfer operation is

$$\text{AbTransfer} \hat{=} \text{AbTransferOkay} \vee \text{AbTransferLost} \vee \text{AbIgnore}$$

### 3.4 Abstract initial state

One conventional definition of the initial state of a system is as being empty; operations are used to add elements to the state until the desired configuration is reached. However, we do not wish to add new abstract purses to the domain of *abAuthPurse*, so we cannot start with a system containing no authentic purses. So we set up an arbitrary initial state, which satisfies the predicate of *AbWorld'*.

$$\text{AbInitState} \hat{=} \text{AbWorld}'$$

<sup>7</sup>SP 1, 'No value created', section 2.2.1.

<sup>8</sup>SP 2, 'All value accounted', section 2.2.2.

So we say that *AbInitState* has some particular value, we just do not say what that particular value *is*. The particular value chosen is irrelevant to the security of the system; any starting state would be secure.

Initialisation also defines the mapping from global (that is, observable) inputs to abstract (that is, modelled) inputs. This is just the identity relation in the  $\mathcal{A}$  model:

$$AbInitIn \hat{=} [ a?, g? : AIN \mid a? = g? ]$$

### 3.5 Abstract finalisation

We must ‘observe’ each security relevant component of the world, in order to determine that the security properties do indeed hold. Observation is usually performed by enquiry operations, and any part of the state not visible through some enquiry operation is deemed unimportant. However, in our case there are no abstract enquiry operations to observe state components, but there are security properties related to them, and so they *are* important. We use *finalisation* to observe them.

Finalisation takes an abstract state, and ‘projects out’ the portion of it we wish to observe, into a global state. Here we choose to observe the entire abstract state.

The global state is the same as the abstract state:

$$GlobalWorld \hat{=} [ gAuthPurse : NAME \leftrightarrow AbPurse ]$$

Finalisation gives the global state corresponding to an abstract state. These are mostly the identity relations in the  $\mathcal{A}$  model:

<i>AbFinState</i>
<i>AbWorld</i>
<i>GlobalWorld</i>
<i>gAuthPurse</i> = <i>abAuthPurse</i>

Finalisation also defines the mapping from abstract outputs to global (that is, observable) outputs.

$$AbFinOut \hat{=} [ a!, g! : AOUT \mid a! = g! ]$$

## Between model, single purse operations

### 4.1 Overview

This chapter covers the purse-level operations, which are: abort, the start operations, the transfer operations *req*, *val* and *ack*, read log, and clear log.

For the sake of simplicity, we assume that concrete and abstract *NAMES* are drawn from the same sets.

In this section we refer to ‘concrete’ rather than ‘between’ purse, because, as we see later, there is no difference between the two structurally. The only difference between the  $\mathcal{B}$  and  $\mathcal{C}$  worlds is fewer global constraints in the latter.

### 4.2 Status

A concrete purse has a *status*, which records its progress through a transaction.

$$STATUS ::= eaFrom \mid eaTo \mid epr \mid epv \mid epa$$

The statuses are: *eaFrom* ‘expecting any payer’, *eaTo* ‘expecting any payee’, *epr* ‘expecting payment req’, *epv* ‘expecting payment val’, and *epa* ‘expecting payment ack’.

### 4.3 Message Details

The abstract level describes the operations that transfer value. Purses are sent instructions via messages, and we present the structure of compound messages in this section.

The abstract level describes a transfer of value from one purse to another. We implement this at the concrete level by a protocol consisting of messages.

- A single transfer involves many messages. So we need a way to distinguish messages: we use a tag for *req*, *val* or *ack*.
- We have no control over the concrete messages, and cannot forbid the duplication of messages. So we need a way to distinguish separate transactions: we use sequence numbers that are increased between transactions. (The transaction sequence number is implemented as a sufficiently large number. Provided that the initial sequence number is quite small, and each increment is small, we need not worry about overflow, since the purse will physically wear out first.)

#### 4.3.1 Start message counterparty details

The counterparty details of a payment, which are transmitted with a *start* message, identify the other purse, the *value* to be transferred, and the other purse's transaction sequence number.

<i>CounterPartyDetails</i> <i>name</i> : NAME <i>value</i> : $\mathbb{N}$ <i>nextSeqNo</i> : $\mathbb{N}$
--

#### 4.3.2 Payment log message details

Purses store current payment details, and exception log records that hold sufficient information about failed or problematic transactions to reconstruct the value lost in the transfer<sup>1</sup>. The payment log details identify the different *from* and *to* purses and the *value* to be transferred (as in the abstract *TransferDetails*) and also the purses' transaction sequence numbers. The combination of purse name and sequence number *uniquely* identifies the transaction.

<i>PayDetails</i> <i>TransferDetails</i> <i>fromSeqNo, toSeqNo</i> : $\mathbb{N}$ <i>from</i> $\neq$ <i>to</i>
---

<sup>1</sup>Concrete SP 2.2, 'Exception logging', section 2.3.1.

We can put the constraint about distinct purses in the *PayDetails*, because this check is made in *ValidStartTo/From*, before the details are set up.

#### 4.4 Clear Exception Log Validation

*CLEAR* is the set of clear codes for purse exception logs.

[*CLEAR*]

A clear code is provided by an external source (section 5.7.1) in order to clear a purse's exception log (section 4.10.2).

*image* is a function to calculate the clear code for a given non-empty set of exception records.

| *image* :  $\mathbb{P}_1 \text{ PayDetails} \rightarrow \text{CLEAR}$

*image* takes a set of exception logs, and produces another value used to validate a log clear command. For each set of *PayDetails*, there is a unique clear code.

The *BetweenWorld* model is designed so that no logs are ever lost. Indeed, we must prove that no logs are lost in the refinement of each operation — this is an implicit part of the refinement correctness proofs. The *BetweenWorld* mechanism to ensure that no logs are lost relies on two assumptions:

- clear codes are only ever generated from sets of *PayDetails* that are stored in the *archive* (a secure store of log records introduced later)
- clear codes unambiguously identify sets of *PayDetails*

The second of these assumptions is captured formally by the *injective* function *image*<sup>2</sup>.

<sup>2</sup>In practice, *image* is not injective on general sets of *PayDetails*, but it is injective when restricted to the sets actually encountered.

## 4.5 Messages

There are various kinds of messages:

```
MESSAGE ::= startFrom⟨⟨CounterPartyDetails⟩⟩
          | startTo⟨⟨CounterPartyDetails⟩⟩
          | readExceptionLog
          | req⟨⟨PayDetails⟩⟩
          | val⟨⟨PayDetails⟩⟩
          | ack⟨⟨PayDetails⟩⟩
          | exceptionLogResult⟨⟨NAME × PayDetails⟩⟩
          | exceptionLogClear⟨⟨NAME × CLEAR⟩⟩
          | ⊥
```

The first group of messages may be unprotected. Their forgeability is modelled by having them all present in the initial message ether (see section 6.1).

The second group of messages are all that need to be cryptographically protected. Their unforgeability is modelled by having them added to the message ether only by specified operations.

⊥, ‘forged’, is a message emitted by operations that ignore the (irrelevant) input message, or emitted by non-authentic purses. It is also the input message to the *Ignore*, *Increase* and *Abort* operations. ⊥ is implemented as an unprotected status message, as an error message, as a ‘forged’ message, or as ‘silence’. As far as the model is concerned, we choose not to distinguish these messages from each other, only from the other distinguished ones. (See also section 5.8.)

A complete payment transaction is made up of a *startFrom*, *startTo*, *req*, *val*, and *ack* message.

## 4.6 A concrete purse

A concrete purse has a current balance, an exception log for recording failed or problematic transfers, a name, a transaction sequence number to be used for the next transaction, the payment details of the current transaction, and a status indicating the purse’s position in the current transaction.

<pre>ConPurse balance : ℕ exLog : P PayDetails name : NAME nextSeqNo : ℕ pdAuth : PayDetails status : STATUS  ∀ pd : exLog • name ∈ {pd.from, pd.to}  status = epr ⇒ name = pdAuth.from                 ∧ pdAuth.value ≤ balance                 ∧ pdAuth.fromSeqNo &lt; nextSeqNo  status = epv ⇒ pdAuth.toSeqNo &lt; nextSeqNo  status = epa ⇒ pdAuth.fromSeqNo &lt; nextSeqNo</pre>
--

The name is included in the purse’s state so that the purse itself can check it is the correct purse for this transaction.

The predicate on the purse state records the following constraints:

P-1  $\forall pd : exLog \bullet name \in \{pd.from, pd.to\}$

All log details in the exception log refer to this purse, as the *from* or the *to* party<sup>3</sup>.

P-2  $status = epr \Rightarrow$

$name = pdAuth.from$   
 $\wedge pdAuth.value \leq balance$   
 $\wedge pdAuth.fromSeqNo < nextSeqNo$

If the purse is expecting a payment request, then:

- (a) it is the *from* purse of the current transaction<sup>4</sup>.
- (b) it has sufficient funds for the request<sup>5</sup> (this condition is required because there is no check for sufficient funds on receipt of the request)
- (c) its next sequence number is greater than the current transaction’s sequence number<sup>6</sup>

P-3  $status = epv \Rightarrow pdAuth.toSeqNo < nextSeqNo$

<sup>3</sup>Used in: *AuxWorld* does not add constraints, section 5.2.1.

<sup>4</sup>Used in: *CReq*, B-9, section 29.4.

<sup>5</sup>Used in: *Req*, case 1, *SufficientFundsProperty*, section 18.7.2; *Req*, case 2, *SufficientFundsProperty*, section 18.8.2; *Req*, case 3, *SufficientFundsProperty*, section 18.9.2.

<sup>6</sup>Used in: *CReq*, B-3, section 29.4.

If the purse is expecting a payment value, then its next sequence number is greater than the current transaction's sequence number<sup>7</sup>

P-4  $status = epa \Rightarrow pdAuth.fromSeqNo < nextSeqNo$

If the purse is expecting a payment acknowledgement, then its next sequence number is greater than the current transaction's sequence number<sup>8</sup>

## 4.7 Single Purse operations

### 4.7.1 Overview

The concrete purse specification is structured around the various purse-level operations:

- invisible operations
  - *IncreasePurse*
  - *AbortPurse*
- value transfer operations
  - *StartFromPurse*
  - *StartToPurse*
  - *ReqPurse*
  - *ValPurse*
  - *AckPurse*
- exception logging operations
  - *ReadExceptionLogPurse*
  - *ClearExceptionLogPurse*

## 4.8 Invisible operations

Several concrete operations have a common effect on the state visible in the model (they affect only implementation state not visible in the model).

<sup>7</sup>Used in: *CAbort*, B-6, section 28.5.

<sup>8</sup>Used in: *CAbort*, B-5, section 28.5.

### 4.8.1 Increase Purse

The *IncreasePurseOkay* operation is used to model actual purse operations that do not have any effect on the state visible in this model, except for increasing the sequence number.

In a simple increase transaction, only the purse's sequence number may change. All other components remain unchanged.

$$ConPurseIncrease \hat{=} ConPurse \setminus (nextSeqNo)$$

$\frac{IncreasePurseOkay}{\Delta ConPurse}$
$m?, m! : MESSAGE$
$\exists ConPurseIncrease$
$nextSeqNo' \geq nextSeqNo$
$m! = \perp$

### 4.8.2 Abort Purse

The *AbortPurseOkay* operation is used to model actual purse operations that do not have any effect on the state visible in this model, but that abort and log incomplete transactions.

In a simple abort transaction, only the purse's sequence number, exception log, *pdAuth* and status may change. All other components remain unchanged.

$$ConPurseAbort \hat{=} ConPurse \setminus (nextSeqNo, exLog, pdAuth, status)$$

*AbortPurseOkay* places the purse in status *eaFrom* (where the *pdAuth* component is undefined), logging any incomplete transactions if necessary<sup>9</sup>. No other component of the purse is altered, except for *nextSeqNo*, which may increase arbitrarily.

<sup>9</sup>Concrete SP 2.2, 'Exception logging', section 2.3.1.

$\text{AbortPurseOkay}$ $\Delta \text{ConPurse}$ $m?, m! : \text{MESSAGE}$ $\exists \text{ConPurseAbort}$ $\text{LogIfNecessary}$ $\text{status}' = \text{eaFrom}$ $\text{nextSeqNo}' \geq \text{nextSeqNo}$
--

We do not, at this stage, put any restrictions on the output message  $m!$ . Later, we either compose *AbortPurseOkay* with another operation, using the latter's  $m!$ , or we promote *AbortPurseOkay* to the world level, where we define  $m! = \perp$ .

#### 4.9 Value transfer operations

The *StartTo* and *StartFrom* operations, when starting from *eaFrom*, change only the sequence number, the stored *pdAuth*, and the status of a purse.

$$\text{ConPurseStart} \hat{=} \text{ConPurse} \setminus (\text{nextSeqNo}, \text{pdAuth}, \text{status})$$

The *Req* operation change only the balance and the status of a purse.

$$\text{ConPurseReq} \hat{=} \text{ConPurse} \setminus (\text{balance}, \text{status})$$

The *Val* operation change only the balance and the status of a purse.

$$\text{ConPurseVal} \hat{=} \text{ConPurse} \setminus (\text{balance}, \text{status})$$

The *Ack* operation changes only the status of a purse, and allows the *pdAuth* to change arbitrarily.

$$\text{ConPurseAck} \hat{=} \text{ConPurse} \setminus (\text{status}, \text{pdAuth})$$

##### 4.9.1 StartFromPurse

A *startFrom* message is valid only if it refers to a different purse from the receiver, and mentions a value for which the *from* purse has sufficient funds.

$\text{ValidStartFrom}$ $\text{ConPurse}$ $m? : \text{MESSAGE}$ $\text{cpd} : \text{CounterPartyDetails}$ $m? \in \text{ran startFrom}$ $\text{cpd} = \text{startFrom} \sim m?$ $\text{cpd.name} \neq \text{name}$ $\text{cpd.value} \leq \text{balance}$
---

To perform the *StartFromPurseEafromOkay* operation, a purse must receive a valid *startFrom* message, and be in *eaFrom*.

$\text{StartFromPurseEafromOkay}$ $\Delta \text{ConPurse}$ $m?, m! : \text{MESSAGE}$ $\text{cpd} : \text{CounterPartyDetails}$ $\text{ValidStartFrom}$ $\text{status} = \text{eaFrom}$ $\exists \text{ConPurseStart}$ $\text{nextSeqNo}' > \text{nextSeqNo}$ $\text{pdAuth}' = (\mu \text{PayDetails} \mid$ $\quad \text{from} = \text{name}$ $\quad \wedge \text{to} = \text{cpd.name}$ $\quad \wedge \text{value} = \text{cpd.value}$ $\quad \wedge \text{fromSeqNo} = \text{nextSeqNo}$ $\quad \wedge \text{toSeqNo} = \text{cpd.nextSeqNo})$ $\text{status}' = \text{epr}$ $m! = \perp$
---

The *StartFromPurseEafromOkay* operation stores the payment details consisting of the counterparty details and its own name and sequence number (for later validation), moves to the *epr* state, increases its sequence number, and sends an unprotected status message.

The *StartFromPurseOkay* operation first aborts (logging the pending payment if necessary, and moving to *eaFrom*), then performs the *StartFromPurse-*



*EafromOkay* operation.

$$\text{StartFromPurseOkay} \triangleq \\ \text{AbortPurseOkay} \wp \text{StartFromPurseEafromOkay} \setminus (\text{cpd})$$

#### 4.9.2 StartToPurse

A *startTo* message is valid only if it refers to a different purse from the receiver.

$\text{ValidStartTo} \text{-----}$ $\text{ConPurse}$ $m? : \text{MESSAGE}$ $\text{cpd} : \text{CounterPartyDetails}$ <hr style="border: 0; border-top: 1px solid black; margin: 5px 0;"/> $m? \in \text{ran startTo}$ $\text{cpd} = \text{startTo} \cdot m?$ $\text{cpd.name} \neq \text{name}$
---

To perform the *StartToPurseEafromOkay* operation, a purse must receive a valid *startTo* message, and be in *eaFrom*.

$\text{StartToPurseEafromOkay} \text{-----}$ $\Delta \text{ConPurse}$ $m?, m! : \text{MESSAGE}$ $\text{cpd} : \text{CounterPartyDetails}$ <hr style="border: 0; border-top: 1px solid black; margin: 5px 0;"/> $\text{ValidStartTo}$ $\text{status} = \text{eaFrom}$ $\exists \text{ConPurseStart}$ $\text{nextSeqNo}' > \text{nextSeqNo}$ $\text{pdAuth}' = (\mu \text{PayDetails}  $ $\quad \text{to} = \text{name}$ $\quad \wedge \text{from} = \text{cpd.name}$ $\quad \wedge \text{value} = \text{cpd.value}$ $\quad \wedge \text{toSeqNo} = \text{nextSeqNo}$ $\quad \wedge \text{fromSeqNo} = \text{cpd.nextSeqNo})$ $\text{status}' = \text{epv}$ $m! = \text{req pdAuth}'$
---

The *StartToPurseOkay* operation logs the pending payment, if necessary; it stores the payment details, consisting of the counterparty details and its own name and sequence number, for later validation; it moves to the *epr* state; it increases its sequence number; and it sends a *req* message containing the stored payment details.

The *StartToPurseOkay* operation first aborts (logging the pending payment if necessary, and moving to *eaFrom*), then performs the *StartToPurseEafromOkay* operation.

$$\text{StartToPurseOkay} \triangleq \\ \text{AbortPurseOkay} \wp \text{StartToPurseEafromOkay} \setminus (\text{cpd})$$

#### 4.9.3 ReqPurse

An authentic request message is a *req* message containing the correct stored payment details (which were stored on receipt of the *startFrom* message).

$\text{AuthenticReqMessage} \text{-----}$ $\text{ConPurse}$ $m? : \text{MESSAGE}$ <hr style="border: 0; border-top: 1px solid black; margin: 5px 0;"/> $m? = \text{req pdAuth}$
---

To perform the *ReqPurseOkay* operation, a purse must receive a *req* message with the payment details, and be in the *epr* state,

$\text{ReqPurseOkay} \text{-----}$ $\Delta \text{ConPurse}$ $m?, m! : \text{MESSAGE}$ <hr style="border: 0; border-top: 1px solid black; margin: 5px 0;"/> $\text{AuthenticReqMessage}$ $\text{status} = \text{epr}$ $\exists \text{ConPurseReq}$ $\text{balance}' = \text{balance} - \text{pdAuth.value}$ $\text{status}' = \text{epa}$ $m! = \text{val pdAuth}$
---

The purse decrements its balance, moves to the *epa* state, and sends a *val* message containing the stored payment details.

#### 4.9.4 ValPurse

An authentic value message is a *val* message containing the correct stored payment details (which were stored on receipt of the *startTo* message).

<i>AuthenticValMessage</i> <i>ConPurse</i> <i>m?</i> : MESSAGE <i>m?</i> = <i>val pdAuth</i>
---

To perform the *ValPurseOkay* operation, a purse must receive a *val* message with the payment details, and be in the *epv* state,

<i>ValPurseOkay</i> $\Delta$ <i>ConPurse</i> <i>m?</i> , <i>m!</i> : MESSAGE <i>AuthenticValMessage</i> <i>status</i> = <i>epv</i> $\exists$ <i>ConPurseVal</i> <i>balance'</i> = <i>balance</i> + <i>pdAuth.value</i> <i>status'</i> = <i>eaTo</i> <i>m!</i> = <i>ack pdAuth</i>
---

The purse increments its balance, moves to the *eaTo* state, and sends an *ack* message containing the stored payment details.

#### 4.9.5 AckPurse

An authentic acknowledge message is an *ack* message containing the correct stored payment details (which were stored on receipt of the *startFrom* message).

<i>AuthenticAckMessage</i> <i>ConPurse</i> <i>m?</i> : MESSAGE <i>m?</i> = <i>ack pdAuth</i>
---

To perform the *AckPurseOkay* operation, a purse must receive an *ack* message with the payment details, and be in the *epa* state.

<i>AckPurseOkay</i> $\Delta$ <i>ConPurse</i> <i>m?</i> , <i>m!</i> : MESSAGE <i>AuthenticAckMessage</i> <i>status</i> = <i>epa</i> $\exists$ <i>ConPurseAck</i> <i>status'</i> = <i>eaFrom</i> <i>m!</i> = $\perp$
---

The purse moves to the *eaFrom* state, and sends an unprotected status message.

### 4.10 Exception logging operations

#### 4.10.1 ReadExceptionLogPurse

To perform the *ReadExceptionLogPurseEafromOkay* operation, a purse must receive a *readExceptionLog* message and be in the *eaFrom* state.

<i>ReadExceptionLogPurseEafromOkay</i> $\exists$ <i>ConPurse</i> <i>m?</i> , <i>m!</i> : MESSAGE <i>m?</i> = <i>readExceptionLog</i> <i>status</i> = <i>eaFrom</i> <i>m!</i> $\in$ $\{\perp\} \cup \{ld : exLog' \bullet exceptionLogResult(name, ld)\}$
---

The operation sends an unprotected status message (modelling 'record not available') or a protected *exceptionLogResult* message containing one of the exception logs tagged with its name<sup>10</sup>.

The *ReadExceptionLogPurseOkay* operation first aborts (logging any pending payment, and moving to *eaFrom*), and then performs the *ReadExceptionLogPurseEafromOkay* operation.

$$ReadExceptionLogPurseOkay \hat{=} AbortPurseOkay \wp ReadExceptionLogPurseEafromOkay$$

<sup>10</sup>This gives a non-deterministic response, because we do not model exception log record numbers.

### 4.10.2 ClearExceptionLogPurse

During a clear log transaction the purse's exception log may change, but no other component can change.

$$\text{ConPurseClear} \hat{=} \text{ConPurse} \setminus (\text{exLog})$$

To perform the *ClearExceptionLogPurseOkay* operation, a purse must have a non-empty exception log and receive a valid *exceptionLogClear* message. If the purse receives a valid *exceptionLogClear* message, has no transaction in progress and has an empty exception log, then the purse ignores the message.

First we define how the purse clears its log in *eaFrom*:

$\text{ClearExceptionLogPurseEafromOkay} \text{ -----}$ $\Delta \text{ConPurse}$ $m?, m! : \text{MESSAGE}$ <hr style="border: 0; border-top: 1px solid black; margin: 5px 0;"/> $\text{exLog} \neq \emptyset$ $m? = \text{exceptionLogClear}(\text{name}, \text{image exLog})$ $\text{status} = \text{eaFrom}$ $\exists \text{ConPurseClear}$ $\text{exLog}' = \emptyset$ $m! = \perp$
--

The purse clears its exception log, and sends an unprotected status message.

The *image* ensures that log messages have at least been read and moved to the archive (see *AuthoriseExLogClear*, section 5.7.1). Procedural mechanisms must ensure that archive information is not lost<sup>11</sup>.

There is a four stage protocol for reading and clearing exception logs: reading a log to the ether, copying a log from the ether to the archive, authorising a purse exception log clear based on what's in the archive, and clearing a purse's exception log having received authorisation. We note that as a result of this protocol, if *ClearExceptionLogPurseOkay* aborts and logs an uncompleted transaction, then the purse's exception log will not be cleared. The reason for this is as follows. The purse gets to *eaFrom* by aborting any uncompleted transaction. If this would create a new exception record, the clear transaction could not occur, because the (imaged) exception log in the message would not match the actual exception log in the purse.

<sup>11</sup>Concrete SP 2.2, 'Exception logging', section 2.3.1.

The full clear exception log operation for a purse is thus defined to abort an uncompleted transaction first, and then clear the log if appropriate.

$$\begin{aligned} \text{ClearExceptionLogPurseOkay} \\ \hat{=} \text{AbortPurseOkay} \text{ } \S \text{ ClearExceptionLogPurseEafromOkay} \end{aligned}$$

---

## Between model, promoted world

### 5.1 The world

The individual purse operations are *promoted* to the 'world of purses'. This world contains the purses, a public *ether* containing all previous messages sent, and a private *archive*, which is a secure store of exception logs, each exception log tagged with the purse that recorded it. Information cannot be deleted from the archive, so that the store of exception logs is persistent. This is to be implemented by mechanisms outside the target of evaluation.

$$\begin{array}{|l} \hline \text{Logbook} : \mathbb{P}(\text{NAME} \leftrightarrow \text{PayDetails}) \\ \hline \text{Logbook} = \mathbb{P}(\{\text{PayDetails} \bullet \text{from} \mapsto \theta \text{PayDetails}\} \\ \cup \{\text{PayDetails} \bullet \text{to} \mapsto \theta \text{PayDetails}\}) \\ \hline \end{array}$$

A *Logbook* is a set of log details, each tagged with a name, where that name is either that of the *to* purse or that of the *from* purse in the log details.

In addition, the *archive*'s tagged log details

$$\begin{array}{|l} \hline \text{ConWorld} \\ \hline \text{conAuthPurse} : \text{NAME} \rightsquigarrow \text{ConPurse} \\ \text{ether} : \mathbb{P} \text{ MESSAGE} \\ \text{archive} : \text{Logbook} \\ \hline \forall n : \text{dom conAuthPurse} \bullet (\text{conAuthPurse } n). \text{name} = n \\ \forall nld : \text{archive} \bullet \text{first } nld \in \text{dom conAuthPurse} \\ \hline \end{array}$$

The *archive* is a *Logbook*. In addition, the *archive*'s tagged log details are tagged only with authentic purse names.

	from	<i>epr</i>	<i>epa</i>	$\begin{pmatrix} \text{diff trans} \\ \text{incl } eaFrom \end{pmatrix}$	
to				no log	log
<i>epv</i>		0	?	0	?
<i>eaTo</i>		×	0	0	0
$\begin{pmatrix} \text{diff trans} \\ \text{incl } eaFrom \end{pmatrix}$	no log	0	0	0	0
	log	0	1	0	1

Figure 5.1: The amount lost on the current transaction for each possible state of the purses. ‘0’ means the value has definitely not been lost; ‘1’ means the value has definitely been lost; ‘?’ means the value may be lost; ‘×’ means that this state is impossible.

## 5.2 Auxiliary definitions

We define some auxiliary components, for ease of proof later. These components are described in detail after the schema. The set *definitelyLost* captures those transactions that have proceeded far enough that we know they cannot succeed. The set *maybeLost* captures those transactions that have proceeded far enough that they will lose money if something goes wrong, but that could equally well continue to successful completion. In the other transactions, either the transaction has not proceeded far enough to lose anything, or has proceeded so far that the value has definitely been received.

The way in which the concrete state of the purses relates to the amount of value ‘lost’ in the transaction can be represented by the table shown in figure 5.1, where the amount lost on the current transaction is shown for each possible state of the purses, including purses that have moved on to a different transaction, with or without logging this one.

```

AuxWorld
ConWorld

allLogs : NAME ↔ PayDetails
authenticFrom, authenticTo : ℙ PayDetails
fromLogged, toLogged : ℙ PayDetails
toInEpv, toInEapayee, fromInEpr, fromInEpa : ℱ PayDetails
definitelyLost : ℙ PayDetails
maybeLost : ℱ PayDetails

allLogs = archive
  ∪ { n : dom conAuthPurse; pd : PayDetails |
    pd ∈ (conAuthPurse n).exLog }

authenticFrom
  = { pd : PayDetails | pd.from ∈ dom conAuthPurse }
authenticTo
  = { pd : PayDetails | pd.to ∈ dom conAuthPurse }

fromLogged = { pd : authenticFrom | pd.from ↦ pd ∈ allLogs }
toLogged = { pd : authenticTo | pd.to ↦ pd ∈ allLogs }

toInEpv = { pd : authenticTo |
  (conAuthPurse pd.to).status = epv
  ∧ (conAuthPurse pd.to).pdAuth = pd }

toInEapayee = { pd : authenticTo |
  (conAuthPurse pd.to).status = eaTo
  ∧ (conAuthPurse pd.to).pdAuth = pd }

fromInEpr = { pd : authenticFrom |
  (conAuthPurse pd.from).status = epr
  ∧ (conAuthPurse pd.from).pdAuth = pd }

fromInEpa = { pd : authenticFrom |
  (conAuthPurse pd.from).status = epa
  ∧ (conAuthPurse pd.from).pdAuth = pd }

definitelyLost = toLogged ∩ (fromLogged ∪ fromInEpa)
maybeLost = (fromInEpa ∪ fromLogged) ∩ toInEpv

```

These auxiliary definitions put no further constraints on the state, but simply

define the derived components. Hence they do not need to be implemented. They are defined merely for ease of use later. We prove that this is so in section 5.2.1 below.

The auxiliary components represent the following:

- *allLogs*: All the exception logs; all those logs in the archive, and those still uncleared in purses.
- *authenticFrom*, *authenticTo*: All possible payment details referring to authentic *from* purses, and authentic *to* purses.
- *fromLogged*: All those payment details logged by a *from* purse.
- *toLogged*: All those details logged by a *to* purse.
- *toInEpv*: All those details for which the *to* purse is authentic, and is currently in *epv* with those details stored. This is a finite set, because *conAuthPurse* is a finite function.
- *toInEapayee*: All those details for which the *to* purse is authentic, and is currently in *eaTo* with those details stored.
- *fromInEpr*: All those details for which the *from* purse is authentic, and is currently in *epr* with those details stored.
- *fromInEpa*: All those details for which the *from* purse is authentic, and is currently in *epa* with those details stored.
- *definitelyLost*: All those details for which we know now that the value has been lost. The *val* message was definitely sent and definitely not received, so ultimately both purses will log the transaction. The authentic *to* purse has logged, which it would not have done had it sent the *ack*, and the authentic *from* purse has sent the *val* and not received the *ack*, and so never will. See figure 5.2
- *maybeLost*: All those details that refer to value that may yet be lost or may yet be transferred successfully from this purse, but which have already definitely *left* the purse. This occurs when the authentic *from* purse has sent the *val* and not received the *ack* and the authentic *to* purse is in *epv*, waiting for the *val* that it may or may not get. See figure 5.2 It is a finite set, because *toInEpv* is a finite set.

We have the identity

$$\begin{aligned} & \text{AuxWorld} \\ & \vdash \\ & \text{definitelyLost} \cup \text{maybeLost} = \\ & (\text{fromInEpa} \cup \text{fromLogged}) \cap (\text{toInEpv} \cup \text{toLogged}) \end{aligned}$$

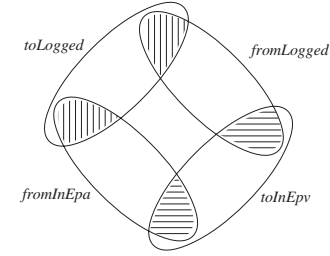


Figure 5.2: The sets *definitelyLost* (vertical hatching) and *maybeLost* (horizontal hatching) as subsets of the other auxiliary definitions.

The later proofs of operations that change purse status (the two start, three protocol and log enquiry operations) are based on how the relevant *pd* moves in and out of the sets *maybeLost* and *definitelyLost*. (These sets are disjoint in the *BetweenWorld*, because of the *BetweenWorld* constraints on log sequence numbers; see lemma ‘lost’, section C.13.)

### 5.2.1 AuxWorld does not add constraints

*AuxWorld* introduces some new variables, but does not add any further constraints on *ConWorld*. We define the schema that represents just the new variables introduced by *AuxWorld*.

$$\text{NewVariables} \hat{=} \exists \text{ConWorld} \bullet \text{AuxWorld}$$

We prove that no further constraints are added by proving the following statement.

$$\text{ConWorld} \vdash \exists_1 \text{NewVariables} \bullet \text{AuxWorld}$$

#### Proof:

First we prove existence. We normalise the schemas, drawing out any predicates hidden in the declarations for the new variables. Only one predicate appears, limiting *allLogs* to be a valid *Logbook*.

$$\text{ConWorld} \vdash \exists_1 \text{NewVariables} \bullet \text{AuxWorld} \wedge \text{allLogs} \in \text{Logbook}$$

Rewrite all the equations for the new variables so that each new variable in *AuxWorld* is defined only in terms of variables of *ConWorld*. We then use the one point rule to remove the existential quantification. This leaves just the normalised predicate in addition to *ConWorld*.

$$\begin{array}{l} \text{ConWorld} \\ \vdash \\ \text{ConWorld} \\ \wedge \text{archive} \cup \{ n : \text{dom conAuthPurse}; pd : \text{PayDetails} \mid \\ \quad pd \in (\text{conAuthPurse } n).exLog \} \\ \in \text{Logbook} \end{array}$$

From the definition of *archive*, *archive* is in *Logbook*. From constraint P-1 in *ConPurse*, the set of named exception logs is also in *Logbook*. This discharges the existence proof.

To prove uniqueness, we need only note that the equations defining the new variables are all equality to an expression, and by the transitivity of equality, all possible values are equal.

■ 5.2.1

### 5.3 Constraints on the ether

We put some further constraints on the state to forbid ‘future messages’ and ‘future logs’, and to record the progress of the protocol.

$$\begin{array}{l} \text{BetweenWorld} \\ \text{AuxWorld} \\ \forall pd : \text{PayDetails} \mid req\ pd \in ether \bullet pd \in authenticTo \\ \\ \forall pd : \text{PayDetails} \mid req\ pd \in ether \bullet \\ \quad pd.toSeqNo < (\text{conAuthPurse } pd.to).nextSeqNo \\ \\ \forall pd : \text{PayDetails} \mid val\ pd \in ether \bullet \\ \quad pd.toSeqNo < (\text{conAuthPurse } pd.to).nextSeqNo \\ \quad \wedge pd.fromSeqNo < (\text{conAuthPurse } pd.from).nextSeqNo \\ \\ \forall pd : \text{PayDetails} \mid ack\ pd \in ether \bullet \\ \quad pd.toSeqNo < (\text{conAuthPurse } pd.to).nextSeqNo \\ \quad \wedge pd.fromSeqNo < (\text{conAuthPurse } pd.from).nextSeqNo \end{array}$$

$$\begin{array}{l} \forall pd : fromLogged \bullet \\ \quad pd.fromSeqNo < (\text{conAuthPurse } pd.from).nextSeqNo \\ \\ \forall pd : toLogged \bullet pd.toSeqNo < (\text{conAuthPurse } pd.to).nextSeqNo \\ \\ \forall pd : fromLogged \mid \\ \quad (\text{conAuthPurse } pd.from).status \in \{epr, epa\} \bullet \\ \quad pd.fromSeqNo \\ \quad \quad < (\text{conAuthPurse } pd.from).pdAuth.fromSeqNo \\ \\ \forall pd : toLogged \mid (\text{conAuthPurse } pd.to).status \in \{epv, eaTo\} \bullet \\ \quad pd.toSeqNo < (\text{conAuthPurse } pd.to).pdAuth.toSeqNo \\ \\ \forall pd : fromInEpr \bullet disjoint (\{val\ pd, ack\ pd\}, ether) \\ \\ \forall pd : \text{PayDetails} \bullet \\ \quad (req\ pd \in ether \wedge ack\ pd \notin ether) \\ \quad \Leftrightarrow (pd \in toInEpr \cup toLogged) \\ \\ \forall pd : \text{PayDetails} \mid val\ pd \in ether \wedge pd \in toInEpr \bullet \\ \quad pd \in fromInEpa \cup fromLogged \\ \\ \forall pd : fromInEpa \cup fromLogged \bullet req\ pd \in ether \\ \\ toLogged \in \mathbb{F} \text{PayDetails} \\ \\ \forall pd : exceptionLogResult \sim (\{ ether \}) \bullet pd \in allLogs \\ \\ \forall pds : \mathbb{P}_1 \text{PayDetails}; name : NAME \mid \\ \quad exceptionLogClear(name, image\ pds) \in ether \bullet \\ \quad \{name\} \times pds \subseteq archive \\ \\ \forall pd : fromLogged \cup toLogged \bullet req\ pd \in ether \end{array}$$

These constraints express the following conditions (numbered for future reference in the refinement proofs):

B-1 All *req* messages in the *ether* refer to authentic *to* purses<sup>1</sup>.

B-2 There are no ‘future’ *req* messages<sup>2</sup>: all *req* messages in the *ether* hold a *to* purse sequence number less than that purse’s next sequence num-

<sup>1</sup>Used in *Req*, case 4, section 18.10.

<sup>2</sup>Used in: *StartTo*, location of *pdThis*, section 17.3; *CStartTo*, B-16, section 29.3; *CReq*, B-3, section 29.4.

ber. (It puts no constraint on the *from* purse's sequence number, because the *from* purse mentioned in a *req* message need not have started the transaction yet, and need not even be authentic.)

- B-3 There are no 'future' *val* messages<sup>3</sup>: all *val* messages in the *ether* hold a *to* purse sequence number less than that purse's next sequence number and a *from* purse sequence number less than that purse's next sequence number.
- B-4 There are no 'future' *ack* messages<sup>4</sup>: all *ack* messages in the *ether* hold a *to* purse sequence number less than that purse's next sequence number and a *from* purse sequence number less than that purse's next sequence number.
- B-5 There are no 'future' *from* logs based on the *nextSeqNo* of the *from* purse<sup>5</sup>.
- B-6 There are no 'future' *to* logs based on the *nextSeqNo* of the *to* purse<sup>6</sup>.
- B-7 There are no 'future' *from* logs based on the *pdAuth.fromSeqNo* of a purse in *epr* or *epa*<sup>7</sup>: all *from* logs refer only to past *from* transactions. So all *from* logs referring to a purse that is currently in a transaction as a *from* purse (that is, in *epr* or *epa*), hold a *from* sequence number strictly less than that purse's stored current transaction sequence number.
- B-8 There are no 'future' *to* logs based on the *pdAuth.toSeqNo* of a purse in *epv* or *eaTo*<sup>8</sup>: all *to* logs refer only to past *to* transactions. So all *to* logs referring to a purse that is currently in a transaction as a *to* purse (in *epv*), hold a *to* sequence number strictly less than that purse's stored current transaction sequence number.
- B-9 If the *from* purse is in *epr* then there is no *val* message<sup>9</sup> or *ack* message<sup>10</sup> in the *ether*.
- B-10 There is a *req* message but no *ack* message in the *ether* precisely when the *to* purse is in *epv* or has logged the transaction<sup>11</sup>.

<sup>3</sup>Used in: *CStartFrom*, B-9, section 29.2; *CStartTo*, B-11, section 29.3. *CVal*, B-4, section 29.5.

<sup>4</sup>Used in: *CStartFrom*, B-9, section 29.2; *CStartTo*, B-10, section 29.3.

<sup>5</sup>Used in: *CStartFrom*, B-7, section 29.2.

<sup>6</sup>Used in: *CStartTo*, B-8, 29.3. 29.3

<sup>7</sup>Used in: *StartFrom*, location of *pdThis*, section 16.3; *CReq*, B-7, section 29.4; lemma 'notLoggedAndIn', section C.12.

<sup>8</sup>Used in: *CVal*, B-8, section 29.5; lemma 'notLoggedAndIn', section C.12.

<sup>9</sup>Used in: *CVal*, B-9, section 29.5.

<sup>10</sup>Used in *Req*, case 4, section 18.10.

<sup>11</sup>Used in: *StartTo*, location of *pdThis*, section 17.3; *Req*, case 4, section 18.10; *Ack*, behaviour of *definitelyLost*, section 20.6.5; *Ack*, behaviour of *maybeLost*, section 20.6.6; *CAbort*, B-10, section 28.5; *CAbort*, B-16, section 28.5; *CAck*, B-11, section 29.6.

- B-11 If the *to* purse is in *epv* and there is a *val* message in the *ether*, then either the *from* purse is in *epa* or has logged the transaction<sup>12</sup>.
- B-12 If the *from* purse is in *epa* or has logged the transaction, then there is a *req* in the *ether*<sup>13</sup>.
- B-13 The set *toLogged* is finite. This is sufficient to ensure that *definitelyLost* is finite<sup>14</sup>.
- B-14 Log result messages are logged. The log details of any *exceptionLogResult* message in the *ether* is either archived or in a purse transaction exception log<sup>15</sup>.
- B-15 Exception log clear messages refer only to archived logs<sup>16</sup>.
- B-16 For each *PayDetails* in the logs there is a corresponding *PayDetails* in a *req* message in the *ether*<sup>17</sup>.

That the actual implementation does indeed satisfy this predicate needs to be proved, by a further, small, refinement, that *ConWorld* and the operations refine *BetweenWorld* and the operations (see Part III).

## 5.4 Framing schema

A framing schema is used to promote the purse operations.

<sup>12</sup>Used in: *Val*, behaviour of *maybeLost*, section 19.6.7.

<sup>13</sup>Used in *StartTo*, location of *pdThis*, section 17.3; *CAbort*, B-12, section 28.5; *CAbort*, B-16, section 28.5.

<sup>14</sup>Used in: various *Rab* schemas, section 10.1

<sup>15</sup>Used in: *Archive*, section 24.2; *CArchive*, section 29.10.

<sup>16</sup>Used in: *ExceptionLogClear*, invoking lemma 'lost unchanged' section 22.2; *CExceptionLogClear*, section 29.8.

<sup>17</sup>Used in: *CStartTo*, alternative to lemma 'logs unchanged', section 29.3.



$\Phi BOp$ $\Delta BetweenWorld$ $\Delta ConPurse$ $m?, m! : MESSAGE$ $name? : NAME$ <hr/> $m? \in ether$ $name? \in \text{dom } conAuthPurse$ $\theta ConPurse = conAuthPurse \text{ name?}$ $conAuthPurse' = conAuthPurse \oplus \{name? \mapsto \theta ConPurse'\}$ $archive' = archive$ $ether' = ether \cup \{m!\}$
--

The predicate ensures the following properties common to all promoted operations:

- $m? \in ether$   
the input message is in the *ether*, which ensures it was either previously sent by another purse (*req*, *val*, *ack*, etc.), in the ether since initialisation (*startFrom*, *startTo*, etc.), or input by a special global operation (that is, *AuthoriseExLogClear*).
- $name? \in \text{dom } conAuthPurse$   
the purse is in the world of authentic purses.
- $\theta ConPurse = conAuthPurse \text{ name?}$   
The before state of *ConPurse* we are operating on is the state of the purse identified by *name?*
- $conAuthPurse' = conAuthPurse \oplus \{name? \mapsto \theta ConPurse'\}$   
The after state of the purse system has *name?* updated to the after state of *ConPurse* (which particular state depends on the particular operation details) and all other purses are unchanged<sup>18</sup>.
- $archive' = archive$   
The archive remains unchanged.
- $ether' = ether \cup \{m!\}$   
the output message is recorded by the *ether*.

<sup>18</sup>Used in *Req* proof, section 18.7.2.

## 5.5 Ignore, Increase and Abort

There are various general behaviours that operations may engage in: ignore the input and do nothing; ignore the input but increase the sequence number; ignore the input but abort the current payment transaction.

Ignoring is modelled as an unchanging world:

$$Ignore \hat{=} [\exists BetweenWorld; name? : NAME; m?, m! : MESSAGE \mid m! = \perp]$$

Increase has been modelled at the purse level, and is now promoted and totalised:

$$Increase \hat{=} Ignore \vee (\exists \Delta ConPurse \bullet \Phi BOp \wedge IncreasePurseOkay)$$

Abort has been modelled at the purse level, and is now promoted and totalised:

$$Abort \hat{=} Ignore \vee (\exists \Delta ConPurse \bullet AbortPurseOkay \wedge [\Phi BOp \mid m! = \perp])$$

## 5.6 Promoted operations

We promote the individual purse operations, and make them total by disjoining them with the operation defined above that does nothing.

### 5.6.1 Value transfer operations

The promoted start operations are:

$$StartFrom \hat{=} Ignore \vee Abort \vee (\exists \Delta ConPurse \bullet \Phi BOp \wedge StartFromPurseOkay)$$

$$StartTo \hat{=} Ignore \vee Abort \vee (\exists \Delta ConPurse \bullet \Phi BOp \wedge StartToPurseOkay)$$

For use in the proofs, we also promote the *Eafrom* part of the operations on their own:

$$\begin{aligned} \text{StartFromEafromOkay} &\hat{=} \exists \Delta \text{ConPurse} \bullet \\ &\quad \Phi \text{BOP} \wedge \text{StartFromPurseEafromOkay} \\ \text{StartToEafromOkay} &\hat{=} \exists \Delta \text{ConPurse} \bullet \\ &\quad \Phi \text{BOP} \wedge \text{StartToPurseEafromOkay} \end{aligned}$$

The promoted protocol operations are:

$$\begin{aligned} \text{Req} &\hat{=} \text{Ignore} \vee (\exists \Delta \text{ConPurse} \bullet \Phi \text{BOP} \wedge \text{ReqPurseOkay}) \\ \text{Val} &\hat{=} \text{Ignore} \vee (\exists \Delta \text{ConPurse} \bullet \Phi \text{BOP} \wedge \text{ValPurseOkay}) \\ \text{Ack} &\hat{=} \text{Ignore} \vee (\exists \Delta \text{ConPurse} \bullet \Phi \text{BOP} \wedge \text{AckPurseOkay}) \end{aligned}$$

### 5.6.2 Exception log operations

The promoted log enquiry operation is:

$$\begin{aligned} \text{ReadExceptionLog} &\hat{=} \text{Ignore} \\ &\quad \vee (\exists \Delta \text{ConPurse} \bullet \Phi \text{BOP} \wedge \text{ReadExceptionLogPurseOkay}) \end{aligned}$$

The promoted exception log clear operation is:

$$\begin{aligned} \text{ClearExceptionLog} &\hat{=} \text{Ignore} \\ &\quad \vee \text{Abort} \\ &\quad \vee (\exists \Delta \text{ConPurse} \bullet \Phi \text{BOP} \wedge \text{ClearExceptionLogPurseOkay}) \end{aligned}$$

For use in the proofs, we also promote the *Eafrom* part of the operations on their own:

$$\begin{aligned} \text{ReadExceptionLogEafromOkay} &\hat{=} \exists \Delta \text{ConPurse} \bullet \\ &\quad \Phi \text{BOP} \wedge \text{ReadExceptionLogPurseEafromOkay} \\ \text{ClearExceptionLogEafromOkay} &\hat{=} \exists \Delta \text{ConPurse} \bullet \\ &\quad \Phi \text{BOP} \wedge \text{ClearExceptionLogPurseEafromOkay} \end{aligned}$$

## 5.7 Operations at the world level only

There are some operations on the world that do not have equivalents on individual purses. These are not implemented by the target of evaluation, but need to be implemented by some manual means or external system.

To retain the simplicity of our proof rules, these operations take the same input and outputs as all the purse operations.

### 5.7.1 Exception Log clear authorisation

The message to clear an exception log can be created only for log details which are already recorded in the archive. The clear code of the message is based on the selected logs in the archive. The exception log clear message couples this clear code with the name of a purse. This supports constraint B-15 which requires that this operation not put a clear message into the ether if the relevant logs have not been archived.

$\begin{aligned} &\text{AuthoriseExLogClearOkay} \text{ -----} \\ &\Delta \text{BetweenWorld} \\ &m?, m! : \text{MESSAGE} \\ &\text{name?} : \text{NAME} \\ &\text{conAuthPurse}' = \text{conAuthPurse} \\ &\exists pds : \mathbb{P}_1 \text{ PayDetails} \bullet \\ &\quad \{\text{name?}\} \times pds \subseteq \text{archive} \\ &\quad \wedge m! = \text{exceptionLogClear}(\text{name?}, \text{image } pds) \\ &\text{ether}' = \text{ether} \cup \{m!\} \\ &\text{archive} = \text{archive}' \end{aligned}$
---

$$\text{AuthoriseExLogClear} \hat{=} \text{Ignore} \vee \text{AuthoriseExLogClearOkay}$$

Exception logs must be kept for all time to ensure that all value remains accounted for. The operation to clear purses of their exception logs must be supported by a mechanism to store the cleared logs. This is what the archive supplies.

The purse supports the *ReadExceptionLog* operation, which puts an exception log record into the *ether* as a message. As the system implementers have no control over the *ether*, we have modelled it as lossy at the concrete level, allowing for messages to be lost from the *ether* at any time. The *archive* is a *secure* store for information, and to support the security of the purse there must be a manual mechanism to move log messages from the *ether* into the *archive* for safe keeping. This is modelled by the *Archive* operation, and is implemented by some mechanism external to the target of evaluation.

<i>Archive</i>
$\Delta$ <i>BetweenWorld</i>
$m?, m! : MESSAGE$
$name? : NAME$
$conAuthPurse' = conAuthPurse$
$ether' = ether$
$archive \subseteq$
$archive' \subseteq$
$archive \cup \{ log : NAME \times PayDetails \mid$
$exceptionLogResult log \in ether \}$
$m! = \perp$

This operation non-deterministically copies some exception log information from messages in the *ether* into the *archive*. It ignores its inputs. As one possible behaviour is to move *no* messages into the archive, it can behave exactly like *Ignore*. The operation is therefore total, and we do not need to disjoin it with *Ignore*.

### 5.8 Forging messages

If arbitrary messages can be sent, then obviously the security can be compromised. We can build into the definition of the *ether* that it is possible to forge only some kinds of messages. The only messages it is possible to forge are

- replays of earlier valid messages (added to the *ether* during an earlier operation)
- unprotected messages (modelled by being in the initial *ether*, and hence being replayable at any time)
- messages it is possible to detect are forged (modelled by the  $\perp$  message, present in the initial *ether*)

This allows us to capture the encryption properties of messages: a message encapsulating arbitrary details cannot be forged by a third party.

### 5.9 The complete protocol

The complete transfer at the between and concrete levels can be described, informally, by the following sequence of operations:

*StartFrom* § *StartTo* § *Req* § *Val* § *Ack*

Other operations may be interleaved in an actual transfer.

The refinement proof in the following sections demonstrates that none of the individual concrete operations violates the security policy.

---

## Between model, initialisation and finalisation

### 6.1 Initialisation

As with the abstract case, we set up a particular initial between state. We do not want to model adding new authentic purses to the system, since some of the operations involved are outside the security boundary. So we allow the world to be ‘switched off’ and a new world ‘switched on’, where the new world consists of the old world as it was, plus the new purses. So our initial state must allow purses to be part-way through transactions.

We set constraints on the initial state of the between system to say that there are all the request messages in the *ether*, any current transactions must be valid, and there are no future messages.

<i>BetweenInitState</i> <i>BetweenWorld'</i> { <i>readExceptionLog</i> , $\perp$ } $\cup$ $\cup \{ cpd : CounterPartyDetails \bullet \{ startFrom cpd, startTo cpd \} \}$ $\subseteq ether'$
---

The initial *ether* contains (or may be considered to contain) the following messages:

- the log enquiry and  $\perp$  messages (hence a purse can always have a forged message sent to it)
- all possible start messages, even those referring to a non-authentic purse

- no future messages (ensured by the constraints in *BetweenWorld'*)

So any purse, at any time, can be sent a read log message, or an instruction to start a transfer; this saves us having to model the IFD sending these messages. Since the IFD does not authenticate start messages, we cannot insist on authentic purses at this point.

The inability to forge messages means that a *req* message always mentions an authentic *to* purse, and a *val* message an authentic *from* purse. So a *val* message sent on receipt of a *req* will mention authentic *to* and *from* purses.

We must also initialise our concrete inputs, since they are different from the global inputs. This defines how concrete inputs are interpreted.

<i>BetwInItIn</i>
$g? : AIN$
$m? : MESSAGE$
$name? : NAME$
$m? \in \text{ran } req \Rightarrow$ $g? = \text{transfer}(\mu \text{ TransferDetails} \mid$ $\quad from = (req \sim m?).from$ $\quad \wedge to = (req \sim m?).to$ $\quad \wedge value = (req \sim m?).value)$
$m? \notin \text{ran } req \Rightarrow g? = aNullIn$

## 6.2 Finalisation

Finalisation maps a *BetweenWorld* to a *GlobalWorld*, to specify how the various concrete state components are observed abstractly.

We finalise by choosing to assume that all the transactions in *maybeLost* actually are lost. (In some sense, finalisation treats incomplete transactions as if they would 'abort'.)

<i>BetwFinState</i>
<i>BetweenWorld</i>
<i>GlobalWorld</i>
$\text{dom } gAuthPurse = \text{dom } conAuthPurse$
$\forall name : \text{dom } conAuthPurse \bullet$ $\quad (gAuthPurse \ name).balance = (conAuthPurse \ name).balance$ $\quad \wedge (gAuthPurse \ name).lost =$ $\quad \quad \text{sumValue}((definitelyLost \cup maybeLost)$ $\quad \quad \cap \{ld : PayDetails \mid ld.from = name\})$

There is a simple relationship between concrete and global *balance* components. The global *lost* component is related to the concrete *maybeLost* and *definitelyLost* logs (the function *sumValue* is defined in section D.3).

We must also finalise our concrete outputs, since they are different from the global outputs. This defines how concrete outputs are interpreted.

<i>BetwFinOut</i>
$g! : AOUT$
$m! : MESSAGE$
$g! = aNullOut$

All concrete outputs are interpreted as the single abstract output, *aNullOut*.

---

## Concrete model: implementation

### 7.1 Concrete World State

The  $C$  world state has the same components as the  $B$  state; we decorate with a subscript zero to distinguish like-named  $B$  and  $C$  components.

Since  $\Delta ConWorld_0$  has components dashed-then-subscripted, whereas we require subscripted-then-dashed, we defined our own  $\Delta$  and  $\Xi$  schemas.

$$\Delta ConWorld_0 \hat{=} ConWorld_0 \wedge ConWorld'_0$$

$$\Xi ConWorld_0 \hat{=} [ \Delta ConWorld_0 \mid \theta ConWorld_0 = \theta ConWorld'_0 ]$$

### 7.2 Framing Schema

The concrete world  $C$  has the same operations as the  $B$  model.

The world we promote to is *ConWorld*, not *BetweenWorld*. (Remember *ConWorld* has the same structure as *BetweenWorld*, but none of the constraints about future messages.) We are also allowed to ‘lose’ messages from the public *ether*, which models the fact that the *ether* may be implemented as a lossy medium.

So the  $C$  framing schema is used to promote the purse operations.

$\Phi COp$
$\Delta ConWorld0$ $\Delta ConPurse$ $m?, m! : MESSAGE$ $name? : NAME$
$m? \in ether_0$ $name? \in \text{dom } conAuthPurse_0$ $\theta ConPurse = conAuthPurse_0 \text{ name?}$ $conAuthPurse'_0 = conAuthPurse_0 \oplus \{name? \mapsto \theta ConPurse'\}$ $archive'_0 = archive_0$ $ether'_0 \subseteq ether_0 \cup \{m!\}$

### 7.3 Ignore, Increase and Abort

The  $\mathcal{B}$  operations *Ignore*, *Increase* and *Abort* have  $C$  equivalents, working on the  $C$  world instead of the  $\mathcal{B}$  world. These operations are not named operations of the purse, i.e. they are not visible at the purse interface. We define them so that they can be used as *components* in  $C$  purse operations.

$$\begin{aligned}
CIgnore &\hat{=} [\exists ConWorld0; name? : NAME; m?, m! : MESSAGE \mid m! = \perp] \\
CIncrease &\hat{=} CIgnore \\
&\quad \vee (\exists \Delta ConPurse \bullet \Phi COp \wedge IncreasePurseOkay) \\
CAbort &\hat{=} CIgnore \\
&\quad \vee (\exists \Delta ConPurse \bullet AbortPurseOkay \wedge [\Phi COp \mid m! = \perp])
\end{aligned}$$

All subsequent operations defined in this chapter correspond to the actual operations of the purse.

### 7.4 Promoted operations

As with the  $\mathcal{B}$  promoted operations, the  $C$  promoted operations are made total by disjoining with *CIgnore*.

#### 7.4.1 Value transfer operations

The promoted start operations are:

$$\begin{aligned}
CStartFrom &\hat{=} CIgnore \\
&\quad \vee CAbort \\
&\quad \vee (\exists \Delta ConPurse \bullet \Phi COp \wedge StartFromPurseOkay) \\
CStartTo &\hat{=} CIgnore \\
&\quad \vee CAbort \\
&\quad \vee (\exists \Delta ConPurse \bullet \Phi COp \wedge StartToPurseOkay)
\end{aligned}$$

The promoted protocol operations are:

$$\begin{aligned}
CReq &\hat{=} CIgnore \vee (\exists \Delta ConPurse \bullet \Phi COp \wedge ReqPurseOkay) \\
CVal &\hat{=} CIgnore \vee (\exists \Delta ConPurse \bullet \Phi COp \wedge ValPurseOkay) \\
CAck &\hat{=} CIgnore \vee (\exists \Delta ConPurse \bullet \Phi COp \wedge AckPurseOkay)
\end{aligned}$$

#### 7.4.2 Exception log operations

The promoted log enquiry operation is:

$$\begin{aligned}
CReadExceptionLog &\hat{=} CIgnore \\
&\quad \vee (\exists \Delta ConPurse \bullet \Phi COp \wedge ReadExceptionLogPurseOkay)
\end{aligned}$$

The promoted clear operation is:

$$\begin{aligned}
CClearExceptionLog &\hat{=} CIgnore \\
&\quad \vee CAbort \\
&\quad \vee (\exists \Delta ConPurse \bullet \Phi COp \wedge ClearExceptionLogPurseOkay)
\end{aligned}$$

### 7.5 Operations at the world level only

As with the  $\mathcal{B}$  model, there are some operations that act on the world, rather than on individual purses. These operations are specified exactly as they are in the  $\mathcal{B}$  model, but acting on *ConWorld* instead of *BetweenWorld*.

### 7.5.1 Exception Log clear authorisation

The message to clear an exception log is generated external to the model.

$$CAuthoriseExLogClear \hat{=} CIgnore \\ \vee ( \exists \exists ConPurse \bullet [ \Phi COP \mid ( \exists lds : \mathbb{P}_1 PayDetails \mid \\ \{ name? \} \times lds \subseteq archive_0 \bullet \\ m! = exceptionLogClear(name?, image lds) ) ] )$$

The operation to move exception log information from the *ether* to the *archive* is

$ \begin{array}{l} \overline{CArchive} \\ \Delta ConWorld_0 \\ m?, m! : MESSAGE \\ name? : NAME \\ \hline conAuthPurse'_0 = conAuthPurse_0 \\ ether'_0 \subseteq ether_0 \\ archive_0 \subseteq \\ \quad archive'_0 \subseteq \\ \quad\quad archive_0 \cup \{ log : NAME \times PayDetails \mid \\ \quad\quad\quad exceptionLogResult log \in ether_0 \} \\ \hline m! = \perp \end{array} $
---

### 7.6 Initial state

The initial state of the *C* world has an ether that is a subset of one that satisfies the 'no future messages' constraints placed on the *B* world (the subset is needed because the *C* ether is lossy).

$ \begin{array}{l} \overline{ConInitState} \\ \overline{ConWorld'_0} \\ \hline \exists BetweenWorld' \mid BetweenInitState \bullet \\ \quad conAuthPurse'_0 = conAuthPurse' \\ \quad \wedge archive'_0 = archive' \\ \quad \wedge \{ \perp \} \subseteq ether'_0 \subseteq ether' \end{array} $
---

### 7.7 Finalisation

The *B* finalisation is defined for any *ConWorld*; we reuse it for the *C* finalisation.

$ \begin{array}{l} \overline{ConFinState} \\ \overline{AuxWorld_0} \\ \overline{GlobalWorld} \\ \hline dom gAuthPurse = dom conAuthPurse_0 \\ \forall name : dom conAuthPurse_0 \bullet \\ \quad (gAuthPurse name).balance \\ \quad = (conAuthPurse_0 name).balance \\ \quad \wedge (gAuthPurse name).lost = \\ \quad\quad sumValue((definitelyLost_0 \cup maybeLost_0) \\ \quad\quad \cap \{ ld : PayDetails \mid ld.from = name \}) \end{array} $
---



## Model consistency proofs

### 8.1 Introduction

In order to increase confidence that the specifications written are not meaningless, it is wise to prove some properties of them.

The least that should be done is to demonstrate that the constraints on the state and those defining each operation do not reduce to *false*. So for each model, the consistency proof obligations are:

- Show it is possible for at least one state to exist (which demonstrates that the state invariant is not contradictory). If we choose this state to be the initial state, we also demonstrate that initialisation is not vacuous, too.

$$\vdash \exists State' \bullet StateInit$$

- Show that each operation does not have an empty precondition (which demonstrates that no operation definition is contradictory).

$$\vdash \exists State, Input \bullet pre Op$$

In fact, here we show that all our operations are total, which is the much stronger condition

$$\vdash \forall State, Input \bullet pre Op$$

We present these proofs for each of our three models below.

## 8.2 Abstract model consistency proofs

### 8.2.1 Existence of initial abstract state

$$\vdash \exists AbWorld' \bullet AbInitState$$

**Proof:**

It is sufficient to find an explicit abstract world that satisfies the constraints of *AbInitState*. Consider the abstract world with the components:

$$abAuthPurse' = \emptyset$$

This satisfies the constraints of *AbWorld*, so is clearly a suitable initial state.

■ 8.2.1

### 8.2.2 Totality of abstract operations

*AbIgnore* is total.

**Proof:**

$$\begin{aligned} & \text{pre } AbIgnore \\ &= \text{pre } [ \Delta AbWorld; a? : AIN; a! : AOUT \mid \\ & \quad abAuthPurse' = abAuthPurse \\ & \quad \wedge a! = aNullOut ] \quad [\text{defn. } AbIgnore] \\ &= [ AbWorld; a? : AIN \mid \\ & \quad \exists AbWorld'; a! : AOUT \mid \\ & \quad \quad abAuthPurse' = abAuthPurse \\ & \quad \quad \wedge a! = aNullOut ] \quad [\text{defn. pre}] \\ &= [ AbWorld; a? : AIN \mid \\ & \quad \exists abAuthPurse' : NAME \leftrightarrow AbPurse; a! : AOUT \mid \\ & \quad \quad abAuthPurse' = abAuthPurse \\ & \quad \quad \wedge a! = aNullOut ] \quad [\text{one point rule}] \\ &= [ AbWorld; a? : AIN ] \end{aligned}$$

■

All the abstract operations are total.

**Proof:**

They are total by construction. They are all of the form *AbOpOkay*  $\vee$  *AbIgnore*, so:

$$\begin{aligned} & \text{pre } AbOp \\ &= \text{pre } (AbOpOkay \vee AbIgnore) \\ &= \text{pre } AbOpOkay \vee \text{pre } AbIgnore \\ &= \text{pre } AbOpOkay \vee [ AbWorld; a? : AIN ] \\ &= [ AbWorld; a? : AIN ] \end{aligned}$$

■

■ 8.2.2

■ 8.2

## 8.3 Between model consistency proofs

### 8.3.1 Existence of between initial state

$$\vdash \exists BetweenWorld' \bullet BetweenInitState$$

**Proof:**

It is sufficient to find an explicit between world that satisfies the constraints of *BetweenWorldInit*.

A world of no purses, an *ether* that consists of exactly the messages explicitly allowed of *BetweenWorldInit*, and an empty *archive*, is sufficient.

$$\begin{aligned} conAuthPurse' &= \emptyset \\ ether' &= \{ readExceptionLog, \perp \} \\ & \quad \cup \cup \{ cpd : CounterPartyDetails \bullet \{ startFrom cpd, startTo cpd \} \} \\ archive' &= \emptyset \end{aligned}$$

This satisfies the constraints in *ConWorld*. It also satisfies the extra constraints of *BetweenWorld*: all the quantifiers are over empty sets (of purses or messages) and hence are trivially true.

■ 8.3.1

### 8.3.2 Totality of between operations

All between operations are total.

**Proof:**

They all offer the option of *Ignore* (explicitly by disjunction, except for *Archive*, which offers it implicitly). *Ignore* is the total identity operation.

- 8.3.2
- 8.3

## 8.4 Concrete model consistency proofs

### 8.4.1 Existence of concrete initial state

$\vdash \exists \text{ConWorld}'_0 \bullet \text{ConInitState}$

**Proof:**

The concrete state is identical to the between state, except for fewer constraints. Therefore as a between state exists, so does a concrete one.

- 8.4.1

### 8.4.2 Totality of concrete operations

All concrete operations are total.

**Proof:**

The concrete operations are identical to the between ones. Therefore if the between operations are total, so are the concrete ones.

- 8.4.2
- 8.4
- 8

## Part II

# First Refinement: $\mathcal{A}$ to $\mathcal{B}$

---

## Refinement Proof Rules

### 9.1 Security of the implementation

We prove the concrete model  $C$  is secure with respect to the abstract model  $\mathcal{A}$  in two stages. We first show (in this part) that  $\mathcal{B}$  refines  $\mathcal{A}$  then we show (in part III) that  $C$  refines  $\mathcal{B}$ .

To show that  $\mathcal{B}$  refines  $\mathcal{A}$  we show that every (promoted)  $\mathcal{B}$  operation correctly refines some  $\mathcal{A}$  operation.

Much of what the  $\mathcal{B}$  (and  $C$ ) operations achieve is invisible at the  $\mathcal{A}$  level, so many  $\mathcal{B}$  operations are refinements of *AbIgnore* (abstractly 'do nothing'). Some of the  $\mathcal{B}$  operations that are refinements of *AbIgnore* do serve to resolve abstract non-determinism.

The refinements are

*AbTransfer*  $\sqsubseteq$  *Req*

*AbIgnore*  $\sqsubseteq$  *StartFrom*

$\vee$  *StartTo*

$\vee$  *Val*

$\vee$  *Ack*

$\vee$  *ReadExceptionLog*

$\vee$  *ClearExceptionLog*

$\vee$  *AuthoriseExLogClear*

$\vee$  *Archive*

$\vee$  *Ignore*

$\vee$  *Increase*

$\vee$  *Abort*

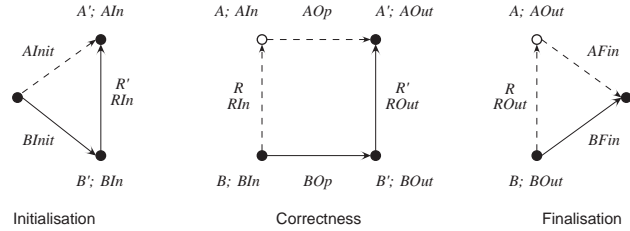


Figure 9.1: A summary of the backward proof rules. The hypothesis is the existence of the lower (solid) path. The proof obligation is to demonstrate the existence of an upper (dashed) path.

Each of these refinements must be proved correct.

For the  $\mathcal{A}$  to  $\mathcal{B}$  refinement proofs, the following set of ‘upward’ or ‘backward’ proof rules are sufficient to show the refinement [Woodcock & Davies 1996]. For the  $\mathcal{B}$  to  $\mathcal{C}$  refinement proofs, the ‘downward’ or ‘forward’ proof rules are sufficient to show the refinement.

These rules are expressed in terms of a ‘concrete’ (lower) and ‘abstract’ (upper) model. In this first refinement the ‘abstract’ model is  $\mathcal{A}$  and the ‘concrete’ model is  $\mathcal{B}$ . In the second refinement the ‘abstract’ model is now  $\mathcal{B}$  and the ‘concrete’ model is  $\mathcal{C}$ .

## 9.2 Backwards rules proof obligations

Appendix A describes the syntax for theorems, and how we lay out the proofs. The backward proof rules are summarised in figure 9.1, and described below.

### 9.2.1 Initialisation

We start from some global state  $G$ , and *initialise* it to an abstract initial state  $A'$  and concrete initial state  $B'$ . These must be related by the retrieve.

$$\vdash \forall G; GIn; B'; BIn; A'; AIn \mid BInitState \wedge BInitIn \wedge R' \wedge RIn \bullet \\ AInitState \wedge AInitIn$$

Given any global initial state  $G$ , if we initialise it with  $BInit$  to  $B'$ , then retrieve  $B'$  to  $A'$ , we must get the same abstract initial state as if we had initialised directly to  $A'$  using  $AInit$ .

This can be simplified to:

$$BInitState; R' \vdash AInitState \\ BInitIn; RIn \vdash AInitIn$$

### 9.2.2 Finalisation

We start from some abstract final state  $A$  and concrete final state  $B$ , related by the retrieve, and *finalise* them to the *same* global final state  $G'$ .

$$\vdash \forall G'; GOut; B; BOut \mid BFinState \wedge BFinOut \bullet \\ \exists A; AOut \bullet R \wedge ROut \wedge AFinState \wedge AFinOut$$

Given any concrete final state  $B$  that finalises with  $BFin$  to  $G'$ , then it is possible to find a corresponding abstract final state  $A$ , that both retrieves from  $B$  and finalises with  $AFin$  to the same  $G'$ .

This can be simplified to:

$$BFinState \vdash \exists A \bullet R \wedge AFinState \\ BFinOut \vdash \exists AOut \bullet ROut \wedge AFinOut$$

### 9.2.3 Applicability

$$\vdash \forall B; BIn \mid (\forall A; AIn \mid R \wedge RIn \bullet \text{pre } AOp) \bullet \text{pre } BOp$$

For each operation: if we are in a concrete state, and if all the abstract states to which it retrieves satisfy the precondition of the abstract operation, then we must also satisfy the precondition of the corresponding concrete operation.

For our case,  $AOp$  is total (this needs to be proved for each of the abstract operations — see section 8.2.2). So  $\text{pre } AOp = \text{true}$ . So

$$(\forall A; AIn \mid R \wedge RIn \bullet \text{pre } AOp) \\ \Rightarrow (\forall A; AIn \bullet R \wedge RIn \Rightarrow \text{pre } AOp) \\ \Rightarrow (\forall A; AIn \bullet R \wedge RIn \Rightarrow \text{true}) \\ \Rightarrow (\forall A; AIn \bullet \text{true}) \\ \Rightarrow \text{true}$$

So, for total abstract operations, the applicability proof obligation reduces to

$$B; BIn \vdash \text{pre } BOp$$

That is, a proof that  $BOp$  is total, too. This is discharged in section 8.3.2.

## 9.2.4 Correctness

$$\begin{aligned} \vdash \forall B; BIn \mid (\forall A; AIn \mid R \wedge RIn \bullet \text{pre } AOp) \bullet \\ (\forall A'; AOut; B'; BOut \mid BOp \wedge R' \wedge ROut \bullet \\ (\exists A; AIn \bullet R \wedge RIn \wedge AOp)) \end{aligned}$$

For each operation: if we start in a concrete state corresponding to the precondition of the abstract operation (the applicability condition ensures we then satisfy the concrete operation's precondition), and do the concrete operation, and then retrieve to the abstract state, then we end up in a state that we could have reached doing the abstract operation.

Using  $\text{pre } AOp = \text{true}$  (proved during applicability), this reduces to

$$\begin{aligned} \vdash \forall B; BIn \bullet (\forall A'; AOut; B'; BOut \mid BOp \wedge R' \wedge ROut \bullet \\ (\exists A; AIn \bullet R \wedge RIn \wedge AOp)) \end{aligned}$$

Moving the quantifier into the hypothesis:

$$\begin{aligned} B; BIn; A'; AOut; B'; BOut \mid BOp \wedge R' \wedge ROut \\ \vdash \exists A; AIn \bullet R \wedge RIn \wedge AOp \end{aligned}$$

Then rearranging the schema predicates from the predicate part to the declaration part, and removing the redundant declarations, gives the final form we use:

$$BOp; R'; ROut \vdash \exists A; AIn \bullet R \wedge RIn \wedge AOp$$

 $\mathcal{A}$  to  $\mathcal{B}$  retrieve relation

The purpose of the retrieve relation is to capture the details of the various states the concrete world can be in, and which abstract state(s) these correspond to, and the relationships between the concrete and abstract inputs and outputs.

For the first refinement, we talk of  $Rab$ : the Retrieve from  $\mathcal{A}$  to  $\mathcal{B}$ . Later, for the second refinement, we talk of  $Rbc$ : the Retrieve from  $\mathcal{B}$  to  $\mathcal{C}$ .

## 10.1 Retrieve state

The domains of the  $\mathcal{B}$  and  $\mathcal{A}$  'world' functions define the authentic purses.

<i>AbstractBetween</i>	
<i>AbWorld</i>	
<i>BetweenWorld</i>	
$\text{dom } abAuthPurse = \text{dom } conAuthPurse$	

$\mathcal{A}$  *balance* and *lost* are related to  $\mathcal{B}$  *balance* and *exLogs*. The relationship is relational, not functional, and highly non-deterministic part-way through a transaction.

10.1.1 Exposing *chosenLost*

*chosenLost* is a non-deterministic choice of a subset of all the *maybeLost* values that we 'choose' to say will be lost.

$ \begin{array}{l} \text{RabCl} \\ \text{AbstractBetween} \\ \text{chosenLost} : \mathbb{P} \text{ PayDetails} \\ \text{chosenLost} \subseteq \text{maybeLost} \\ \forall \text{name} : \text{dom conAuthPurse} \bullet \\ \quad (\text{abAuthPurse name}).\text{lost} = \\ \quad \quad \text{sumValue}((\text{definitelyLost} \cup \text{chosenLost}) \\ \quad \quad \cap \{ \text{pd} : \text{PayDetails} \mid \text{pd.from} = \text{name} \}) \\ \wedge (\text{abAuthPurse name}).\text{balance} = \\ \quad (\text{conAuthPurse name}).\text{balance} \\ \quad + \text{sumValue}((\text{maybeLost} \setminus \text{chosenLost}) \\ \quad \cap \{ \text{pd} : \text{PayDetails} \mid \text{pd.to} = \text{name} \}) \end{array} $
--

The predicate links the  $\mathcal{B}$  and  $\mathcal{A}$  values<sup>1</sup>:

- For a purse  $\text{name}$ , its  $\text{lost}$  value is the sum of the values in all those transactions that are definitely lost or that we have chosen to assume lost with  $\text{name}$  as the  $\text{from}$  purse. (Note the deliberate similarity of this definition and that in  $\text{BetwFinState}$ .)
- The  $\mathcal{A}$   $\text{balance}$  of a purse is its  $\mathcal{B}$  balance plus the value of all those transactions we have chosen to assume will not be lost, with  $\text{name}$  as the  $\text{to}$  purse. (For a give  $\text{name}$ , there is at most one such transaction.)

A consequence of this relationship is that the abstract  $\text{lost}$  and  $\text{balance}$  values of a purse can depend on the corresponding values of *more than one* concrete purse.

### 10.1.2 Hiding $\text{chosenLost}$

The retrieve relation is then  $\text{RabCl}$  with the non-deterministic choice  $\text{chosenLost}$  hidden<sup>2</sup>:

$$\text{Rab} \hat{=} \exists \text{chosenLost} : \mathbb{P} \text{ PayDetails} \bullet \text{RabCl}$$

We define the retrieve in this way because in the proof we need to have direct access to  $\text{chosenLost}$ .

<sup>1</sup>It is valid to apply  $\text{sumValue}$  in this predicate, because both  $\text{definitelyLost}$  and  $\text{maybeLost}$  are finite.  $\text{definitelyLost}$  is finite because of  $\text{BetweenWorld}$  constraint B-13.  $\text{maybeLost}$  is finite because  $\text{tolnEpy}$  is finite: each  $\text{pd}$  in the set comprehension for  $\text{tolnEpy}$  comes from a distinct purse in  $\text{conAuthPurse}$ , which itself is a finite function.

<sup>2</sup>We use this form to simplify the general correctness proofs, section 14.4.3.

### 10.1.3 Exposing $\text{pdThis}$

In the proof, we find that we wish to focus on a single  $\text{pd}$  (any  $\text{pd}$ ). We define a new schema,  $\text{RabClPd}$ , identical to  $\text{RabCl}$  except for an extra declaration of a  $\text{pd}$ .

$ \begin{array}{l} \text{RabClPd} \\ \text{RabCl} \\ \text{pdThis} : \text{PayDetails} \end{array} $
--

We split the predicate part of  $\text{RabClPd}$  into two cases that partition the possibilities:

- $\forall \text{name} : \text{dom conAuthPurse} \mid \text{name} \notin \{ \text{pdThis.from}, \text{pdThis.to} \}$  purses not involved in the  $\text{pdThis}$  transaction.
- $\forall \text{name} : \text{dom conAuthPurse} \mid \text{name} \in \{ \text{pdThis.from}, \text{pdThis.to} \}$  purses involved in the  $\text{pdThis}$  transaction.

In all cases the purses other than the  $\text{from}$  and  $\text{to}$  purses retrieve their  $\text{balance}$  and  $\text{lost}$  values in the same way, so we factor this part of the predicate out into a separate schema,  $\text{OtherPursesRab}$ , which we include with the remaining part of the predicate.

$ \begin{array}{l} \text{OtherPursesRab} \\ \text{AbstractBetween} \\ \text{chosenLost} : \mathbb{P} \text{ PayDetails} \\ \text{pdThis} : \text{PayDetails} \\ \forall \text{name} : \text{dom conAuthPurse} \mid \text{name} \notin \{ \text{pdThis.from}, \text{pdThis.to} \} \bullet \\ \quad (\text{abAuthPurse name}).\text{lost} = \\ \quad \quad \text{sumValue}((\text{definitelyLost} \cup \text{chosenLost}) \\ \quad \quad \cap \{ \text{pd} : \text{PayDetails} \mid \text{pd.from} = \text{name} \}) \\ \wedge (\text{abAuthPurse name}).\text{balance} = \\ \quad (\text{conAuthPurse name}).\text{balance} \\ \quad + \text{sumValue}((\text{maybeLost} \setminus \text{chosenLost}) \\ \quad \cap \{ \text{pd} : \text{PayDetails} \mid \text{pd.to} = \text{name} \}) \end{array} $
---

We split  $\text{RabClPd}$  into four cases that partition the possibilities:

- $\text{RabOkayClPd} : \text{pdThis} \in \text{maybeLost} \setminus \text{chosenLost}$  half way through a transaction that will succeed. Since  $\text{maybeLost}$  refers only to authentic purses,

we know that  $\{pdThis.from, pdThis.to\} \subseteq \text{dom } conAuthPurse$ , and so the remaining quantifier is reduced to these two cases.

- *RabWillBeLostCIPd* :  $pdThis \in chosenLost$  half way through a transaction that will lose the value (the *to* purse has not yet aborted, but we choose that it will, rather than receive the *val*). Since  $chosenLost \subseteq maybeLost$  refers only to authentic purses, we know that  $\{pdThis.from, pdThis.to\} \subseteq \text{dom } conAuthPurse$ , and so the remaining quantifier is reduced to these two cases.
- *RabHasBeenLostCIPd* :  $pdThis \in definitelyLost$  half way through a transaction that has lost the value (the *to* purse has already moved on). Since  $definitelyLost$  refers only to authentic purses, we know that  $\{pdThis.from, pdThis.to\} \subseteq \text{dom } conAuthPurse$ , and so the remaining quantifier is reduced to these two cases.
- *RabEndCIPd* :  $pdThis \notin definitelyLost \cup maybeLost$  At the beginning or end of a transaction, so there is no non-determinism in the *lost* or *balance* components. A general  $pdThis$  may refer to non-authentic purses, so the quantifier is reduced no further.

In the later proofs of operations that change purse status (*Abort*, *Req*, *Val* and *Ack*), we argue how the relevant  $pd$  moves in and out of the sets  $maybeLost$  and  $definitelyLost$ , and thereby choose the appropriate one of the four cases of the retrieve to use before and after the operation.

We perform this split by systematically subtracting out the chosen  $pd$  from the *lost* and *balance* expressions. If the  $pd$  was in fact in the relevant set, we then have to add the subtracted value back in, otherwise we do nothing, since we have made no change to the expression.

---

*RabOkayCIPd*

---

*AbstractBetween*  
*chosenLost* :  $\mathbb{P} PayDetails$   
*pdThis* :  $PayDetails$

---

$chosenLost \subseteq maybeLost$   
 $pdThis \in maybeLost \setminus chosenLost$   
 $(abAuthPurse\ pdThis.from).balance =$   
 $(conAuthPurse\ pdThis.from).balance$   
 $+ sumValue((maybeLost \setminus chosenLost)$   
 $\cap \{pd : PayDetails \mid pd.to = pdThis.from\})$   
 $\setminus \{pdThis\})$   
 $(abAuthPurse\ pdThis.to).balance =$   
 $pdThis.value$   
 $+ (conAuthPurse\ pdThis.to).balance$   
 $+ sumValue((maybeLost \setminus chosenLost)$   
 $\cap \{pd : PayDetails \mid pd.to = pdThis.to\})$   
 $\setminus \{pdThis\})$   
 $\forall name : \{pdThis.from, pdThis.to\} \bullet$   
 $(abAuthPurse\ name).lost =$   
 $sumValue(((definitelyLost \cup chosenLost)$   
 $\cap \{pd : PayDetails \mid pd.from = name\})$   
 $\setminus \{pdThis\})$

---

*OtherPursesRab*

In the *Okay* case,  $pdThis$  is not lost, so its value has to be added back into the *to* purse's *balance* component.



```

RabWillBeLostCIPd


---


AbstractBetween
chosenLost :  $\mathbb{P}$  PayDetails
pdThis : PayDetails


---


chosenLost  $\subseteq$  maybeLost
pdThis  $\in$  chosenLost
(abAuthPurse pdThis.from).lost =
  pdThis.value
  + sumValue((definitelyLost  $\cup$  chosenLost)
     $\cap$  { pd : PayDetails | pd.from = pdThis.from })
    \{pdThis})
(abAuthPurse pdThis.to).lost =
  sumValue((definitelyLost  $\cup$  chosenLost)
     $\cap$  { pd : PayDetails | pd.from = pdThis.to })
    \{pdThis})
 $\forall$  name : {pdThis.from, pdThis.to} •
  (abAuthPurse name).balance =
    (conAuthPurse name).balance
    + sumValue((maybeLost \ chosenLost)
       $\cap$  { pd : PayDetails | pd.to = name })
      \{pdThis})


---


OtherPursesRab

```

In the *WillBeLost* case, *pdThis* is chosen lost, so its value has to be added back into the from purse's *lost* component.

```

RabHasBeenLostCIPd


---


AbstractBetween
chosenLost :  $\mathbb{P}$  PayDetails
pdThis : PayDetails


---


chosenLost  $\subseteq$  maybeLost
pdThis  $\in$  definitelyLost
(abAuthPurse pdThis.from).lost =
  pdThis.value
  + sumValue((definitelyLost  $\cup$  chosenLost)
     $\cap$  { pd : PayDetails | pd.from = pdThis.from })
    \{pdThis})
(abAuthPurse pdThis.to).lost =
  sumValue((definitelyLost  $\cup$  chosenLost)
     $\cap$  { pd : PayDetails | pd.from = pdThis.to })
    \{pdThis})
 $\forall$  name : {pdThis.from, pdThis.to} •
  (abAuthPurse name).balance =
    (conAuthPurse name).balance
    + sumValue((maybeLost \ chosenLost)
       $\cap$  { pd : PayDetails | pd.to = name })
      \{pdThis})


---


OtherPursesRab

```

In the *HasBeenLost* case, *pdThis* is definitely lost, so its value has to be added back into the from purse's *lost* component.

<p><i>RabEndClPd</i></p> <hr/> <p><i>AbstractBetween</i>  <i>chosenLost</i> : <math>\mathbb{P}</math> <i>PayDetails</i>  <i>pdThis</i> : <i>PayDetails</i></p> <hr/> <p><i>chosenLost</i> <math>\subseteq</math> <i>maybeLost</i>  <i>pdThis</i> <math>\notin</math> <i>definitelyLost</i> <math>\cup</math> <i>maybeLost</i>  <math>\forall</math> <i>name</i> : <math>\text{dom } \text{conAuthPurse} \cap \{pdThis.from, pdThis.to\} \bullet</math></p> <p style="padding-left: 20px;">(<i>abAuthPurse name</i>).<i>lost</i> =  <math>\text{sumValue}((\text{definitelyLost} \cup \text{chosenLost})</math>  <math>\cap \{pd : \text{PayDetails} \mid pd.from = name\})</math>  <math>\setminus \{pdThis\})</math></p> <p style="padding-left: 20px;"><math>\wedge</math> (<i>abAuthPurse name</i>).<i>balance</i> =  <math>(\text{conAuthPurse name}).balance</math>  <math>+ \text{sumValue}((\text{maybeLost} \setminus \text{chosenLost})</math>  <math>\cap \{pd : \text{PayDetails} \mid pd.to = name\})</math>  <math>\setminus \{pdThis\})</math></p> <hr/> <p><i>OtherPursesRab</i></p>
---

In the *End* case, *pdThis* is in neither component, so its value does not have to be added back in anywhere.

#### 10.1.4 Partition

We have the identity<sup>3</sup>:

$$\begin{aligned}
 & \text{RabClPd} \\
 & \vdash \\
 & \text{RabClPd} \Leftrightarrow \\
 & (\text{RabOkayClPd} \\
 & \quad \vee \text{RabWillBeLostClPd} \\
 & \quad \vee \text{RabHasBeenLostClPd} \\
 & \quad \vee \text{RabEndClPd})
 \end{aligned}$$

**Proof:**

The four cases differ in the predicate on *pdThis*, which together *partition* the possibilities. It is obvious that the four cases cover the possibilities. We use Lemma 'lost', which says that *definitelyLost* and *maybeLost* are disjoint, to show that the four cases are non-overlapping.

<sup>3</sup>Used in: *Req check-operation*, splitting into four cases, section 18.6.

■ 10.1.4

#### 10.1.5 Quantified forms

Because the introduction of the *pd* in *RabClPd* is arbitrary, we have the following identities:

$$\text{RabCl} \vdash \text{RabCl} \Leftrightarrow (\forall pdThis : \text{PayDetails} \bullet \text{RabClPd})$$

and

$$\text{RabCl} \vdash \text{RabCl} \Leftrightarrow (\exists pdThis : \text{PayDetails} \bullet \text{RabClPd})$$

**Proof:**

That both these identities hold may seem odd, but can be intuitively understood by looking at a similar, smaller example. Consider a non-empty subset of  $\mathbb{N}$  called *X*. Then it is certainly true that

$$\exists x : X \bullet X = X \setminus \{x\} \cup \{x\}$$

and also

$$\forall x : X \bullet X = X \setminus \{x\} \cup \{x\}$$

■ 10.1.5

We have just chosen to extract an arbitrary element from the set for special naming. We do the same with *RabCl*, selecting an arbitrary *pdThis* for special naming, but without changing the meaning of the schema. This means that we can split up *RabCl* into a collection of four disjunctions on a *pd* in different ways as the proof dictates<sup>4</sup>.

#### 10.1.6 The full Retrieve state relation

We also define versions of these schemas with the *pdThis* and *chosenLost* hidden (so they have the same signature as *Rab*):

$$\text{RabOkay} \hat{=} \text{RabOkayClPd} \setminus (pdThis, chosenLost)$$

$$\text{RabWillBeLost} \hat{=} \text{RabWillBeLostClPd} \setminus (pdThis, chosenLost)$$

$$\text{RabHasBeenLost} \hat{=} \text{RabHasBeenLostClPd} \setminus (pdThis, chosenLost)$$

$$\text{RabEnd} \hat{=} \text{RabEndClPd} \setminus (pdThis, chosenLost)$$

<sup>4</sup>Used in: lemma 'deterministic', exposing *pdThis* (twice), section 14.4.3.

## 10.2 Retrieve inputs

Each  $\mathcal{A}$  operation has the same type of input, an *AIN*. Each  $\mathcal{B}$  operation has the same type of input, a *NAME* and a *MESSAGE*. The input part of the retrieve captures the relationship between these  $\mathcal{A}$  and  $\mathcal{B}$  inputs.

$$RabIn \hat{=} BetwInitIn[a?/g?]$$

The  $\mathcal{B}$  inputs are related to  $\mathcal{A}$  inputs in the following manner:

RI-1 *Req*: the  $\mathcal{A}$  transfer details are in the *req*

RI-2 All other  $\mathcal{B}$  inputs: the  $\mathcal{A}$  input is *aNullIn*.

## 10.3 Retrieve outputs

The output retrieve is particularly simple: all  $\mathcal{B}$  outputs retrieve to the single  $\mathcal{A}$  output.

$$RabOut \hat{=} BetwFinOut[a!/g!]$$

# $\mathcal{A}$ to $\mathcal{B}$ initialisation proof

## 11.1 Proof obligations

The requirement is to prove that the between initial state correctly refines the abstract initial state, and the between inputs correctly refine the abstract inputs. That is,

$$\begin{aligned} & \textit{BetweenInitState}; Rab' \vdash AbInitState \\ & \textit{BetwInitIn}; RabIn \vdash AbInitIn \end{aligned}$$

## 11.2 Proof of initial state

We successively thin the hypothesis to expose the consequent.

$$\begin{aligned} & \textit{BetweenWorldInit} \wedge Rab' && \text{[hyp]} \\ & \Rightarrow Rab' && \text{[thin]} \\ & \Rightarrow AbWorld' && \text{[thin]} \\ & \Rightarrow AbInitState && \text{[defn AbInitState]} \end{aligned}$$

■ 11.2

## 11.3 Proof of initial inputs

Expand *RabIn* and *AbInitIn*.

$$\textit{BetwInitIn}; \textit{BetwInitIn}[a?/g?] \vdash a? = g?$$

$BetwInitIn$  defines  $g?$  as a total function of  $(m?, name?)$ ; call it  $f$ . Thin.

$$\begin{aligned} g?, a? : AIN \mid \exists f : MESSAGE \times NAME \rightarrow AIN \bullet \\ \forall m : MESSAGE; n : NAME \bullet \\ g? = f(m, n) \wedge a? = f(m, n) \\ \vdash a? = g? \end{aligned}$$

Simplify and thin.

$$g?, a? : AIN \mid g? = a? \vdash a? = g?$$

- 11.3
- 11

## $\mathcal{A}$ to $\mathcal{B}$ finalisation proof

### 12.1 Proof obligations

The requirement is to prove that the between final state correctly refines the abstract final state, and the between outputs correctly refine the abstract outputs. That is,

$$BetwFinOut \vdash \exists a! : AOUT \bullet RabOut \wedge AbFinOut$$

$$BetwFinState \vdash \exists AbWorld \bullet Rab \wedge AbFinState$$

This proof obligation is summarised in figure 12.1.

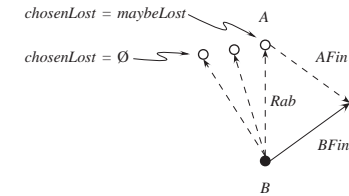


Figure 12.1: Backwards rules finalisation proof obligation

## 12.2 Output proof

Expand *RabOut* and *AbFinOut*.

$$BetwFinOut \vdash \exists a! : AOUT \bullet BetwFinOut[a!/g!] \wedge a! = g!$$

[*one point*] away the *a!* in the consequent

$$BetwFinOut \vdash BetwFinOut[g!/g!]$$

■ 12.2

## 12.3 State proof

We [*cut*] in an *AbWorld*, and put it equal to the *GlobalWorld*.

$$\begin{array}{l} BetwFinState; AbWorld \mid abAuthPurse = gAuthPurse \\ \vdash \\ \exists AbWorld \bullet Rab \wedge AbFinState \end{array}$$

Cutting in this new hypothesis requires us to discharge a side-lemma about the existence of such an *AbWorld*. This is trivial to do, by the [*one point*] rule.

We use [*consq exists*] to remove the existential quantifier in the consequent, by using the value just cut in:

$$\begin{array}{l} BetwFinState; AbWorld \mid abAuthPurse = gAuthPurse \\ \vdash \\ Rab \wedge AbFinState \end{array}$$

We prove each of the conjuncts in the consequent separately [*consq conj*], dropping unneeded hypotheses as appropriate [*thin*].

### 12.3.1 Case *AbFinState*

$$BetwFinState; AbWorld \mid abAuthPurse = gAuthPurse \vdash AbFinState$$

The predicates in *AbFinState* occur in the hypothesis, so are satisfied trivially.

■ 12.3.1

### 12.3.2 Case *Rab*

We expand out *Rab* into its conjuncts:

$$BetwFinState; AbWorld \mid abAuthPurse = gAuthPurse \vdash Rab$$

## Retrieve of equality

We have the equation

$$\text{dom } abAuthPurse = \text{dom } conAuthPurse$$

which can be shown from the equality of *gAuthPurse* and *conAuthPurse* in *BFinState*, and between *gAuthPurse* and *abAuthPurse* in the hypothesis.

Similarly, in each case the part of the retrieve to be proven has an equality between the abstract and concrete. We show this holds from an equality in that component between global and concrete in *BetwFinState*, and an equality between global and abstract in the hypothesis.

■ 12.3.2

### Case *Rab*

$$BetwFinState; AbWorld \mid abAuthPurse = gAuthPurse \vdash Rab$$

Expanding *BetwFinState*, thinning unwanted predicates, substituting for *global*, and expanding *Rab*, we get:

$$\begin{array}{l} AuxWorld; AbWorld \mid \\ \forall name : \text{dom } conAuthPurse \bullet \\ (abAuthPurse \text{ name}).lost = \\ \quad sumValue((definitelyLost \cup maybeLost) \\ \quad \cap \{ pd : PayDetails \mid pd.from = name \}) \\ \wedge (abAuthPurse \text{ name}).balance = (conAuthPurse \text{ name}).balance \\ \vdash \\ \exists chosenLost : \mathbb{P} \text{ maybeLost} \bullet \\ \forall name : \text{dom } conAuthPurse \bullet \\ (abAuthPurse \text{ name}).lost = \\ \quad sumValue((definitelyLost \cup chosenLost) \\ \quad \cap \{ pd : PayDetails \mid pd.from = name \}) \\ \wedge (abAuthPurse \text{ name}).balance = \\ \quad (conAuthPurse \text{ name}).balance \\ \quad + sumValue((maybeLost \setminus chosenLost) \\ \quad \cap \{ pd : PayDetails \mid pd.to = name \}) \end{array}$$

We [*one point*] away the *chosenLost* in the consequent by putting it equal to *maybeLost* (having [*cut*] in such a value and proved it exists). We also simplify

the equations, now that  $maybeLost \setminus chosenLost$  is empty:

$$\begin{aligned}
 & AuxWorld; AbWorld; chosenLost : \mathbb{P} PayDetails \mid \\
 & \quad chosenLost = maybeLost \\
 & \wedge (\forall name : \text{dom } conAuthPurse \bullet \\
 & \quad (abAuthPurse name).lost = \\
 & \quad \quad sumValue((definitelyLost \cup maybeLost) \\
 & \quad \quad \quad \cap \{pd : PayDetails \mid pd.from = name\}) \\
 & \quad \wedge (abAuthPurse name).balance \\
 & \quad \quad = (conAuthPurse name).balance) \\
 & \vdash \\
 & \forall name : \text{dom } conAuthPurse \bullet \\
 & \quad (abAuthPurse name).lost = \\
 & \quad \quad sumValue((definitelyLost \cup maybeLost) \\
 & \quad \quad \quad \cap \{pd : PayDetails \mid pd.from = name\}) \\
 & \quad \wedge (abAuthPurse name).balance = (conAuthPurse name).balance
 \end{aligned}$$

The consequent also appears as an hypothesis, so the proof is complete.

- 12.3.2
- 12.3.2
- 12.3
- 12

---

## $\mathcal{A}$ to $\mathcal{B}$ applicability proofs

### 13.1 Proof obligation

In section 9.2.3 we showed that it is sufficient to prove totality of the concrete operations.

### 13.2 Proof

Totality for each between operation was shown in the specification consistency proofs, section 8.3.2.

- 13

---

## Lemmas for the $\mathcal{A}$ to $\mathcal{B}$ correctness proofs

### 14.1 Introduction

The correctness proof obligation, to be discharged for each abstract operation  $AOp$ , where  $AOp \sqsubseteq BOpFull = BOp_1 \vee BOp_2 \vee \dots$  is the corresponding refinement, is:

$$BOpFull; Rab'; RabOut \vdash \exists AbWorld; a? : AIN \bullet Rab \wedge RabIn \wedge AOp$$

This proof obligation is summarised in figure 14.1. There are multiple lower paths both because the concrete operation is non-deterministic, and because the retrieve is non-deterministic. For each lower path triple of  $(B, B', A')$ , we have to find an  $A$  that ensures the existence of an upper path; it does not have to be the same  $A$  in each case.

There are various classes of  $\mathcal{B}$  operation depending on which  $\mathcal{A}$  operation is being refined. There are commonalities in the proof structures for these classes. This chapter develops general mechanisms and lemmas to facilitate proving most operations. This fits into the following main areas

- lemma 'multiple refinement': When the  $\mathcal{B}$  operation that refines an  $\mathcal{A}$  operation in a disjunction of several individual  $\mathcal{B}$  operations, the proof obligation can be split into one for each individual  $\mathcal{B}$  operation.
- lemma 'ignore': The ignore branch, and any 'abort' branch, of each  $\mathcal{B}$  operation need be proved once only.
- lemma 'deterministic': A simplification of all correctness proofs, by exposing the non-determinism in the retrieve, to the three cases **exists-pd**, **exists-chosenLost**, and **check-operation** (with the introduction of two ar-

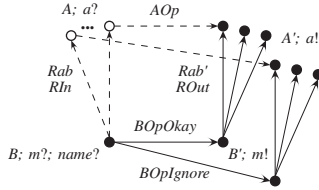


Figure 14.1: The correctness proof. The hypothesis is the existence all of the lower (solid) paths. The proof obligation is to demonstrate the existence of an upper (dashed) path in each case.

bitrary predicates  $\mathcal{P}$  and  $\mathcal{Q}$ , instantiated differently depending on the particular operation).

- lemma ‘lost unchanged’: Where *maybeLost* and *definitelyLost* are unchanged, the **exists-pd** and **exists-chosenLost** obligations can be automatically discharged.
- lemma ‘Abignore’: A further simplification of the **check-operation** proof obligation, for the operations that refine *AbIgnore*, to **check-operation-ignore**.
- proof that concrete *Ignore* refines *AbIgnore*
- proof that concrete *Abort* refines *AbIgnore*
- lemma ‘abort backward’: For an operation expressed as *Abort* composed with a simpler version of the operation, we need prove only that the simpler operation is a refinement

The lemmas developed in this chapter are collected together in Appendix C for ease of reference.

## 14.2 Lemma ‘multiple refinement’

In most cases of *AOp*, the corresponding *BOpFull* is a disjunction of many individual  $\mathcal{B}$  operations,  $BOp_1 \vee BOp_2 \vee \dots$  whose differences are invisible abstractly. For example, *AbIgnore* is refined by a disjunction of several separate operations.

We use the inference rule [*hyp disj*] to split these large disjunctions into separate proof obligations for each of the  $\mathcal{B}$  operations.

## 14.3 Lemma ‘ignore’: separating the branches

Each between operation *BOp* is promoted from *BOpPurseOkay*, disjoined with *Ignore*, and sometimes with *Abort*. Call the first disjunction *BOpOkay*:

$$BOpOkay \hat{=} \exists \Delta ConPurse \bullet \Phi BOp \wedge BOpPurseOkay$$

We use the inference rule [*hyp disj*], to split the correctness proof into two (or three) parts, one for each disjunct, each of which must be proved.

$$Abort; Rab'; RabOut \vdash \exists AbWorld; a? : AIN \bullet Rab \wedge RabIn \wedge AOp$$

$$Ignore; Rab'; RabOut \vdash \exists AbWorld; a? : AIN \bullet Rab \wedge RabIn \wedge AOp$$

$$BOpOkay; Rab'; RabOut \vdash \exists AbWorld; a? : AIN \bullet Rab \wedge RabIn \wedge AOp$$

All the abstract operations include an option of failing (equivalent to the concrete *Ignore*), which results in no change to the abstract state. We can therefore strengthen the conclusion of the *Ignore* and *Abort* theorems and prove

$$Ignore; Rab'; RabOut \vdash \exists AbWorld; a? : AIN \bullet Rab \wedge RabIn \wedge AbIgnore$$

$$Abort; Rab'; RabOut \vdash \exists AbWorld; a? : AIN \bullet Rab \wedge RabIn \wedge AbIgnore$$

These are independent of the particular operation *AOp*. Thus we need prove these theorems only once (which we do in sections 14.7 and 14.8). To prove the correctness of *BOp* we need additionally to prove the remaining *BOpOkay* theorem.

## 14.4 Lemma ‘deterministic’: simplifying the Okay branch

The *Okay* branch of the correctness proof is, in general,

$$BOpOkay; Rab'; RabOut \vdash \exists AbWorld; a? : AIN \bullet Rab \wedge RabIn \wedge AOp$$

In order to find an *AbWorld* that is appropriate, we expose the non-determinism in the retrieve. The non-determinism occurs in the *Rab* branch of the retrieve in terms of uncertainty about which transactions still in process will terminate successfully, and which will terminate with a lost value.

We also expose the transaction that is currently in progress, to make it available to the proof.



### 14.4.1 Choosing an input

We choose a value of  $a?$  that is consistent with  $RabIn$ . Since  $RabIn$  is functional from  $m?$  and  $name?$  to  $a?$ , we know this choice of  $a?$  is uniquely determined. We [cut] this value for  $a?$  into the hypothesis, and remove the quantifier on  $a?$  by the [consq exists] rule.

We note that  $RabIn$  in the consequent is independent of the choice of  $AbWorld$ , so can be pulled out of that quantifier.

$$\begin{array}{l} BOpOkay; RabOut; Rab'; a? : AIN \mid RabIn \\ \vdash \\ RabIn \wedge (\exists AbWorld \bullet Rab \wedge AOp) \end{array}$$

We split the proof into two on the conjunction in the consequent [consq conj], one for  $RabIn$ , one for  $\exists AbWorld \bullet Rab \wedge AOp$ .

$RabIn$  is trivially satisfied by this choice of  $a?$  in the hypothesis.

The declaration of  $a?$  in  $RabIn$  allows us to drop the explicit declaration in the hypothesis, giving

$$BOpOkay; RabOut; Rab'; RabIn \vdash \exists AbWorld \bullet Rab \wedge AOp$$

### 14.4.2 Cutting in $\Delta ConPurse$

It helps to work with the unpromoted form of the operation. We do this by expanding  $BOpOkay$ , according to its promoted definition, and [cut]ting  $\Delta ConPurse$  into the hypothesis such that  $BOpPurseOkay$  and  $\Phi BOp$  hold. (The side-lemma is satisfied from the expanded definition of  $BOpOkay$  in the hypothesis; which states that such a  $\Delta ConPurse$  exists.)

$$\begin{array}{l} (\exists \Delta ConPurse \bullet \Phi BOp \wedge BOpPurseOkay); \\ RabOut; Rab'; RabIn; \Delta ConPurse \mid \\ \Phi BOp \wedge BOpPurseOkay \\ \vdash \\ \exists AbWorld \bullet Rab \wedge AOp \end{array}$$

We rearrange the hypothesis, moving  $\Phi BOp$  and  $BOpPurseOkay$  from the predicate part to the declaration part. Since  $\Phi BOp$  declares  $\Delta ConPurse$ , we remove the latter. We [thin] the hypothesis of the expanded definition of  $BOpOkay$ .

$$\Phi BOp; BOpPurseOkay; RabOut; Rab'; RabIn \vdash \exists AbWorld \bullet Rab \wedge AOp$$

### 14.4.3 Exposing $chosenLost$ and $pdThis$

We need to make some of the internal components visible to the proof to enable us to break the proof into sections.

We replace  $Rab'$  with the quantified form of  $RabCl'$  (section 10.1.2), giving

$$\begin{array}{l} \Phi BOp; BOpPurseOkay; RabOut; \\ (\exists chosenLost' : \mathbb{P} PayDetails \bullet RabCl'); RabIn \\ \vdash \\ \exists AbWorld \bullet Rab \wedge AOp \end{array}$$

We now use [hyp exists] to remove the quantification, giving us

$$\begin{array}{l} \Phi BOp; BOpPurseOkay; RabOut; RabCl'; RabIn \\ \vdash \\ \exists AbWorld \bullet Rab \wedge AOp \end{array}$$

Next, we [cut] in a declaration of an arbitrary payment detail  $pdThis$ . In practice, this is the  $pd$  for the payment being processed by  $BOpOkay$ , but in this general manipulation we don't have enough information to specify this. We therefore constrain the  $pdThis$  with some arbitrary predicate  $\mathcal{P}$ .

This generates a non-trivial lemma, **exists-pd**, to be proved in each specific case, as

$$\begin{array}{l} \Phi BOp; BOpPurseOkay; RabOut; RabCl'; RabIn \\ \vdash \\ \exists pdThis : PayDetails \bullet \mathcal{P} \end{array}$$

and leaves our proof obligation as

$$\begin{array}{l} \Phi BOp; BOpPurseOkay; RabOut; RabCl'; RabIn; pdThis : PayDetails \mid \\ \mathcal{P} \\ \vdash \\ \exists AbWorld \bullet Rab \wedge AOp \end{array}$$

In the hypothesis we rewrite  $RabCl'$  as the universally quantified form of  $RabClPd'$  (section 10.1.5).

$$\begin{array}{l} \Phi BOp; BOpPurseOkay; RabOut; \\ (\forall pdThis' : PayDetails \bullet RabClPd'); \\ RabIn; pdThis : PayDetails \mid \\ \mathcal{P} \\ \vdash \\ \exists AbWorld \bullet Rab \wedge AOp \end{array}$$

Rather than hypothesising this is true for all  $pdThis$ 's, we choose a particular value in the quantification. (This is valid, [hyp uni], because assuming it true for only a particular value is weaker than assuming it is true for *all* values.) The value we choose for  $pdThis'$  is that of the value  $pdThis$ . This substitutes the value  $pdThis$  for  $pdThis'$  in the  $Rab'$  schema. This gives

$$\begin{array}{l} \Phi BOp; BOpPurseOkay; RabOut; RabCIPd'[pdThis/pdThis']; RabIn | \\ \quad pdThis : PayDetails | \\ \mathcal{P} \\ \vdash \\ \exists AbWorld \bullet Rab \wedge AOp \end{array}$$

The declaration in  $RabCIPd'$  allows us to drop the explicit declaration of  $pdThis$ . So we rewrite this more simply as

$$\begin{array}{l} \Phi BOp; BOpPurseOkay; RabOut; RabCIPd'[pdThis/pdThis']; RabIn | \\ \quad \mathcal{P} \\ \vdash \\ \exists AbWorld \bullet Rab \wedge AOp \end{array}$$

In the consequent we do a similar thing: expose  $chosenLost$ , and rewrite  $Rab$  as the existentially quantified form of  $RabCIPd$  (section 10.1.5)

$$\begin{array}{l} \Phi BOp; BOpPurseOkay; RabOut; RabCIPd'[pdThis/pdThis']; RabIn | \\ \quad \mathcal{P} \\ \vdash \\ \exists AbWorld \bullet \\ \quad (\exists chosenLost : \mathbb{P} PayDetails; pd : PayDetails \\ \quad \bullet RabCIPd[pd/pdThis]) \\ \wedge AOp \end{array}$$

We strengthen the consequent by adding the requirement that the value of  $pd$  claimed to exist on the right hand side is actually equal to the value  $pdThis$  declared on the left hand side. Similarly, we constrain  $chosenLost$  sufficiently. This we do by adding one requirement we always need (namely, that  $chosenLost \subseteq maybeLost$ ), and one arbitrary predicate  $Q$ , as we did with  $pdThis$ . This predicate is instantiated to some specific predicate each time this general manipu-

lation is invoked.

$$\begin{array}{l} \Phi BOp; BOpPurseOkay; RabOut; RabCIPd'[pdThis/pdThis']; RabIn | \\ \quad \mathcal{P} \\ \vdash \\ \exists AbWorld \bullet \\ \quad (\exists chosenLost : \mathbb{P} PayDetails; pd : PayDetails \bullet \\ \quad \quad pd = pdThis \wedge Q \\ \quad \quad \wedge chosenLost \subseteq maybeLost \\ \quad \quad \wedge RabCIPd[pd/pdThis]) \\ \wedge AOp \end{array}$$

We can remove the  $pd$  in the consequent with the [one point] rule, because we have an explicit value for it (namely,  $pdThis$ ).

$$\begin{array}{l} \Phi BOp; BOpPurseOkay; RabOut; RabCIPd'[pdThis/pdThis']; RabIn | \\ \quad \mathcal{P} \\ \vdash \\ \exists AbWorld \bullet \\ \quad (\exists chosenLost : \mathbb{P} PayDetails \bullet \\ \quad \quad Q \wedge chosenLost \subseteq maybeLost \\ \quad \quad \wedge RabCIPd) \\ \wedge AOp \end{array}$$

We [cut] into the hypothesis a  $chosenLost$  with the same properties as it has in the consequent (that is, the predicate  $Q \wedge chosenLost \subseteq maybeLost$ ). This generates a side lemma that such a value exists, **exists-chosenLost**, which must be discharged in each specific case, as

$$\begin{array}{l} \Phi BOp; BOpPurseOkay; RabOut; RabCIPd'[pdThis/pdThis']; RabIn | \\ \quad \mathcal{P} \\ \vdash \\ \exists chosenLost : \mathbb{P} PayDetails \bullet Q \wedge chosenLost \subseteq maybeLost \end{array}$$

This leaves:

$$\begin{array}{l}
\Phi BOp; BOpPurseOkay; RabOut; RabCIPd'[pdThis/pdThis']; RabIn; \\
\quad chosenLost : \mathbb{P} PayDetails \mid \\
\quad \mathcal{P} \wedge \mathcal{Q} \wedge chosenLost \subseteq maybeLost \\
\vdash \\
\exists AbWorld \bullet \\
\quad (\exists chosenLost : \mathbb{P} PayDetails \bullet \\
\quad \quad \mathcal{Q} \wedge chosenLost \subseteq maybeLost \\
\quad \quad \wedge RabCIPd) \\
\wedge AOp
\end{array}$$

We remove the existential quantification using the  $[consq\ exists]$  for  $chosenLost$ :

$$\begin{array}{l}
\Phi BOp; BOpPurseOkay; RabOut; RabCIPd'[pdThis/pdThis']; RabIn; \\
\quad chosenLost : \mathbb{P} PayDetails \mid \\
\quad \mathcal{P} \wedge \mathcal{Q} \wedge chosenLost \subseteq maybeLost \\
\vdash \\
\exists AbWorld \bullet RabCIPd \wedge AOp
\end{array}$$

We break this into two parts, separating the two retrieves in the consequent from  $AOp$ . We then prove each part.

Cut in  $AbWorld$  such that  $RabCIPd$  holds. This creates a side lemma to prove that such an  $AbWorld$  exists, consisting of just the retrieve. (This is discharged in section 14.4.4.)

We are left with

$$\begin{array}{l}
\Phi BOp; BOpPurseOkay; RabOut; RabCIPd'[pdThis/pdThis']; \\
\quad AbWorld; RabCIPd; RabIn; chosenLost : \mathbb{P} PayDetails \mid \\
\quad \mathcal{P} \wedge \mathcal{Q} \wedge chosenLost \subseteq maybeLost \\
\vdash \\
RabCIPd \wedge AOp
\end{array}$$

We discharge the retrieves in the consequent directly from the hypothesis, and remove  $chosenLost$  and  $chosenLost \subseteq maybeLost$  as these already occur in  $RabCIPd$ , leaving

$$\begin{array}{l}
\Phi BOp; BOpPurseOkay; RabOut; RabCIPd'[pdThis/pdThis']; \\
\quad AbWorld; RabCIPd; RabIn \mid \\
\quad \mathcal{P} \wedge \mathcal{Q} \\
\vdash \\
AOp
\end{array}$$

■ 14.4.3

#### 14.4.4 The existence of $AbWorld$

We have to prove the side condition generated when we cut in an  $AbWorld$  (above).

$$\begin{array}{l}
\Phi BOp; BOpPurseOkay; RabOut; RabCIPd'[pdThis/pdThis']; RabIn; \\
\quad chosenLost : \mathbb{P} PayDetails \mid \\
\quad \mathcal{P} \wedge \mathcal{Q} \wedge chosenLost \subseteq maybeLost \\
\vdash \\
\exists AbWorld \bullet RabCIPd
\end{array}$$

We can prove this by invoking lemma 'AbWorldUnique' (section C.15), provided we can show that the constraints of the hypothesis of that lemma hold.

Certainly we have  $BetweenWorld$  (from  $\Phi BOp$ ), a  $pdThis$  and a  $chosenLost$  such that the constraint  $chosenLost \subseteq maybeLost$  holds. This is sufficient to invoke the lemma.

■ 14.4.4

#### 14.4.5 Statement of lemma 'deterministic'

We summarise the results that section 14.4 has developed as a lemma.

**Lemma 14.1** (deterministic) The correctness proof for a general  $Okay$  branch consists of the following three proof obligations:

**exists-pd:**

$$\begin{array}{l}
\Phi BOp; BOpPurseOkay; RabOut; RabCl'; RabIn \\
\vdash \\
\exists pdThis : PayDetails \bullet \mathcal{P}
\end{array}$$

**exists-chosenLost:**

$$\begin{array}{l}
\Phi BOp; BOpPurseOkay; RabOut; RabCIPd'[pdThis/pdThis']; RabIn \mid \\
\quad \mathcal{P} \\
\vdash \\
\exists chosenLost : \mathbb{P} PayDetails \bullet \mathcal{Q} \wedge chosenLost \subseteq maybeLost
\end{array}$$

**check-operation:**

$$\begin{array}{l}
\Phi BOp; BOpPurseOkay; RabOut; RabCIPd'[pdThis/pdThis']; \\
\quad AbWorld; RabCIPd; RabIn \mid \\
\quad \mathcal{P} \wedge \mathcal{Q} \\
\vdash \\
AOp
\end{array}$$

■

## ■ 14.4

**14.5 Lemma ‘lost unchanged’**

Many operations do not change *maybeLost* or *definitelyLost*. We call a general such operation *BOp*∃*Lost*.

**Lemma 14.2** (lost unchanged) For *BOp*∃*Lost* operations, where *maybeLost* = *maybeLost'* and *definitelyLost'* = *definitelyLost*, the proof obligations **exists-pd** and **exists-chosenLost** are satisfied automatically by the instantiation of the predicates *P* and *Q* as:

$$P \Leftrightarrow \text{true}$$

$$Q \Leftrightarrow \text{chosenLost} = \text{chosenLost}'$$

leaving the remaining **check-operation** proof obligation as

$$\begin{array}{l} \Phi BOp; BOp\exists\text{LostPurseOkay}; RabOut; RabCIPd'[pdThis/pdThis']; \\ \quad AbWorld; RabCIPd; RabIn \mid \\ \quad \text{chosenLost} = \text{chosenLost}' \\ \quad \wedge \text{maybeLost} = \text{maybeLost}' \\ \quad \wedge \text{definitelyLost}' = \text{definitelyLost} \\ \vdash \\ AOp \end{array}$$

■

**14.5.1 Proof**

We add the hypotheses *maybeLost* = *maybeLost'* and *definitelyLost'* = *definitelyLost* to the proof obligations for these *BOp*∃*Lost* operations.

**exists-pd**

$$\begin{array}{l} \Phi BOp; BOp\exists\text{LostPurseOkay}; RabOut; RabCIPd'; RabIn \mid \\ \quad \text{maybeLost}' = \text{maybeLost} \\ \quad \wedge \text{definitelyLost}' = \text{definitelyLost} \\ \vdash \\ \exists pdThis : \text{PayDetails} \bullet \text{true} \end{array}$$

This is trivially true.

## ■ 14.5.1

**exists-chosenLost**

$$\begin{array}{l} \Phi BOp; BOp\exists\text{LostPurseOkay}; RabOut; RabCIPd'[pdThis/pdThis']; \\ \quad RabIn \mid \\ \quad \text{maybeLost}' = \text{maybeLost} \\ \quad \wedge \text{definitelyLost}' = \text{definitelyLost} \\ \vdash \\ \exists \text{chosenLost} : \mathbb{P} \text{PayDetails} \bullet \\ \quad \text{chosenLost} = \text{chosenLost}' \wedge \text{chosenLost} \subseteq \text{maybeLost} \end{array}$$

We apply the [one point] rule to remove the existential quantifier in the consequent, substitute for *maybeLost*, and [thin].

$$RabCIPd'[pdThis/pdThis'] \vdash \text{chosenLost}' \subseteq \text{maybeLost}'$$

The hypothesis *RabCIPd'*[*pdThis/pdThis'*] has *chosenLost'* ⊆ *maybeLost'*.

## ■ 14.5.1

## ■ 14.5

**14.5.2 Sufficient conditions for invoking lemma ‘lost unchanged’**

Since  $\Phi BOp$  gives us that *archive* is unchanged, sufficient conditions for invoking lemma ‘lost unchanged’ are that the operation in question changes neither the purse’s status (hence no movement into or out of *epv* or *epa*) nor its exception log (hence no change to *from* logs or *to* logs).

**14.6 Lemma ‘AbIgnore’: Operations that refine AbIgnore**

As shown in section 14.2, to prove the refinement of the abstract identity operation *AbIgnore*, we can separately prove correctness for each of the between operations *StartFrom*, *StartTo*, *Val*, *Ack*, *ReadExceptionLog*, *ClearExceptionLog*, *AuthoriseExLogClear*, *Archive*, *Ignore*, *Increase*, and *Abort*.

For those which are structured as promoted operations (that is, all except *Archive* and *Ignore*), consider a general such operation, call it *BOpIg*. We note that all *BOpIg* operations have the properties:

- *BOpIg* is a promoted operation, and thus alters only one concrete purse. It has the form

$$\exists \Delta \text{ConPurse} \bullet \Phi BOp \wedge BOpIgPurse$$

- for any purse, the *name* is unchanged (by definition of the single purse operations)
- the domain of *conAuthPurse* is unchanged (by construction of the promotion)
- for any purse, either *nextSeqNo* is unchanged, or increased.

$$\forall BOPigPurse \bullet nextSeqNo \leq nextSeqNo'$$

We use these properties to simplify the proof obligation for the *BOPig* operations.

We invoke lemma 'deterministic' (section 14.4) to reduce the *BOPig* proof obligation to **exists-pd**, **exists-chosenLost** and **check-operation**:

$$\begin{array}{l} \Phi BOP; BOPigPurse; RabOut; RabCIPd'[pdThis/pdThis']; \\ \quad AbWorld; RabCIPd; RabIn \mid \\ \mathcal{P} \wedge \mathcal{Q} \\ \vdash \\ AbIgnore \end{array}$$

**Lemma 14.3** (*AbIgnore*) For a *BOPig* operation, the **check-operation** proof obligation reduces to **check-operation-ignore**<sup>1</sup>:

$$\begin{array}{l} \Phi BOP; BOPigPurse; RabCIPd'[pdThis/pdThis']; AbWorld; RabCIPd \mid \\ \mathcal{P} \wedge \mathcal{Q} \\ \vdash \\ \forall n : \text{dom } abAuthPurse \bullet \\ \quad (abAuthPurse' n).lost = (abAuthPurse n).lost \\ \quad \wedge (abAuthPurse' n).balance = (abAuthPurse n).balance \end{array}$$

■

**Proof:**

We take the **check-operation** proof obligation, and expand *AbIgnore*. The *BOPigPurse* operations have certain properties in common; we explicitly state

<sup>1</sup>Used in: *Ignore*, 14.7.2.

these in the hypothesis.

$$\begin{array}{l} \Phi BOP; BOPigPurse; RabOut; RabCIPd'[pdThis/pdThis']; \\ \quad AbWorld; RabCIPd; RabIn \mid \\ \mathcal{P} \wedge \mathcal{Q} \\ \wedge name' = name \\ \wedge nextSeqNo' \geq nextSeqNo \\ \vdash \\ AbOp \wedge abAuthPurse' = abAuthPurse \end{array}$$

We use [*consq conj*] to split this proof into two parts. The *AbOp* part is trivial: there are no constraints. This leaves the other conjunct to be proven, which is rewritten as follows:

$$\begin{array}{l} \Phi BOP; BOPigPurse; RabOut; RabCIPd'[pdThis/pdThis']; \\ \quad AbWorld; RabCIPd; RabIn \mid \\ \mathcal{P} \wedge \mathcal{Q} \\ \wedge name' = name \\ \wedge nextSeqNo' \geq nextSeqNo \\ \vdash \\ \forall n : \text{dom } abAuthPurse \bullet abAuthPurse' n = abAuthPurse n \end{array}$$

We prove this component by component. From  $\Phi BOP$  in the hypothesis, all concrete purses other than purse *name?* remain unchanged. For the purse *name?*, we also have the equality of the pre and post states of *name*. This leaves the components *balance* and *lost*. We use this with [*consq conj*] to reduce our proof requirement to the following:

$$\begin{array}{l} \Phi BOP; BOPigPurse; RabOut; RabCIPd'[pdThis/pdThis']; \\ \quad AbWorld; RabCIPd; RabIn \mid \\ \mathcal{P} \wedge \mathcal{Q} \\ \wedge name' = name \\ \wedge nextSeqNo' \geq nextSeqNo \\ \vdash \\ \forall n : \text{dom } abAuthPurse \bullet \\ \quad (abAuthPurse' n).balance = (abAuthPurse n).balance \\ \quad \wedge (abAuthPurse' n).lost = (abAuthPurse n).lost \end{array}$$

We then [*thin*] the hypothesis to get the following, which proves the *AbIgnore*

lemma.

$$\begin{array}{l} \Phi BOp; BOPlgPurse; RabClPd' [pdThis/pdThis']; AbWorld; RabClPd \mid \\ \mathcal{P} \wedge \mathcal{Q} \\ \vdash \\ \forall n : \text{dom } abAuthPurse \bullet \\ (abAuthPurse' n).balance = (abAuthPurse n).balance \\ \wedge (abAuthPurse' n).lost = (abAuthPurse n).lost \end{array}$$

■ 14.6

### 14.7 Ignore refines AbIgnore

As we saw at the end of section 14.3, by splitting up promoted operations, we have generated a requirement to prove the correctness of the *Ignore* branch once only. We do that here.

#### 14.7.1 Invoking lemma ‘deterministic’

Lemma ‘deterministic’ (section 14.4.5) cannot be applied as-is, because *Ignore* is not written as a promotion (in order to ensure it is total). However, the arguments to split the proof obligation into three parts follow in exactly the same manner even if the unpromoted purse is not exposed. The proof obligations simply have *BOpOkay* in the hypothesis, instead of  $\Phi BOp; BOpPurseOkay$ . We use that form to simplify the *Ignore* proof obligation to three parts, and then invoke lemma ‘lost unchanged’ to discharge the first two obligations. We similarly use lemma ‘AbIgnore’ to simplify the third proof obligation to **check-operation-ignore**.

#### 14.7.2 check-operation-ignore

$$\begin{array}{l} Ignore; RabClPd' [pdThis/pdThis']; AbWorld; RabClPd \mid \\ chosenLost = chosenLost' \\ \wedge maybeLost = maybeLost' \\ \wedge definitelyLost = definitelyLost' \\ \vdash \\ \forall n : \text{dom } abAuthPurse \bullet \\ (abAuthPurse' n).balance = (abAuthPurse n).balance \\ \wedge (abAuthPurse' n).lost = (abAuthPurse n).lost \end{array}$$

The proof of this is immediate: *Ignore* changes no values, *definitelyLost*, *maybeLost* and *chosenLost* do not change, from the hypothesis; so the abstract *balance* and *lost*, which depend only on these unchanging values, are unchanged.

■ 14.7.2

■ 14.7

### 14.8 Abort refines AbIgnore

As we saw at the end of section 14.3, by splitting up promoted operations, we have generated a requirement to prove the correctness of the *Abort* branch once only. We do that here. We cast it as a lemma, because we also use it to simplify the proofs of operations that first abort (lemma ‘abort backward’).

**Lemma 14.4** (*Abort refines AbIgnore*) Concrete *Abort* refines abstract *Ignore*.<sup>2</sup>

$$Abort; Rab'; RabOut \vdash \exists AbWorld; a? : AIN \bullet Rab \wedge RabIn \wedge AbIgnore$$

■

**Proof:**

*Abort* is written as a disjunction between *Ignore* and a promoted *Abort-PurseOkay*. We use lemma ‘ignore’ (section 14.3) to simplify the proof obligation to the correctness of *Ignore* (which we discharge in section 14.7), and the *Okay* branch, which we prove here.

#### 14.8.1 Invoking lemma ‘deterministic’

We use lemma ‘deterministic’ (section 14.4.5) to simplify the proof obligations and then lemma ‘AbIgnore’ (section 14.6) to simplify the **check-operation** step.

We have to instantiate the predicates  $\mathcal{P}$  and  $\mathcal{Q}$ .

$\mathcal{P}$  is a predicate identifying the *pdThis* involved in the transaction. This is the *pdAuth* stored in the aborting purse, unless the aborting purse is in *eaFrom*, in which case we don’t have a defined transaction. We cater for the case of no transaction in the  $\mathcal{Q}$  predicate, so  $\mathcal{P}$  can safely be defined as

$$\mathcal{P} \Leftrightarrow pdThis = pdAuth$$

$\mathcal{Q}$  is a predicate on *chosenLost*. The after set *chosenLost'* either has *pdThis* removed (if the transaction moves it from *chosenLost* to *definitelyLost*), or is

<sup>2</sup>Used in proof of lemma abort, 14.9

unchanged (because  $pdThis$  was not in  $chosenLost$  to start with) or is unchanged because there was no transaction to abort. Hence

$$\begin{aligned} \mathcal{Q} \Leftrightarrow & (pdThis \in maybeLost \wedge chosenLost = chosenLost' \cup \{pdThis\}) \\ & \vee (pdThis \notin maybeLost \wedge status \neq eaFrom \wedge \\ & \quad chosenLost = chosenLost') \\ & \vee (status = eaFrom \wedge chosenLost = chosenLost') \end{aligned}$$

### 14.8.2 exists-pd

The unpromoted operation *AbortPurseOkay* is incomplete. The output,  $m! = \perp$ , is not provided until promotion.

$$\begin{aligned} & \Phi BOp; AbortPurseOkay; RabOut; RabCl; RabIn \mid m! = \perp \\ & \vdash \\ & \exists pdThis : PayDetails \bullet pdThis = pdAuth \end{aligned}$$

This is immediate by the one point rule.

#### ■ 14.8.2

### 14.8.3 Three cases

We split the remaining two proofs, of **exists-chosenLost** and **check-operation**, into three cases each, for each of the three disjuncts of  $\mathcal{Q}$ . We start by arguing the behaviour of *maybeLost* and *definitelyLost* in the three cases.

- **Case 1: aborted transaction in 'limbo'**: The aborting purse is the *to* purse in *epv*; the corresponding *from* purse is in *epa* or has logged. Hence aborting the transaction will definitely lose the value.

$$pdThis \in maybeLost$$

- **Case 2: aborted transaction not in 'limbo'**: The aborting purse is not the *to* purse in *epv*, or the corresponding *from* purse is not in *epa* and has not logged. The transaction has either not got far enough to lose anything, or has progressed sufficiently far that the value was already either successfully transferred or definitely lost.

$$pdThis \notin maybeLost \wedge status \neq eaFrom$$

- **Case 3: no transaction to abort**: The aborting purse is in *eaFrom*, so has no defined transaction. Nothing is aborted, so no value is lost.

$$status = eaFrom$$

### Case 1: old transaction in limbo

$$pdThis \in (fromInEpa \cup fromLogged) \cap toInEpv$$

We argue about the behaviour of *maybeLost* and *definitelyLost* using the fact that the purse is the *to* purse initially in *epv* in the aborting transaction, and it logs the old transaction and moves to *eaFrom*. We argue that the transaction  $pdThis$ , initially in *maybeLost* by construction, is moved into *definitelyLost'* by this case of the *Abort* operation. The transaction was far enough progressed that value may be lost, and it is lost in this case.

**Behaviour of *fromInEpa* and *fromLogged***  $pdThis$  is in *toInEpv* (by our case assumption), so the only purse undergoing any change (*name?*) is the *to* purse; hence there can be no change to the status or logs of any *from* purse. Hence

$$\begin{aligned} fromInEpa &= fromInEpa' \\ fromLogged &= fromLogged' \end{aligned}$$

**Behaviour of *toInEpv***  $pdThis$  is in *toInEpv* (by our case assumption);  $pdThis$  is not in *toInEpv'* (*Abort* puts the purse into *eaFrom*); all other purses and transactions remain unchanged. So

$$toInEpv = toInEpv' \cup \{pdThis\}$$

**Behaviour of *toLogged***  $pdThis$  is not in *toLogged* (using lemma 'notLogged-AndIn' with  $pdThis \in toInEpv$ );  $pdThis$  is in *toLogged'* (the purse makes a *to* log when it aborts from *epv*); all other purses and transactions remain unchanged. So

$$toLogged = toLogged' \setminus \{pdThis\}$$

**Behaviour of *definitelyLost***

$$\begin{aligned}
& \text{definitelyLost} \\
&= \text{toLogged} \cap (\text{fromLogged} \cup \text{fromInEpa}) \quad [\text{defn definitelyLost}] \\
&= (\text{toLogged}' \setminus \{pdThis\}) \cap (\text{fromLogged}' \cup \text{fromInEpa}') \quad [\text{above}] \\
&= (\text{toLogged}' \cap (\text{fromLogged}' \cup \text{fromInEpa}')) \setminus \{pdThis\} \quad [\text{rearrange}] \\
&= \text{definitelyLost}' \setminus \{pdThis\} \quad [\text{defn definitelyLost}']
\end{aligned}$$

**Behaviour of *maybeLost***

$$\begin{aligned}
& \text{maybeLost} \\
&= (\text{fromInEpa} \cup \text{fromLogged}) \cap \text{toInEpv} \quad [\text{defn maybeLost}] \\
&= (\text{fromInEpa}' \cup \text{fromLogged}') \cap (\text{toInEpv}' \cup \{pdThis\}) \quad [\text{above}] \\
&= ((\text{fromInEpa}' \cup \text{fromLogged}') \cap \text{toInEpv}') \\
&\quad \cup ((\text{fromInEpa}' \cup \text{fromLogged}') \cap \{pdThis\}) \quad [\text{Spivey}] \\
&= ((\text{fromInEpa}' \cup \text{fromLogged}') \cap \text{toInEpv}') \\
&\quad \cup \{pdThis\} \quad [\text{case assumption}] \\
&= \text{maybeLost}' \cup \{pdThis\} \quad [\text{defn maybeLost}']
\end{aligned}$$

**Case 2: old transaction not in limbo**

$$pdThis \notin (\text{fromInEpa} \cup \text{fromLogged}) \cap \text{toInEpv} \wedge \text{status} \neq \text{eaFrom}$$

We argue that the transaction *pdThis* is not moved into or out of *maybeLost* or *definitelyLost* by this case of the *Abort* operation.

**Behaviour of *fromInEpa*  $\cup$  *fromLogged*** If *pdThis* is in *fromInEpa* it is also in *fromLogged'* (the purse is in *epa*, so it makes a *from* log when it aborts); if *pdThis* is in *fromLogged* it is also in *fromLogged'* (logs cannot be removed); if *pdThis* is not in *fromInEpa*  $\cup$  *fromLogged* it is not in *fromLogged'* (the purse is not in *epa*, so does not make a *from* log when it aborts), and not in *fromInEpa'* (because it ends in *eaFrom*); all other purses and transactions remain unchanged. So

$$\text{fromInEpa} \cup \text{fromLogged} = \text{fromInEpa}' \cup \text{fromLogged}'$$

**Behaviour of *definitelyLost*** The cases allowed by our case assumption are:

- *pdThis* refers to the *to* purse in *epv*, hence is not in

$$\text{fromInEpa} \cup \text{fromLogged}$$

and hence not in *definitelyLost*. Also it is not in *fromInEpa'*  $\cup$  *fromLogged'*, and hence not in *definitelyLost'*. So *definitelyLost* is unchanged.

- *pdThis* refers to the *to* purse, but not in *epv*, or *pdThis* refers to the *from* purse. Hence *toLogged* is unchanged, since no *to* log is written, and logs cannot be lost. Also *fromInEpa*  $\cup$  *fromLogged* is unchanged. So *definitelyLost* is unchanged.

So

$$\text{definitelyLost}' = \text{definitelyLost}$$

**Behaviour of *maybeLost*** The cases allowed by our case assumption are:

- *pdThis* refers to the *to* purse in *epv*, hence is not in

$$\text{fromInEpa} \cup \text{fromLogged}$$

and hence not in *maybeLost*. Also it is not in *fromInEpa'*  $\cup$  *fromLogged'*, and hence not in *maybeLost'*. So *maybeLost* is unchanged.

- *pdThis* refers to the *to* purse, but not in *epv*, or *pdThis* refers to the *from* purse. Hence *toInEpv* is unchanged, since no purse moves out of or in to *epv*. Also *fromInEpa*  $\cup$  *fromLogged* is unchanged. So *maybeLost* is unchanged.

So

$$\text{maybeLost}' = \text{maybeLost}$$

**Case 3: no transaction to abort**

$$\text{status} = \text{eaFrom}$$

From *AbortPurseOkay*, no purses change state and no logs are written. Therefore, *definitelyLost* and *maybeLost* don't change.

$$\text{definitelyLost}' = \text{definitelyLost}$$

$$\text{maybeLost}' = \text{maybeLost}$$



#### 14.8.4 exists-chosenLost

We now use the behaviour of *maybeLost* and *definitelyLost* in the three cases to prove **exists-chosenLost**.

$$\begin{array}{l}
\Phi BOp; AbortPurseOkay; RabOut; RabClPd'[pdThis/pdThis']; RabIn | \\
m! = \perp \\
\wedge pdThis = pdAuth \\
\vdash \\
\exists chosenLost : \mathbb{P} PayDetails \bullet \\
(pdThis \in maybeLost \wedge chosenLost = chosenLost' \cup \{pdThis\} \\
\vee pdThis \notin maybeLost \wedge status \neq eaFrom \\
\wedge chosenLost = chosenLost' \\
\vee status = eaFrom \wedge chosenLost = chosenLost') \\
\wedge chosenLost \subseteq maybeLost
\end{array}$$

We push the existential quantifier in the consequent into the predicates:

$$\begin{array}{l}
\Phi BOp; AbortPurseOkay; RabOut; RabClPd'[pdThis/pdThis']; RabIn | \\
m! = \perp \\
\wedge pdThis = pdAuth \\
\vdash \\
pdThis \in maybeLost \\
\wedge (\exists chosenLost : \mathbb{P} PayDetails \bullet \\
chosenLost = chosenLost' \cup \{pdThis\} \\
\wedge chosenLost \subseteq maybeLost) \\
\vee pdThis \notin maybeLost \wedge status \neq eaFrom \\
\wedge (\exists chosenLost : \mathbb{P} PayDetails \bullet \\
chosenLost = chosenLost' \\
\wedge chosenLost \subseteq maybeLost) \\
\vee status = eaFrom \\
\wedge (\exists chosenLost : \mathbb{P} PayDetails \bullet \\
chosenLost = chosenLost' \\
\wedge chosenLost \subseteq maybeLost)
\end{array}$$

In each case, we [*one point*] away the *chosenLost* because the predicate includes an explicit definition for it.

$$\begin{array}{l}
\Phi BOp; AbortPurseOkay; RabOut; RabClPd'[pdThis/pdThis']; RabIn | \\
m! = \perp \\
\wedge pdThis = pdAuth \\
\vdash \\
pdThis \in maybeLost \\
\wedge chosenLost' \cup \{pdThis\} \subseteq maybeLost \\
\vee pdThis \notin maybeLost \wedge status \neq eaFrom \\
\wedge chosenLost' \subseteq maybeLost \\
\vee status = eaFrom \\
\wedge chosenLost' \subseteq maybeLost
\end{array}$$

In each case, the predicate is of the form  $(a \wedge b)$ , and we argue below that  $a \Rightarrow b$ . This allows us to replace  $(a \wedge b)$  with  $a$ . If we do this, we obtain

$$\begin{array}{l}
\Phi BOp; AbortPurseOkay; RabOut; RabClPd'[pdThis/pdThis']; RabIn | \\
m! = \perp \\
\wedge pdThis = pdAuth \\
\vdash \\
pdThis \in maybeLost \\
\vee pdThis \notin maybeLost \wedge status \neq eaFrom \\
\vee status = eaFrom
\end{array}$$

which is *true*. We now carry out the argument as described above for each of the three disjuncts.

#### Case 1: old transaction in limbo

We must show that under the assumptions of this lemma and in this case

$$pdThis \in maybeLost \Rightarrow chosenLost' \cup \{pdThis\} \subseteq maybeLost$$

This follows by:

$$\begin{array}{l}
chosenLost' \cup \{pdThis\} \\
\subseteq maybeLost' \cup \{pdThis\} \quad \text{[hypothesis]} \\
\subseteq maybeLost \quad \text{[previous argument for case 1]}
\end{array}$$

■ 14.8.4

**Case 2: old transaction not in limbo**

We must show that under the assumptions of this lemma and in this case

$$pdThis \notin maybeLost \wedge status \neq eaFrom \Rightarrow \\ chosenLost' \subseteq maybeLost$$

This follows by

$$chosenLost' \subseteq maybeLost' \quad \text{[hypothesis]} \\ \Rightarrow chosenLost' \subseteq maybeLost \quad \text{[previous argument for case 2]}$$

■ 14.8.4

**Case 3: no transaction to abort**

We must show that under the assumptions of this lemma and in this case

$$status = eaFrom \Rightarrow \\ chosenLost' \subseteq maybeLost$$

This follows by

$$chosenLost' \subseteq maybeLost' \quad \text{[hypothesis]} \\ \Rightarrow chosenLost' \subseteq maybeLost \quad \text{[previous argument for case 3]}$$

■ 14.8.4

■ 14.8.4

**14.8.5 check-operation-ignore**

We now use the behaviour of *maybeLost* and *definitelyLost* in the three cases to prove **check-operation-ignore**.

$$\Phi BOP; AbortPurseOkay; RabCIPd'[pdThis/pdThis']; \\ AbWorld; RabCIPd \mid \\ pdThis = pdAuth \\ \wedge (pdThis \in maybeLost \wedge chosenLost = chosenLost' \cup \{pdThis\} \\ \vee pdThis \notin maybeLost \wedge status \neq eaFrom \\ \wedge chosenLost = chosenLost' \\ \vee status = eaFrom \wedge chosenLost = chosenLost') \\ \vdash \\ \forall n : \text{dom } abAuthPurse \bullet \\ (abAuthPurse' n).balance = (abAuthPurse n).balance \\ \wedge (abAuthPurse' n).lost = (abAuthPurse n).lost$$

We can prove this for each of the three disjuncts in the hypothesis by [hyp disj].

**Case 1: old transaction in limbo**

*lost* is a function of *definitelyLost*  $\cup$  *chosenLost*. The *pdThis* moves from *chosenLost* to *definitelyLost'*, so the union is unchanged.

*balance* is a function of *maybeLost*  $\setminus$  *chosenLost*. The *pdThis* moves from *chosenLost*, and hence from *maybeLost*, so the difference is unchanged.

■ 14.8.5

**Case 2+3: old transaction not in limbo or no transaction**

From *chosenLost* = *chosenLost'* and the arguments above, all the relevant sets are unchanging, so *lost* and *balance* are unchanging.

■ 14.8.5

■ 14.8.5

■ 14.8

**14.9 Lemma 'abort backward': operations that first abort**

Some of the concrete operations are written as a composition of *AbortPurseOkay* with a simpler operation starting from *eaFrom* (*StartFrom*, *StartTo*, *ReadExceptionLog*, *ExceptionLogClear*).

**Lemma 14.5** (abort backward) Where a concrete operation is written as a composition of *AbortPurseOkay* and a simpler operation starting from *eaFrom*, it is sufficient to prove that the promotion of the simpler operation alone refines the relevant abstract operation.

$$\begin{array}{l} \exists \Delta \text{ConPurse} \bullet \Phi \text{BOP} \wedge (\text{AbortPurseOkay} \wp \text{BOPurseEafromOkay}); \\ \text{Rab}' ; \text{RabOut}; \\ (\forall \text{BOPeafromOkay}; \text{Rab}' ; \text{RabOut} \bullet \\ \exists \text{AbWorld}; a? : \text{AIN} \bullet \text{Rab} \wedge \text{RabIn} \wedge \text{AOp}) \\ \vdash \\ \exists \text{AbWorld}; a? : \text{AIN} \bullet \text{Rab} \wedge \text{RabIn} \wedge \text{AOp} \end{array}$$

■

**Proof**

- Use lemma ‘promoted composition’ (section C.11) to rewrite the promotion of the composition to a composition of promotions, yielding

$$\begin{array}{l} (\text{AbortOkay} \wp \text{BOPeafromOkay}); \\ \text{Rab}' ; \text{RabOut}; \\ (\forall \text{BOPeafromOkay}; \text{Rab}' ; \text{RabOut} \bullet \\ \exists \text{AbWorld}; a? : \text{AIN} \bullet \text{Rab} \wedge \text{RabIn} \wedge \text{AOp}) \\ \vdash \\ \exists \text{AbWorld}; a? : \text{AIN} \bullet \text{Rab} \wedge \text{RabIn} \wedge \text{AOp} \end{array}$$

- If *BOP1* refines *AOP1* and *BOP2* refines *AOP2*, then *BOP1*  $\wp$  *BOP2* refines *AOP1*  $\wp$  *AOP2* (invoke lemma ‘compose backward’, section C.9).
- Take *BOP1* = *AbortOkay*, *AOP1* = *AbIgnore*, and invoke lemma ‘Abort refines AbIgnore’ (section 14.8), to discharge this proof.
- Take *BOP2* = *BOPeafromOkay*, *AOP2* = *AOp*, and note that we have that *BOP* refines *AOp* in the hypothesis.
- Note that *AbIgnore*  $\wp$  *AOp* = *AOp*, to reduce this expression in the consequent.

■ 14.9

**14.10 Summary of lemmas**

In section 9.2.4 we reduced the refinement correctness proof for an operation to:

$$\text{BOP}; \text{Rab}' ; \text{RabOut} \vdash \exists \text{AbWorld}; a? : \text{AIN} \bullet \text{Rab} \wedge \text{RabIn} \wedge \text{AOp}$$

We then built up a set of lemmas which may be used to simplify this proof requirement.

*AOp* and *BOP* are often disjunctions of simpler operations, and lemmas ‘multiple refinement’ (section 14.2) and ‘ignore’ (section 14.3) are used to prove that any *Ignore* or *Abort* branches of *BOP* need be proved once only for all *BOPs*. These two branches are proved in lemmas later on, after further simplification for a general disjunct (*Ignore*, *Abort* or *Okay*) of *BOP*. This simplification starts with lemma ‘deterministic’ (section 14.4) which removes the  $\exists \text{AbWorld}$  in the consequent of the correctness obligation. In doing so, it requires us to prove three side-lemmas (**exists-pd**, **exists-chosenLost**, **check-operation**). Lemma ‘lost unchanged’ (section 14.5) allows the side-lemmas **exists-pd** and **exists-chosenLost** to be discharged immediately given certain conditions. Lemma ‘AbIgnore’ (section 14.6) then provides a simplification of the side-lemma **check-operation** when *AOp* is *AbIgnore*.

We can now prove that the *Ignore* and *Abort* branches of *BOP* are correct with respect to *AOp*. Section 14.7 proves that *Ignore* refines *AbIgnore*, and lemma ‘Abort refines AbIgnore’ (section 14.8) handles the *Abort* branch. With lemmas ‘multiple refinement’ and ‘ignore’, this has now proved the correctness of the *Ignore* and *Abort* branches of all *BOP*.

Where the *Okay* branch of an operation is composed of *Abort* followed by the ‘active’ operation, lemma ‘abort backward’ gives us that we only need to prove the ‘active’ part.

Returning to the proof obligation written above, any of the *Ignore* or *Abort* branches of a *BOP* operation are dealt with by the lemmas. This leaves the *Okay* branch (if this contains an initial *Abort*, this can be ignored — from lemma ‘abort backward’ we need only prove the non-aborting part). Usually, we then apply lemma ‘deterministic’ yielding a number of side-lemmas. These may sometimes be further simplified using lemmas ‘lost unchanged’ and ‘AbIgnore’. The remaining proof is then particular to the *BOP*.

## Correctness of *Increase*

### 15.1 Proof obligation

We have to prove the correct refinement of each abstract operation. In section 9.2.4 we give a general simplification of the correctness proof. We use lemma 'multiple refinement' (section 14.2) to split the proof obligation for each  $\mathcal{A}$  operation into one for each individual  $\mathcal{B}$  operation.

This chapter proves the  $\mathcal{B}$  operation.

- We use lemma 'ignore' (see section 14.3) to simplify the proof obligation by proving the correctness of *Ignore* (in section 14.7), leaving the *Okay* branch to be proven here.
- We use lemma 'deterministic' (section C.1) to reduce the proof obligation to the three cases **exists-pd**, **exists-chosenLost**, and **check-operation**.
- Since this operation leaves the sets *maybeLost* and *definitelyLost* unchanged, we use lemma 'lost unchanged' (section C.2) to discharge the **exists pd-and exists chosenLost-obligations** automatically.
- Since this operation refines *AbIgnore*, we use lemma '*AbIgnore*' (from section C.3) to simplify **check-operation** to **check-operation-ignore**.

### 15.2 Invoking lemma 'lost unchanged'

Section 14.5.2 gives sufficient conditions to be able to invoke lemma 'lost unchanged'. These are that the unpromoted operation changes neither the *status* nor the exception log of the purse. *Increase* includes  $\exists \text{ConPurseIncrease}$ , which says exactly that. We can therefore invoke lemma 'Lost unchanged'.

### 15.3 check-operation-ignore

$$\begin{aligned}
&\Phi BOp; IncreasePurseOkay; RabOut; RabClPd'[pdThis/pdThis']; \\
&\quad AbWorld; RabClPd; RabIn | \\
&\quad chosenLost' = chosenLost \\
&\quad \wedge maybeLost' = maybeLost \\
&\quad \wedge definitelyLost' = definitelyLost \\
&\vdash \\
&\forall n : \text{dom } abAuthPurse \bullet \\
&\quad (abAuthPurse' n).balance = (abAuthPurse n).balance \\
&\quad \wedge (abAuthPurse' n).lost = (abAuthPurse n).lost
\end{aligned}$$

**Proof:** We have that *maybeLost* and *definitelyLost* are unchanged from the hypothesis. This shows that the *balance* and *lost* components of all the abstract purses remain unchanged.

- 15.3
- 15

---

## Correctness of *StartFrom*

### 16.1 Proof obligation

We have to prove the correct refinement of each abstract operation. In section 9.2.4 we give a general simplification of the correctness proof. We use lemma ‘multiple refinement’ (section 14.2) to split the proof obligation for each  $\mathcal{A}$  operation into one for each individual  $\mathcal{B}$  operation.

This chapter proves the  $\mathcal{B}$  operation.

- We use lemma ‘ignore’ (see section 14.3) to simplify the proof obligation by proving the correctness of *Ignore* (in section 14.7), and *Abort* (in section 14.8), leaving the *Okay* branch to be proven here.
- Since the *Okay* branch of this operation is expressed as a promotion of *AbortPurseOkay* composed with a simpler *EafromPurseOkay* operation, we use lemma ‘abort backward’ (section C.5), and prove only that the promotion of the simpler operation is a refinement.
- We use lemma ‘deterministic’ (section C.1) to reduce the proof obligation to the three cases **exists-pd**, **exists-chosenLost**, and **check-operation**.
- Since this operation refines *AbIgnore*, we use lemma ‘*AbIgnore*’ (from section C.3) to simplify **check-operation** to **check-operation-ignore**.

## 16.2 Instantiating lemma ‘deterministic’

We take the  $pdThis$  to be the  $pdAuth$  created by the start operation, and  $chosenLost$  to be unchanging.

$$\begin{aligned} \mathcal{P} &\Leftrightarrow pdThis = (conAuthPurse' name?).pdAuth \\ \mathcal{Q} &\Leftrightarrow chosenLost = chosenLost' \end{aligned}$$

## 16.3 Behaviour of $maybeLost$ and $definitelyLost$

We argue that  $pdThis$  is not in  $fromInEpa$  or  $fromLogged$  before or after the operation, where  $pdThis = (conAuthPurse' pdThis.from).pdAuth$ .

First, before the operation the purse is in  $eaFrom$ , and after it is in  $epr$ , and hence  $pdThis$  can never be in  $fromInEpa$ .

From *BetweenWorld* constraint B-7 if  $pdThis$  were in  $fromLogged'$  then we would have

$$(conAuthPurse name?).pdAuth.fromSeqNo > pdThis.fromSeqNo$$

but we know these two  $pdAuths$  are equal, so  $pdThis$  cannot be in  $fromLogged'$ . If the log isn't there after the operation, it certainly isn't there before, so  $pdThis$  is not in  $toLogged$  either.

Only the *from* purse changes in this operation, so the sets  $toInEpv$  and  $toLogged$  can't change. Hence

$$\begin{aligned} toInEpv' &= toInEpv \\ toLogged' &= toLogged \\ fromInEpa' &= fromInEpa \\ fromLogged' &= fromLogged \end{aligned}$$

It follows that  $maybeLost$  is unchanged:

$$\begin{aligned} maybeLost' & \\ &= toInEpv' \cap (fromInEpa' \cup fromLogged') \\ &= toInEpv \cap (fromInEpa \cup fromLogged) \\ &= maybeLost \end{aligned}$$

Also,  $definitelyLost$  is unchanged:

$$\begin{aligned} definitelyLost' & \\ &= toLogged' \cap (fromInEpa' \cup fromLogged') \\ &= toLogged \cap (fromInEpa \cup fromLogged) \\ &= definitelyLost \end{aligned}$$

## 16.4 exists-pd

$$\begin{aligned} &\Phi BOp; StartFromPurseEafromOkay; RabOut; RabCl'; RabIn \\ &\vdash \\ &\exists pdThis : PayDetails \bullet pdThis = (conAuthPurse' name?).pdAuth \end{aligned}$$

**Proof**

Use the [one point] rule with the expression for  $pdThis$  in the quantifier.  
 ■ 16.4

## 16.5 exists-chosenLost

$$\begin{aligned} &\Phi BOp; StartFromPurseEafromOkay; RabOut; \\ &RabClPd' [pdThis/pdThis']; RabIn | \\ &pdThis = (conAuthPurse' name?).pdAuth \\ &\vdash \\ &\exists chosenLost : \mathbb{P} PayDetails \bullet \\ &chosenLost = chosenLost' \\ &\wedge chosenLost \subseteq maybeLost \end{aligned}$$

**Proof:**

We use the [one point] rule on  $chosenLost$  to give

$$\begin{aligned} &\Phi BOp; StartFromPurseEafromOkay; RabOut; \\ &RabClPd' [pdThis/pdThis']; RabIn | \\ &pdThis = (conAuthPurse' name?).pdAuth \\ &\vdash \\ &chosenLost' \subseteq maybeLost \end{aligned}$$

We then have

$$\begin{aligned} chosenLost' &\subseteq maybeLost' && [RabClPd'] \\ &\subseteq maybeLost && [\text{unchanging } maybeLost] \end{aligned}$$

■ 16.5

## 16.6 check-operation

$$\begin{aligned} & \Phi BOp; StartFromPurseEafromOkay; RabClPd'[pdThis/pdThis']; \\ & \quad AbWorld; RabClPd | \\ & \quad pdThis = (conAuthPurse' name?).pdAuth \\ & \quad \wedge chosenLost = chosenLost' \\ & \vdash \\ & \forall n : \text{dom } abAuthPurse \bullet \\ & \quad (abAuthPurse' n).balance = (abAuthPurse n).balance \\ & \quad \wedge (abAuthPurse' n).lost = (abAuthPurse n).lost \end{aligned}$$

### Proof:

From *Rab*, we have that *lost* is a function of  $definitelyLost \cup chosenLost$ , which is unchanging, and that *balance* is a function of  $maybeLost \setminus chosenLost$ , which is also unchanging.

■ 16.6  
■ 16

## Correctness of *StartTo*

### 17.1 Proof obligation

We have to prove the correct refinement of each abstract operation. In section 9.2.4 we give a general simplification of the correctness proof. We use lemma 'multiple refinement' (section 14.2) to split the proof obligation for each  $\mathcal{A}$  operation into one for each individual  $\mathcal{B}$  operation.

This chapter proves the  $\mathcal{B}$  operation.

- We use lemma 'ignore' (see section 14.3) to simplify the proof obligation by proving the correctness of *Ignore* (in section 14.7), and *Abort* (in section 14.8), leaving the *Okay* branch to be proven here.
- Since the *Okay* branch of this operation is expressed as a promotion of *AbortPurseOkay* composed with a simpler *EafromPurseOkay* operation, we use lemma 'abort backward' (section C.5), and prove only that the promotion of the simpler operation is a refinement.
- We use lemma 'deterministic' (section C.1) to reduce the proof obligation to the three cases **exists-pd**, **exists-chosenLost**, and **check-operation**.
- Since this operation refines *AbIgnore*, we use lemma '*AbIgnore*' (from section C.3) to simplify **check-operation** to **check-operation-ignore**.

### 17.2 Instantiating lemma ‘deterministic’

We take  $pdThis$  to be the  $pdAuth$  created by the start operation, and  $chosenLost$  to be unchanging.

$$\mathcal{P} \Leftrightarrow pdThis = (conAuthPurse' name?).pdAuth$$

$$\mathcal{Q} \Leftrightarrow chosenLost = chosenLost'$$

### 17.3 Behaviour of $maybeLost$ and $definitelyLost$

We argue that  $pdThis$  is not in any of the before sets  $fromInEpa$ ,  $fromLogged$ ,  $toInEpv$ , or  $toLogged$ , where we have

$$pdThis = (conAuthPurse' name?).pdAuth.$$

$$(conAuthPurse name?).nextSeqNo \quad [defn. StartTo]$$

$$= (conAuthPurse' name?).pdAuth.toSeqNo$$

$$\Rightarrow (conAuthPurse name?).nextSeqNo \quad [defn. pdThis]$$

$$= pdThis.toSeqNo$$

$$\Rightarrow req\ pdThis \notin ether \quad [BetweenWorld\ constraint\ B-2]$$

$$\Rightarrow pdThis \notin fromInEpa \cup fromLogged \quad [BetweenWorld\ constraint\ B-12]$$

$$\wedge pdThis \notin toInEpv \cup toLogged \quad [BetweenWorld\ constraint\ B-10]$$

The operation moves one purse from  $eaFrom$  into  $epv$ ; no logs are written. Hence  $pdThis$  is in  $toInEpv'$ , but not newly added to any of the other after sets. So

$$toInEpv' = toInEpv \cup \{pdThis\}$$

$$toLogged' = toLogged$$

$$fromInEpa' = fromInEpa$$

$$fromLogged' = fromLogged$$

It follows that  $maybeLost$  is unchanged:

$$maybeLost'$$

$$= toInEpv' \cap (fromInEpa' \cup fromLogged')$$

$$= (toInEpv \cup \{pdThis\}) \cap (fromInEpa \cup fromLogged)$$

$$= maybeLost \cup (\{pdThis\} \cap (fromInEpa \cup fromLogged))$$

$$= maybeLost$$

Also,  $definitelyLost$  is unchanged:

$$definitelyLost'$$

$$= toLogged' \cap (fromInEpa' \cup fromLogged')$$

$$= toLogged \cap (fromInEpa \cup fromLogged)$$

$$= definitelyLost$$

### 17.4 exists-pd

$$\Phi BOp; StartToPurseEafromOkay; RabOut; RabCl'; RabIn$$

$$\vdash$$

$$\exists pdThis : PayDetails \bullet pdThis = (conAuthPurse' name?).pdAuth$$

**Proof:**

Use the [one point] rule with the expression for  $pdThis$  in the quantifier.

■ 17.4

### 17.5 exists-chosenLost

$$\Phi BOp; StartToPurseEafromOkay; RabOut; RabClPd' [pdThis/pdThis'];$$

$$RabIn \mid$$

$$pdThis = (conAuthPurse' name?).pdAuth$$

$$\vdash$$

$$\exists chosenLost : \mathbb{P} PayDetails \bullet$$

$$chosenLost = chosenLost'$$

$$\wedge chosenLost \subseteq maybeLost$$

**Proof:**

We apply the [one point] rule for  $chosenLost$  in the consequent to give

$$\Phi BOp; StartToPurseEafromOkay; RabOut; RabClPd' [pdThis/pdThis'];$$

$$RabIn \mid$$

$$pdThis = (conAuthPurse' name?).pdAuth$$

$$\vdash$$

$$chosenLost' \subseteq maybeLost$$

$$chosenLost' \subseteq maybeLost' \quad [RabClPd']$$

$$\subseteq maybeLost \quad [\text{unchanging } maybeLost]$$

■ 17.5



### 17.6 check-operation

$$\begin{array}{l}
\Phi BOp; StartToPurseEafromOkay; RabClPd' [pdThis/pdThis']; \\
\quad AbWorld; RabClPd | \\
\quad pdThis = (conAuthPurse' name?).pdAuth \\
\quad \wedge chosenLost = chosenLost' \\
\vdash \\
\forall n : \text{dom } abAuthPurse \bullet \\
\quad (abAuthPurse' n).balance = (abAuthPurse n).balance \\
\quad \wedge (abAuthPurse' n).lost = (abAuthPurse n).lost
\end{array}$$

**Proof:**

From *Rab*, we have that *lost* is a function of *definitelyLost*  $\cup$  *chosenLost*, which is unchanging, and that *balance* is a function of *maybeLost*  $\setminus$  *chosenLost*, which is also unchanging.

- 17.6
- 17

## Correctness of *Req*

### 18.1 Proof obligation

We have to prove the correct refinement of each abstract operation. In section 9.2.4 we give a general simplification of the correctness proof. We use lemma ‘multiple refinement’ (section 14.2) to split the proof obligation for each  $\mathcal{A}$  operation into one for each individual  $\mathcal{B}$  operation.

This chapter proves the  $\mathcal{B}$  operation.

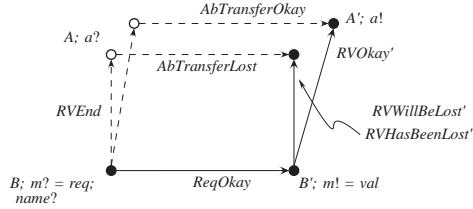
- We use lemma ‘ignore’ (see section 14.3) to simplify the proof obligation by proving the correctness of *Ignore* (in section 14.7), leaving the *Okay* branch to be proven here.
- We use lemma ‘deterministic’ (section C.1) to reduce the proof obligation to the three cases **exists-pd**, **exists-chosenLost**, and **check-operation**.

### 18.2 Instantiating lemma ‘deterministic’

We must instantiate two general predicates relating to *pdThis* and *chosenLost*. The choices for these predicates are based on the fact that the important transaction is the one referred to by the *req* message being consumed by the *ReqOkay* operation, and that before the operation, the set of transactions chosen to be lost should be all those chosen to be lost after the operation, but specifically excluding the transaction *pdThis*. Thus

$$P \Leftrightarrow req^- m? = pdThis$$

$$Q \Leftrightarrow chosenLost = chosenLost' \setminus \{pdThis\}$$

Figure 18.1: The correctness proof for *Req*.

### 18.3 Discussion

The correctness proof for *Req* is summarised in figure 18.1. There are three cases:

- The *to* purse for the transaction is in *epv*, and we choose that the transfer will succeed.  
Before the operation,  $pdThis \notin maybeLost \cup definitelyLost$ , and the appropriate retrieve is *RabEnd*.  
After the operation,  $pdThis \in maybeLost' \setminus chosenLost'$ , and the appropriate retrieve is *RabOkay'*; the abstract operation is *AbTransferOkay*.
- The *to* purse is in *epv*, and we choose the transfer will fail (the *to* purse will move out of *epv* before receiving the *val*).  
Before,  $pdThis \notin maybeLost \cup definitelyLost$ , and the appropriate retrieve is *RabEnd'*.  
After,  $pdThis \in chosenLost'$ , and the appropriate retrieve is *RabWillBeLost'*; the abstract operation is *AbTransferLost*.
- The *to* purse has already moved out of *epv*, so will not receive the *val*: the transfer has failed.  
Before,  $pdThis \notin maybeLost \cup definitelyLost$ , and the appropriate retrieve is *RabEnd*.  
After,  $pdThis \in definitelyLost'$ , and the appropriate retrieve is *RabHasBeenLost'*; the abstract operation is *AbTransferLost*.

The following proof establishes that these are indeed the only cases, and that *ReqOkay* correctly refines *AbTransfer* in each case.

### 18.4 exists-pd

$$\begin{aligned} & \Phi BOp; ReqPurseOkay; RabOut; RabCl'; RabIn \\ & \vdash \\ & \exists pdThis : PayDetails \bullet req \sim m? = pdThis \end{aligned}$$

**Proof:**

We discharge this by removing the existential for *pdThis* because we have an explicit equation for it, using the [one point] rule.

■ 18.4

### 18.5 exists-chosenlost

$$\begin{aligned} & \Phi BOp; ReqPurseOkay; RabOut; RabClPd'[pdThis/pdThis']; RabIn \mid \\ & req \sim m? = pdThis \\ & \vdash \\ & \exists chosenLost : \mathbb{P} PayDetails \bullet \\ & \quad chosenLost = chosenLost' \setminus \{pdThis\} \\ & \quad \wedge chosenLost \subseteq maybeLost \end{aligned}$$

**Proof:**

That we can construct a *chosenLost* as the set difference is true because set difference is always defined. That the subset constraint holds follows as below:

$$\begin{aligned} & chosenLost' \subseteq maybeLost' && [RabClPd'] \\ & chosenLost' \setminus \{pdThis\} \subseteq maybeLost' \setminus \{pdThis\} && [\text{property of set minus}] \\ & chosenLost \subseteq maybeLost' \setminus \{pdThis\} && [\text{eqn for } chosenLost] \\ & chosenLost \subseteq maybeLost && [\text{lemma 'not lost before', section C.14}] \end{aligned}$$

■ 18.5

### 18.6 check-operation

$$\begin{aligned} & \Phi BOp; ReqPurseOkay; RabOut; RabClPd'[pdThis/pdThis']; \\ & \quad AbWorld; RabClPd; RabIn \mid \\ & req \sim m? = pdThis \\ & \quad \wedge chosenLost = chosenLost' \setminus \{pdThis\} \\ & \vdash \\ & AbTransfer \end{aligned}$$

**Proof:**

We invoke lemma ‘not lost before’ to add constraints on *maybeLost* and *definitelyLost* to the hypothesis. This allows us to further alter the hypothesis by replacing *RabClPd* with *RabEndClPd*.

$$\begin{array}{l} \Phi BOp; ReqPurseOkay; RabOut; RabClPd'[pdThis/pdThis']; \\ \quad AbWorld; RabEndClPd; RabIn \mid \\ req^{\sim} m? = pdThis \\ \wedge chosenLost = chosenLost' \setminus \{pdThis\} \\ \wedge maybeLost = maybeLost' \setminus \{pdThis\} \\ \wedge definitelyLost = definitelyLost' \setminus \{pdThis\} \\ \vdash \\ AbTransfer \end{array}$$

We use [*hyp disj*] to split *RabClPd'*[...] into four separate cases (section 10.1.4) to prove (using identity in section 10.1.5). In each case, we strengthen the consequent by choosing an appropriate disjunct of *AbTransfer*.

- **case 1:** We choose that the value is not lost, so the corresponding abstract operation is *AbTransferOkay*

$$\begin{array}{l} \Phi BOp; ReqPurseOkay; RabOut; RabOkayClPd'[pdThis/pdThis']; \\ \quad AbWorld; RabEndClPd; RabIn \mid \\ req^{\sim} m? = pdThis \\ \wedge chosenLost = chosenLost' \setminus \{pdThis\} \\ \wedge maybeLost = maybeLost' \setminus \{pdThis\} \\ \wedge definitelyLost = definitelyLost' \setminus \{pdThis\} \\ \vdash \\ AbTransferOkay \end{array}$$

- **case 2:** We choose that the value will be lost, so the corresponding abstract operation is *AbTransferLost*

$$\begin{array}{l} \Phi BOp; ReqPurseOkay; RabOut; \\ \quad RabWillBeLostClPd'[pdThis/pdThis']; \\ \quad \quad AbWorld; RabEndClPd; RabIn \mid \\ req^{\sim} m? = pdThis \\ \wedge chosenLost = chosenLost' \setminus \{pdThis\} \\ \wedge maybeLost = maybeLost' \setminus \{pdThis\} \\ \wedge definitelyLost = definitelyLost' \setminus \{pdThis\} \\ \vdash \\ AbTransferLost \end{array}$$

- **case 3:** We say that the value has already been lost, so the corresponding abstract operation is *AbTransferLost*

$$\begin{array}{l} \Phi BOp; ReqPurseOkay; RabOut; \\ \quad RabHasBeenLostClPd'[pdThis/pdThis']; \\ \quad \quad AbWorld; RabEndClPd; RabIn \mid \\ req^{\sim} m? = pdThis \\ \wedge chosenLost = chosenLost' \setminus \{pdThis\} \\ \wedge maybeLost = maybeLost' \setminus \{pdThis\} \\ \wedge definitelyLost = definitelyLost' \setminus \{pdThis\} \\ \vdash \\ AbTransferLost \end{array}$$

- **case 4:** The fourth case is impossible. We choose *RabEndClPd'*, and prove that the hypothesis is contradictory, so the choice of corresponding abstract operation is unimportant.

$$\begin{array}{l} \Phi BOp; ReqPurseOkay; RabOut; RabEndClPd'[pdThis/pdThis']; \\ \quad AbWorld; RabEndClPd; RabIn \mid \\ req^{\sim} m? = pdThis \\ \wedge chosenLost = chosenLost' \setminus \{pdThis\} \\ \wedge maybeLost = maybeLost' \setminus \{pdThis\} \\ \wedge definitelyLost = definitelyLost' \setminus \{pdThis\} \\ \vdash \\ AbTransfer \end{array}$$

We now have four independent cases to prove. The next four sections each prove one case.

**18.7 case 1: ReqOkay and RabOkayClPd'**

$$\begin{array}{l} \Phi BOp; ReqPurseOkay; RabOut; RabOkayClPd'[pdThis/pdThis']; \\ \quad AbWorld; RabEndClPd; RabIn \mid \\ req^{\sim} m? = pdThis \\ \wedge chosenLost = chosenLost' \setminus \{pdThis\} \\ \wedge maybeLost = maybeLost' \setminus \{pdThis\} \\ \wedge definitelyLost = definitelyLost' \setminus \{pdThis\} \\ \vdash \\ AbTransferOkay \end{array}$$

### 18.7.1 The behaviour of *maybeLost* and *definitelyLost*

We argue that the transaction *pdThis* is initially not in *maybeLost* or *definitelyLost*, and is moved into *maybeLost'* \ *chosenLost'* by this case of the *ReqOkay* operation. The transaction initially was not far enough progressed to have the potential of being lost; afterwards it has progressed far enough that it may be lost, but we are actually on the branch that will succeed.

We have from *RabOkayCIPd'* that

$$pdThis \in maybeLost' \setminus chosenLost'$$

Therefore *pdThis*  $\notin$  *chosenLost'* (by the definition of set minus) and *pdThis*  $\notin$  *definitelyLost'* (by lemma 'lost'). So we have

$$\begin{aligned} definitelyLost &= definitelyLost' \\ maybeLost &= maybeLost' \setminus \{pdThis\} \\ chosenLost &= chosenLost' \end{aligned}$$

### 18.7.2 AbTransferOkay

In this section we prove that an *AbWorld* that has the correct retrieve properties also satisfies *AbTransferOkay*. Recall that our proof obligation is

$$\begin{aligned} &\Phi BOp; ReqPurseOkay; RabOut; RabOkayCIPd'[pdThis/pdThis']; \\ &AbWorld; RabEndCIPd; RabIn \mid \\ &req \sim m? = pdThis \\ &\wedge chosenLost = chosenLost' \setminus \{pdThis\} \\ &\wedge maybeLost = maybeLost' \setminus \{pdThis\} \\ &\wedge definitelyLost = definitelyLost' \setminus \{pdThis\} \\ &\vdash \\ &AbTransferOkay \end{aligned}$$

Each element of *AbWorld* is defined by an explicit equation in *RabEndCIPd*, and we show that this value satisfies *AbTransferOkay* by showing each predicate holds.

A-1 *AbOp*: This trivial: *AbOp* imposes no constraints.

A-2 *AbWorldSecureOp*

- *a?*  $\in$  *ran transfer*  
true by construction of *a?* from *m?* in *RabIn*.

- no purses other than *from?* and *to?* change  
For *balance* and *lost* we show that *RabEndCIPd* and

$$RabOkayCIPd'[pdThis/pdThis']$$

are essentially the same. This is immediate because in both cases the relevant predicates are captured in the same schema *OtherPursesRab*.

A-3 *Authentic[from?/name?], Authentic[to?/name?]*

We have *pdThis*  $\in$  *maybeLost'*, hence it is in both *authenticFrom'* and in *authenticTo'*. Hence, by  $\Phi BOp$  and *AbstractBetween*, it is also in both *authenticFrom* and in *authenticTo*.

A-4 *SufficientFundsProperty*

true from *ConPurse* constraint P-2b

A-5 *to?  $\neq$  from?*

true because *pdThis* is a *PayDetails*.

A-6 *abAuthPurse' from? = ... , abAuthPurse' to? = ...*

Each of the four elements (*from* and *to* purses, each with *balance* and *lost*) are handled below, followed by all the other elements in one section.

#### The *from* purse's *balance* component

$$\begin{aligned} &(abAuthPurse pdThis.from).balance \\ &= (conAuthPurse pdThis.from).balance \\ &\quad + sumValue(((maybeLost \setminus chosenLost) \\ &\quad \quad \cap \{pd : PayDetails \mid pd.to = pdThis.from\}) \\ &\quad \quad \setminus \{pdThis\}) \quad [RabEndCIPd] \\ &= (conAuthPurse pdThis.from).balance \\ &\quad + sumValue((((maybeLost' \setminus \{pdThis\}) \setminus chosenLost') \\ &\quad \quad \cap \{pd : PayDetails \mid pd.to = pdThis.from\}) \\ &\quad \quad \setminus \{pdThis\}) \quad [\text{section 18.7.1}] \\ &= (conAuthPurse pdThis.from).balance \\ &\quad + sumValue(((maybeLost' \setminus chosenLost') \\ &\quad \quad \cap \{pd : PayDetails \mid pd.to = pdThis.from\}) \\ &\quad \quad \setminus \{pdThis\}) \quad [\text{rearranging}] \end{aligned}$$

$$\begin{aligned}
&= pdThis.value + (conAuthPurse' pdThis.from).balance \\
&\quad + sumValue(((maybeLost' \ chosenLost') \\
&\quad \quad \cap \{pd : PayDetails \mid pd.to = pdThis.from\}) \\
&\quad \quad \setminus \{pdThis\}) \quad [ReqPurseOkay] \\
&= pdThis.value + (abAuthPurse' pdThis.from).balance \\
&\quad \quad \quad [RabOkayCIPd' \dots]
\end{aligned}$$

So

$$(abAuthPurse' from?).balance = (abAuthPurse from?).balance - value?$$

#### The from purse's lost component

$$\begin{aligned}
&(abAuthPurse pdThis.from).lost \\
&= sumValue(((definitelyLost \ chosenLost) \\
&\quad \cap \{pd : PayDetails \mid pd.from = pdThis.from\}) \\
&\quad \setminus \{pdThis\}) \quad [RabEndCIPd] \\
&= sumValue(((definitelyLost' \ chosenLost') \\
&\quad \cap \{pd : PayDetails \mid pd.from = pdThis.from\}) \\
&\quad \setminus \{pdThis\}) \quad [\text{section 18.7.1}] \\
&= (abAuthPurse' pdThis.from).lost \quad [RabOkayCIPd' \dots]
\end{aligned}$$

#### The to purse's balance component

$$\begin{aligned}
&(abAuthPurse pdThis.to).balance \\
&= (conAuthPurse pdThis.to).balance \\
&\quad + sumValue(((maybeLost \ chosenLost) \\
&\quad \quad \cap \{pd : PayDetails \mid pd.to = pdThis.to\}) \\
&\quad \quad \setminus \{pdThis\}) \quad [RabEndCIPd] \\
&= (conAuthPurse pdThis.to).balance \\
&\quad + sumValue(((maybeLost' \ \{pdThis\}) \ chosenLost') \\
&\quad \quad \cap \{pd : PayDetails \mid pd.to = pdThis.to\}) \\
&\quad \quad \setminus \{pdThis\}) \quad [\text{section 18.7.1}]
\end{aligned}$$

$$\begin{aligned}
&= (conAuthPurse pdThis.to).balance \\
&\quad + sumValue(((maybeLost' \ chosenLost') \\
&\quad \quad \cap \{pd : PayDetails \mid pd.to = pdThis.to\}) \\
&\quad \quad \setminus \{pdThis\}) \quad [\text{rearranging}] \\
&= (conAuthPurse' pdThis.to).balance \\
&\quad + sumValue(((maybeLost' \ chosenLost') \\
&\quad \quad \cap \{pd : PayDetails \mid pd.to = pdThis.to\}) \\
&\quad \quad \setminus \{pdThis\}) \quad [\Phi BOp] \\
&= (abAuthPurse' pdThis.to).balance + pdThis.value \\
&\quad \quad \quad [RabOkayCIPd' \dots]
\end{aligned}$$

From the form of  $(abAuthPurse' pdThis.to).balance = pdThis.value + n$  in *AbTransferOkay*, we see that this last subtraction gives a positive result. So

$$(abAuthPurse' to?).balance = (abAuthPurse to?).balance + value?$$

#### The to purse's lost component

$$\begin{aligned}
&(abAuthPurse pdThis.to).lost \\
&= sumValue(((definitelyLost \ chosenLost) \\
&\quad \cap \{pd : PayDetails \mid pd.from = pdThis.to\}) \\
&\quad \setminus \{pdThis\}) \quad [RabEndCIPd] \\
&= sumValue(((definitelyLost' \ chosenLost') \\
&\quad \cap \{pd : PayDetails \mid pd.from = pdThis.to\}) \\
&\quad \setminus \{pdThis\}) \quad [\text{section 18.7.1}] \\
&= (abAuthPurse' pdThis.to).lost \quad [RabOkayCIPd' \dots]
\end{aligned}$$

#### The remaining from and to purse components

These are unchanging, by  $\exists ConPurseReq$ , and that the retrieves each define a unique abstract world.

- 18.7.2
- 18.7

### 18.8 case 2: *ReqOkay* and *RabWillBeLostPd'*

$$\begin{array}{l} \Phi BOp; ReqPurseOkay; RabOut; RabWillBeLostCIPd'[pdThis/pdThis']; \\ \quad AbWorld; RabEndCIPd; RabIn \mid \\ req\sim m? = pdThis \\ \wedge chosenLost = chosenLost' \setminus \{pdThis\} \\ \wedge maybeLost = maybeLost' \setminus \{pdThis\} \\ \wedge definitelyLost = definitelyLost' \setminus \{pdThis\} \\ \vdash \\ AbTransferLost \end{array}$$

#### 18.8.1 The behaviour of *maybeLost* and *definitelyLost*

We argue that the transaction *pd* is initially not in *maybeLost* or *definitelyLost*, and is moved into *chosenLost'* by this case of the *ReqOkay* operation. The transaction initially was not far enough progressed to have the potential of being lost; afterwards it has progressed far enough that it may be lost, and we choose that it will be lost.

We have from *RabWillBeLostCIPd'*[...] that

$$pdThis \in chosenLost'$$

Therefore

$$pdThis \in maybeLost'$$

because *chosenLost' ⊆ maybeLost'*. But we can say that *pdThis ∉ definitelyLost'* (by lemma 'lost'). So we have

$$\begin{array}{l} definitelyLost = definitelyLost' \\ maybeLost = maybeLost' \setminus \{pdThis\} \\ chosenLost = chosenLost' \setminus \{pdThis\} \end{array}$$

### 18.8.2 *AbTransferLost*

In this section we prove that an *AbWorld* that has the correct retrieve properties also satisfies *AbTransferLost*. Recall, our proof obligation is

$$\begin{array}{l} \Phi BOp; ReqPurseOkay; RabOut; RabWillBeLostCIPd'[pdThis/pdThis']; \\ \quad AbWorld; RabEndCIPd; RabIn \mid \\ req\sim m? = pdThis \\ \wedge chosenLost = chosenLost' \setminus \{pdThis\} \\ \wedge maybeLost = maybeLost' \setminus \{pdThis\} \\ \wedge definitelyLost = definitelyLost' \setminus \{pdThis\} \\ \vdash \\ AbTransferLost \end{array}$$

Each element of *AbWorld* is defined by an explicit equation in *RabEndCIPd*, and we show that this value satisfies *AbTransferLost* by showing each predicate holds.

A-1 *AbOp*: This trivial: *AbOp* imposes no constraints.

A-2 *AbWorldSecureOp*

- *a?* ∈ ran *transfer*  
true by construction of *a?*
- no purses other than *from?* and *to?* change  
For *balance* and *lost* we show that *RabEndCIPd* and *RabWillBeLostCIPd'*[*pdThis/pdThis'*] are essentially the same. This is immediate because in both cases the relevant predicates are captured in the same schema *OtherPursesRab*.

A-3 *Authentic*[*from?/name?*], *Authentic*[*to?/name?*]

We have *pdThis* ∈ *maybeLost'*, hence it is in both *authenticFrom'* and in *authenticTo'*. Hence, by *ΦBOp* and *AbstractBetween*, it is also in both *authenticFrom* and in *authenticTo*.

A-4 *SufficientFundsProperty*

true from *ConPurse* constraint P-2b

A-5 *to? ≠ from?*

true because *pdThis* is a *PayDetails*.

A-6 *abAuthPurse' from? = ... , abAuthPurse' to? = ...*

Each of the four elements (*from* and *to* purses, each with *balance* and *lost*) are handled below, followed by all the other elements in one section.



$$\begin{aligned}
&= \text{sumValue}(((\text{definitelyLost}' \cup \text{chosenLost}' \setminus \{pdThis\}) \\
&\quad \cap \{pd : \text{PayDetails} \mid pd.\text{from} = pdThis.\text{to}\}) \\
&\quad \setminus \{pdThis\}) \quad [\text{section 18.8.1}] \\
&= \text{sumValue}(((\text{definitelyLost}' \cup \text{chosenLost}' \\
&\quad \cap \{pd : \text{PayDetails} \mid pd.\text{from} = pdThis.\text{to}\}) \\
&\quad \setminus \{pdThis\}) \quad [\text{rearrange}] \\
&= (\text{abAuthPurse}' pdThis.\text{to}).\text{lost} \quad [\text{RabWillBeLostCIPd}' \dots]
\end{aligned}$$

### The remaining from and to purse components

These are unchanging, by  $\exists \text{ConPurseReq}$ , and that the retrieves each define a unique abstract world.

- 18.8.2
- 18.8

## 18.9 case 3: ReqOkay and RabHasBeenLostPd'

$$\begin{aligned}
&\Phi BOp; \text{ReqPurseOkay}; \text{RabOut}; \text{RabHasBeenLostCIPd}'[pdThis/pdThis']; \\
&\quad \text{AbWorld}; \text{RabEndCIPd}; \text{RabIn} \mid \\
&\quad \text{req} \sim m? = pdThis \\
&\quad \wedge \text{chosenLost} = \text{chosenLost}' \setminus \{pdThis\} \\
&\quad \wedge \text{maybeLost} = \text{maybeLost}' \setminus \{pdThis\} \\
&\quad \wedge \text{definitelyLost} = \text{definitelyLost}' \setminus \{pdThis\} \\
&\vdash \\
&\text{AbTransferLost}
\end{aligned}$$

### 18.9.1 The behaviour of maybeLost and definitelyLost

We argue that the transaction  $pd$  is initially not in  $\text{maybeLost}$  or  $\text{definitelyLost}$ , and is moved into  $\text{definitelyLost}'$  by this case of the  $\text{ReqOkay}$  operation. The transaction initially was not far enough progressed to have the potential of being lost; afterwards it has progressed far enough that it has in fact been lost.

We have from  $\text{RabHasBeenLostCIPd}'$  that

$$pdThis \in \text{definitelyLost}'$$

Therefore  $pdThis \notin \text{maybeLost}'$  (by lemma 'lost'), and also  $pdThis \notin \text{chosenLost}'$

(because this is a subset of  $\text{maybeLost}'$ ). So we have

$$\begin{aligned}
\text{definitelyLost} &= \text{definitelyLost}' \setminus \{pdThis\} \\
\text{maybeLost} &= \text{maybeLost}' \\
\text{chosenLost} &= \text{chosenLost}'
\end{aligned}$$

### 18.9.2 AbTransferLost

In this section we prove that an  $\text{AbWorld}$  that has the correct retrieve properties also satisfies  $\text{AbTransferLost}$ . Recall, our proof obligation is

$$\begin{aligned}
&\Phi BOp; \text{ReqPurseOkay}; \text{RabOut}; \text{RabHasBeenLostCIPd}'[pdThis/pdThis']; \\
&\quad \text{AbWorld}; \text{RabEndCIPd}; \text{RabIn} \mid \\
&\quad \text{req} \sim m? = pdThis \\
&\quad \wedge \text{chosenLost} = \text{chosenLost}' \setminus \{pdThis\} \\
&\quad \wedge \text{maybeLost} = \text{maybeLost}' \setminus \{pdThis\} \\
&\quad \wedge \text{definitelyLost} = \text{definitelyLost}' \setminus \{pdThis\} \\
&\vdash \\
&\text{AbTransferLost}
\end{aligned}$$

Each element of  $\text{AbWorld}$  is defined by an explicit equation in  $\text{RabEndCIPd}$ , and we show that this value satisfies  $\text{AbTransferLost}$  by showing each predicate holds.

A-1  $\text{AbOp}$ : This trivial:  $\text{AbOp}$  imposes no constraints.

A-2  $\text{AbWorldSecureOp}$

- $a? \in \text{ran transfer}$   
true by construction of  $a?$
- no purses other than  $\text{from?}$  and  $\text{to?}$  change

For  $\text{balance}$  and  $\text{lost}$  we show that  $\text{RabEndCIPd}$  and  $\text{RabHasBeenLostCIPd}'[pdThis/pdThis]$  are essentially the same. This is immediate because in both cases the relevant predicates are captured in the same schema  $\text{OtherPursesRab}$ .

A-3  $\text{Authentic}[\text{from?}/\text{name?}], \text{Authentic}[\text{to?}/\text{name?}]$

We have  $pdThis \in \text{maybeLost}'$ , hence it is in both  $\text{authenticFrom}'$  and in  $\text{authenticTo}'$ . Hence, by  $\Phi BOp$  and  $\text{AbstractBetween}$ , it is also in both  $\text{authenticFrom}$  and in  $\text{authenticTo}$ .

A-4  $\text{SufficientFundsProperty}$

true from  $\text{ConPurse}$  constraint P-2b



A-5  $to? \neq from?$

true because  $pdThis$  is a  $PayDetails$ .

A-6  $abAuthPurse' from? = \dots, abAuthPurse' to? = \dots$

Each of the four elements ( $from$  and  $to$  purses, each with  $balance$  and  $lost$ ) are handled below, followed by all the other elements in one section.

#### The $from$ purse's balance component

$$\begin{aligned}
 & (abAuthPurse\ pdThis.from).balance \\
 &= (conAuthPurse\ pdThis.from).balance \\
 &\quad + \text{sumValue}(((maybeLost \setminus chosenLost) \\
 &\quad \cap \{pd : PayDetails \mid pd.to = pdThis.from\}) \\
 &\quad \setminus \{pdThis\}) \quad [RabEndClPd] \\
 &= (conAuthPurse\ pdThis.from).balance \\
 &\quad + \text{sumValue}(((maybeLost' \setminus chosenLost') \\
 &\quad \cap \{pd : PayDetails \mid pd.to = pdThis.from\}) \\
 &\quad \setminus \{pdThis\}) \quad [\text{section 18.9.1}] \\
 &= pdThis.value + (conAuthPurse'\ pdThis.from).balance \\
 &\quad + \text{sumValue}(((maybeLost' \setminus chosenLost') \\
 &\quad \cap \{pd : PayDetails \mid pd.to = pdThis.from\}) \\
 &\quad \setminus \{pdThis\}) \quad [ReqPurseOkay] \\
 &= pdThis.value + (abAuthPurse'\ pdThis.from).balance \\
 &\quad \quad \quad [RabHasBeenLostClPd'[\dots]]
 \end{aligned}$$

So

$$(abAuthPurse' from?).balance = (abAuthPurse from?).balance - value?$$

#### The $from$ purse's lost component

$$\begin{aligned}
 & (abAuthPurse\ pdThis.from).lost \\
 &= \text{sumValue}(((definitelyLost \cup chosenLost) \\
 &\quad \cap \{pd : PayDetails \mid pd.from = pdThis.from\}) \\
 &\quad \setminus \{pdThis\}) \quad [RabEndClPd] \\
 &= \text{sumValue}(((definitelyLost' \setminus \{pdThis\} \cup chosenLost') \\
 &\quad \cap \{pd : PayDetails \mid pd.from = pdThis.from\}) \\
 &\quad \setminus \{pdThis\}) \quad [\text{section 18.9.1}]
 \end{aligned}$$

$$\begin{aligned}
 &= \text{sumValue}(((definitelyLost' \cup chosenLost') \\
 &\quad \cap \{pd : PayDetails \mid pd.from = pdThis.from\}) \\
 &\quad \setminus \{pdThis\}) \quad [\text{rearrange}] \\
 &= (abAuthPurse'\ pdThis.from).lost - pdThis.value \\
 &\quad \quad \quad [RabHasBeenLostClPd'[\dots]]
 \end{aligned}$$

#### The $to$ purse's balance component

$$\begin{aligned}
 & (abAuthPurse\ pdThis.to).balance \\
 &= (conAuthPurse\ pdThis.to).balance \\
 &\quad + \text{sumValue}(((maybeLost \setminus chosenLost) \\
 &\quad \cap \{pd : PayDetails \mid pd.to = pdThis.to\}) \\
 &\quad \setminus \{pdThis\}) \quad [RabEndClPd] \\
 &= (conAuthPurse\ pdThis.to).balance \\
 &\quad + \text{sumValue}(((maybeLost' \setminus chosenLost') \\
 &\quad \cap \{pd : PayDetails \mid pd.to = pdThis.to\}) \\
 &\quad \setminus \{pdThis\}) \quad [\text{section 18.9.1}] \\
 &= (conAuthPurse'\ pdThis.to).balance \\
 &\quad + \text{sumValue}(((maybeLost' \setminus chosenLost') \\
 &\quad \cap \{pd : PayDetails \mid pd.to = pdThis.to\}) \\
 &\quad \setminus \{pdThis\}) \quad [\Phi BOp] \\
 &= (abAuthPurse'\ pdThis.to).balance \quad [RabHasBeenLostClPd'[\dots]]
 \end{aligned}$$

#### The $to$ purse's lost component

$$\begin{aligned}
 & (abAuthPurse\ pdThis.to).lost \\
 &= \text{sumValue}(((definitelyLost \cup chosenLost) \\
 &\quad \cap \{pd : PayDetails \mid pd.from = pdThis.to\}) \\
 &\quad \setminus \{pdThis\}) \quad [RabEndClPd] \\
 &= \text{sumValue}(((definitelyLost' \setminus \{pdThis\} \cup chosenLost') \\
 &\quad \cap \{pd : PayDetails \mid pd.from = pdThis.to\}) \\
 &\quad \setminus \{pdThis\}) \quad [\text{section 18.9.1}]
 \end{aligned}$$

$$\begin{aligned}
&= \text{sumValue}((\text{definitelyLost}' \cup \text{chosenLost}') \\
&\quad \cap \{pd : \text{PayDetails} \mid pd.\text{from} = pd\text{This}.\text{to}\}) \\
&\quad \setminus \{pd\text{This}\}) \quad [\text{rearrange}] \\
&= (\text{abAuthPurse}' pd\text{This}.\text{to}).\text{lost} \quad [\text{RabHasBeenLostCIPd}'[\dots]]
\end{aligned}$$

### The remaining from and to purse components

These are unchanging, by  $\exists \text{ConPurseReq}$ , and that the retrieves each define a unique abstract world.

- 18.9.2
- 18.9

### 18.10 case 4: ReqOkay and RabEndPd'

$$\begin{aligned}
&\Phi BOp; \text{ReqPurseOkay}; \text{RabOut}; \text{RabEndCIPd}'[pd\text{This}/pd\text{This}']; \\
&\quad \text{AbWorld}; \text{RabEndCIPd}; \text{RabIn} \mid \\
&\quad \text{req} \sim m? = pd\text{This} \\
&\quad \wedge \text{chosenLost} = \text{chosenLost}' \setminus \{pd\text{This}\} \\
&\quad \wedge \text{maybeLost} = \text{maybeLost}' \setminus \{pd\text{This}\} \\
&\quad \wedge \text{definitelyLost} = \text{definitelyLost}' \setminus \{pd\text{This}\} \\
&\quad \vdash \\
&\quad \text{AbTransfer}
\end{aligned}$$

We show that  $\text{RabEndCIPd}'[\dots]$  is *false* under  $\text{ReqOkay}$ , and then proceed by [contradiction], because this shows the antecedent of the theorem is false, and hence the theorem is true.

$$\begin{aligned}
&\Phi BOp; \text{ReqPurseOkay}; \text{RabOut}; \text{AbWorld}'; \\
&\quad pd\text{This} : \text{PayDetails}; \text{chosenLost}' : \mathbb{P} \text{PayDetails} \mid \\
&\quad \text{req} \sim m? = pd\text{This} \\
&\quad \vdash \\
&\quad \neg \text{RabEndCIPd}'[pd\text{This}/pd\text{This}']
\end{aligned}$$

It suffices to show that  $pd\text{This} \in \text{definitelyLost}' \cup \text{maybeLost}'$ . We have

$$\begin{aligned}
&\text{definitelyLost}' \cup \text{maybeLost}' \\
&= (\text{fromInEpa}' \cup \text{fromLogged}') \cap (\text{toInEpv}' \cup \text{toLogged}')
\end{aligned}$$

$\text{ReqPurseOkay}$  gives us that the after state of the purse is *epa*;  $pd\text{This}$  is in

$\text{authenticFrom}$ , from  $\Phi BOp$ ; hence  $pd\text{This}$  is in  $\text{fromInEpa}'$ . So it is sufficient to show either  $pd\text{This}$  is in  $\text{toInEpv}'$  or in  $\text{toLogged}'$ .

We know from the existence of the  $\text{req}$ , with  $\text{BetweenWorld}$  constraint B-1, that  $pd\text{This} \in \text{authenticTo}$ . There is no  $\text{ack}$  in the  $\text{ether}'$ :

$$\begin{aligned}
pd\text{This} \in \text{fromInEpr} & \quad [\text{precondition ReqPurseOkay}] \\
\Rightarrow \text{ack } pd\text{This} \notin \text{ether} & \quad [\text{BetweenWorld constraint B-9}] \\
\Rightarrow \text{ack } pd\text{This} \notin \text{ether}' & \quad [\text{defn. ReqPurseOkay and } \Phi BOp]
\end{aligned}$$

Hence

$$\begin{aligned}
\text{req } pd\text{This} \in \text{ether}' & \quad [\text{precondition ReqPurseOkay}] \\
\wedge \text{ack } pd\text{This} \notin \text{ether}' & \quad [\text{above}] \\
\Rightarrow pd\text{This} \in \text{toInEpv}' \cup \text{toLogged}' & \quad [\text{BetweenWorld constraint B-10}]
\end{aligned}$$

as required.

- 18.10
- 18.6
- 18

---

## Correctness of *Val*

### 19.1 Proof obligation

We have to prove the correct refinement of each abstract operation. In section 9.2.4 we give a general simplification of the correctness proof. We use lemma ‘multiple refinement’ (section 14.2) to split the proof obligation for each  $\mathcal{A}$  operation into one for each individual  $\mathcal{B}$  operation.

This chapter proves the  $\mathcal{B}$  operation.

- We use lemma ‘ignore’ (see section 14.3) to simplify the proof obligation by proving the correctness of *Ignore* (in section 14.7), leaving the *Okay* branch to be proven here.
- We use lemma ‘deterministic’ (section C.1) to reduce the proof obligation to the three cases **exists-pd**, **exists-chosenLost**, and **check-operation**.
- Since this operation refines *AbIgnore*, we use lemma ‘*AbIgnore*’ (from section C.3) to simplify **check-operation** to **check-operation-ignore**.

### 19.2 Instantiating lemma ‘deterministic’

The choices for the predicates relating to *pdThis* and *chosenLost* are based on the fact that the important transaction is the one stored in the purse performing the *ValOkay* operation, and that before the operation, the set of transactions chosen to be lost should be all those chosen to be lost after the operation. Thus

$$\mathcal{P} \Leftrightarrow \text{pdThis} = (\text{conAuthPurse name?}).\text{pdAuth}$$

$$\mathcal{Q} \Leftrightarrow \text{chosenLost} = \text{chosenLost}'$$

### 19.3 exists-pd

$$\begin{array}{l} \Phi BOp; ValPurseOkay; RabOut; RabCl'; RabIn \\ \vdash \\ \exists pdThis : PayDetails \bullet pdThis = (conAuthPurse name?).pdAuth \end{array}$$

**Proof:**

This is immediate by the [one point] rule, as we have an explicit definition of  $pdThis$ .

■ 19.3

### 19.4 exists-chosenlost

$$\begin{array}{l} \Phi BOp; ValPurseOkay; RabOut; RabClPd' [pdThis/pdThis']; RabIn | \\ pdThis = (conAuthPurse name?).pdAuth \\ \vdash \\ \exists chosenLost : \mathbb{P} PayDetails \bullet \\ chosenLost = chosenLost' \\ \wedge chosenLost \subseteq maybeLost \end{array}$$

**Proof:**

We can [one point] away the quantification because we have an explicit definition of  $chosenLost$  (as  $chosenLost'$ ). We show that the constraint holds by

$$\begin{array}{ll} chosenLost = chosenLost' & [\text{defn.}] \\ \subseteq maybeLost' & [RabClPd' \dots] \\ \subseteq maybeLost \setminus \{pdThis\} & [\text{see 19.6.7}] \\ \subseteq maybeLost & [\text{defn. } \setminus] \end{array}$$

■ 19.4

### 19.5 check-operation

$$\begin{array}{l} \Phi BOp; ValPurseOkay; RabClPd' [pdThis/pdThis']; AbWorld; RabClPd | \\ pdThis = (conAuthPurse name?).pdAuth \\ \wedge chosenLost = chosenLost' \\ \vdash \\ \forall n : \text{dom } abAuthPurse \bullet \\ (abAuthPurse' n).balance = (abAuthPurse n).balance \\ \wedge (abAuthPurse' n).lost = (abAuthPurse n).lost \end{array}$$

We prove this first by investigating the way in which the key sets  $definitelyLost$  and  $maybeLost$  are modified by the operation. Having got equations for these changes, we then look at the equations for the components  $balance$  and  $lost$  for two types of purses: the  $to$  purse in the transaction  $pdThis$ , and all other purses.

### 19.6 Behaviour of $maybeLost$ and $definitelyLost$

We argue that the transaction  $pdThis$  is initially in  $maybeLost$ , and is moved out of it, but not into  $definitelyLost'$ , by the  $ValOkay$  operation. This operation determines that the transaction is successful.

#### 19.6.1 fromLogged

No logs change, so

$$fromLogged' = fromLogged$$

#### 19.6.2 toLogged

No logs change, so

$$toLogged' = toLogged$$

After the operation the purse is in  $eaTo$ , and  $pdThis$  is in  $authenticTo$ , from  $\Phi BOp$ , hence  $pdThis \in toInEapayee'$ . Lemma 'notLoggedAndIn' (section C.12) gives us:

$$pdThis \notin toLogged'$$

#### 19.6.3 toInEpv

From the precondition of  $ValPurseOkay$  we know the purse is in  $epv$ , and we know that the name of this purse is equal to  $pdThis.to$ . After the operation, this purse is in  $eaTo$  (that is, not in  $epv$ ). No other purses change.

$$toInEpv' = toInEpv \setminus \{pdThis\}$$

$$toInEpv = toInEpv' \cup \{pdThis\}$$



$$\begin{aligned}
&= (\text{conAuthPurse } n).balance \\
&\quad + \text{sumValue}((\text{maybeLost} \setminus \text{chosenLost}) \\
&\quad \cap \{pd : \text{PayDetails} \mid pd.to = n\}) \setminus \{pdThis\}) \\
&\hspace{10em} [\text{equation earlier}]
\end{aligned}$$

$$\begin{aligned}
&= (\text{conAuthPurse } n).balance \\
&\quad + \text{sumValue}((\text{maybeLost} \setminus \text{chosenLost}) \\
&\quad \cap \{pd : \text{PayDetails} \mid pd.to = n\}) \setminus \{pdThis\}) \\
&\hspace{10em} [\Phi BOp]
\end{aligned}$$

$$= (\text{abAuthPurse } n).balance \hspace{10em} [RabOkayClPd]$$

■ 19.7.1

**19.7.2 Case lost component for non- $pdThis.to$  purse**

In this case the defining equations in the retrieve depend upon *definitelyLost*  $\cup$  *chosenLost*, which we derived as unchanging earlier.  $\Phi BOp$  does not change the concrete values, so the abstract values do not change either.

■ 19.7.2

**19.7.3 Case balance component for  $pdThis.to$  purse**

$$\begin{aligned}
&(\text{abAuthPurse } pdThis.to).balance \\
&= (\text{conAuthPurse } pdThis.to).balance \\
&\quad + \text{sumValue}((\text{maybeLost}' \setminus \text{chosenLost}') \\
&\quad \cap \{pd : \text{PayDetails} \mid pd.to = pdThis.to\}) \setminus \{pdThis\}) \\
&\hspace{10em} [RabEndClPd' \dots]
\end{aligned}$$

$$\begin{aligned}
&= (\text{conAuthPurse } pdThis.to).balance \\
&\quad + \text{sumValue}(((\text{maybeLost}' \setminus \text{chosenLost}') \cup \{pdThis\}) \\
&\quad \cap \{pd : \text{PayDetails} \mid pd.to = pdThis.to\}) \setminus \{pdThis\}) \\
&\hspace{10em} [\text{union and subtraction cancel}]
\end{aligned}$$

$$\begin{aligned}
&= (\text{conAuthPurse } pdThis.to).balance \\
&\quad + \text{sumValue}((\text{maybeLost} \setminus \text{chosenLost}) \\
&\quad \cap \{pd : \text{PayDetails} \mid pd.to = pdThis.to\}) \setminus \{pdThis\}) \\
&\hspace{10em} [\text{equation earlier}]
\end{aligned}$$

$$\begin{aligned}
&= (\text{conAuthPurse } pdThis.to).balance + pdThis.value \\
&\quad + \text{sumValue}((\text{maybeLost} \setminus \text{chosenLost}) \\
&\quad \cap \{pd : \text{PayDetails} \mid pd.to = pdThis.to\}) \setminus \{pdThis\}) \\
&\hspace{10em} [\text{ValPurseOkay}]
\end{aligned}$$

$$= (\text{abAuthPurse } pdThis.to).balance \hspace{10em} [RabOkayClPd]$$

■ 19.7.3

**19.7.4 Case lost component for  $pdThis.to$  purse**

In this case the defining equations in the retrieve depend upon *definitelyLost*  $\cup$  *chosenLost*, which we derived as unchanging earlier. *ValOkay* does not change the concrete values, so the abstract values do not change either.

■ 19.7.4

■ 19.7

■ 19

## Correctness of *Ack*

### 20.1 Proof obligation

We have to prove the correct refinement of each abstract operation. In section 9.2.4 we give a general simplification of the correctness proof. We use lemma 'multiple refinement' (section 14.2) to split the proof obligation for each  $\mathcal{A}$  operation into one for each individual  $\mathcal{B}$  operation.

This chapter proves the  $\mathcal{B}$  operation.

- We use lemma 'ignore' (see section 14.3) to simplify the proof obligation by proving the correctness of *Ignore* (in section 14.7), leaving the *Okay* branch to be proven here.
- We use lemma 'deterministic' (section C.1) to reduce the proof obligation to the three cases **exists-pd**, **exists-chosenLost**, and **check-operation**.
- Since this operation refines *AbIgnore*, we use lemma '*AbIgnore*' (from section C.3) to simplify **check-operation** to **check-operation-ignore**.

### 20.2 Instantiating lemma 'deterministic'

We must instantiate two general predicates relating to *pdThis* and *chosenLost*. The choices for these predicates are based on the fact that the important transaction is the one stored in the purse performing the *AckOkay* operation, and that before the operation, the set of transactions chosen to be lost should be all those chosen to be lost after the operation, because this operation plays no

part in deciding which transactions succeed and which ones lose. Thus

$$\mathcal{P} \Leftrightarrow pdThis = (conAuthPurse\ name?).pdAuth$$

$$\mathcal{Q} \Leftrightarrow chosenLost = chosenLost'$$

### 20.3 exists-pd

$$\Phi BOp; AckPurseOkay; RabOut; RabCl'; RabIn$$

⊢

$$\exists pdThis : PayDetails \bullet pdThis = (conAuthPurse\ name?).pdAuth$$

**Proof:**

This is immediate by [one point] rule, as we have an explicit definition of *pdThis*.

■ 20.3

### 20.4 exists-chosenlost

$$\Phi BOp; AckPurseOkay; RabOut; RabClPd'[pdThis/pdThis']; RabIn |$$

$$pdThis = (conAuthPurse\ name?).pdAuth$$

⊢

$$\exists chosenLost : \mathbb{P}\ PayDetails \bullet$$

$$chosenLost = chosenLost'$$

$$\wedge chosenLost \subseteq maybeLost$$

**Proof:**

We can [one point] away the quantification because we have an explicit definition of *chosenLost* (as *chosenLost'*). We show that the constraint holds by

$$chosenLost = chosenLost' \quad [\text{def}]$$

$$\subseteq maybeLost' \quad [RabClPd'[\dots]]$$

$$\subseteq maybeLost \quad [\text{see 20.6.6}]$$

■ 20.4

### 20.5 check-operation

$$\Phi BOp; AckPurseOkay; RabClPd'[pdThis/pdThis']; AbWorld; RabClPd |$$

$$pdThis = (conAuthPurse\ name?).pdAuth$$

$$\wedge chosenLost = chosenLost'$$

⊢

$$\forall n : \text{dom } abAuthPurse \bullet$$

$$(abAuthPurse'\ n).balance = (abAuthPurse\ n).balance$$

$$\wedge (abAuthPurse'\ n).lost = (abAuthPurse\ n).lost$$

**Proof:**

We prove this by investigating the way in which the key sets *definitelyLost* and *maybeLost* are modified by the operation.

#### 20.6 Behaviour of *maybeLost* and *definitelyLost*

We argue that the transaction *pd* is initially in neither *maybeLost* nor *definitelyLost*, and is not moved into either of them by the *AckOkay* operation. The transaction was initially far enough along to have already succeeded.

##### 20.6.1 Behaviour of *fromLogged*

From  $\Phi BOp$ , which says that only the purse *name?* changes, and then only according to *AckPurseOkay*, and from the definition of *AckPurseOkay*, in which  $exLog' = exLog$ , we can see that

$$fromLogged' = fromLogged$$

##### 20.6.2 Behaviour of *toLogged*

Exactly as we argued for *fromLogged*,

$$toLogged' = toLogged$$

##### 20.6.3 Behaviour of *toInEpv*

If  $toInEpv' \neq toInEpv$ , there must be some *pd* in one and not in the other. From the definition of *toInEpv*, this means that for some purse that changes, either before or after the operation its status must equal *epv*. That is,

$$(conAuthPurse\ pd.to).status = epv$$

∨

$$(conAuthPurse'\ pd.to).status = epv$$



From  $\Phi BOp$  we have that the only purse that changes is  $name?$ . From *AckPurseOkay* we have that

$$\begin{aligned} (conAuthPurse\ name?).status &= epa \\ (conAuthPurse'\ name?).status &= eaFrom \end{aligned}$$

(neither equal to  $epv$ ). Therefore, no such  $pd$  exists, and we have

$$toInEpv' = toInEpv$$

#### 20.6.4 Behaviour of $fromInEpa$

If  $fromInEpa' \neq fromInEpa$ , there must be some  $pd$  in one and not in the other. From the definition of  $fromInEpa$ , this means that for some purse that changes, either before or after the operation its status must equal  $epa$ . That is,

$$\begin{aligned} (conAuthPurse\ pd.from).status &= epa \\ \vee \\ (conAuthPurse'\ pd.from).status &= epa \end{aligned}$$

The only name that changes is  $name?$ , and from *AckPurseOkay* we have that

$$\begin{aligned} (conAuthPurse\ name?).status &= epa \\ (conAuthPurse'\ name?).status &= eaFrom \end{aligned}$$

Therefore, we have

$$\begin{aligned} fromInEpa' &= fromInEpa \setminus \{ pd : PayDetails \mid pd.from = name? \\ &\quad \wedge (conAuthPurse\ name?).status = epa \\ &\quad \wedge (conAuthPurse\ name?).pdAuth = pd \} \end{aligned}$$

In fact, the last predicate in this set limits the  $pd$  to a single value, equal to  $pdThis$ , so we have

$$fromInEpa' = fromInEpa \setminus \{ pdThis \}$$

We now build up the two sets  $definitelyLost$  and  $maybeLost$ .

#### 20.6.5 Behaviour of $definitelyLost$

$$\begin{aligned} definitelyLost' &= toLogged' \cap (fromLogged' \cup fromInEpa') && [\text{defn}] \\ &= toLogged' && [\text{above identities}] \\ &\quad \cap (fromLogged' \cup (fromInEpa \setminus \{ pdThis \})) \\ &= toLogged' && [pdThis \notin fromLogged', \text{ see below}] \\ &\quad \cap ((fromLogged' \cup fromInEpa) \setminus \{ pdThis \}) \\ &= (fromLogged' \cup fromInEpa) && [\text{algebra}] \\ &\quad \cap (toLogged' \setminus \{ pdThis \}) \\ &= (fromLogged' \cup fromInEpa) \cap toLogged' && [pdThis \notin toLogged', \text{ see below}] \\ &= definitelyLost && [\text{defn}] \end{aligned}$$

We have  $pdThis \notin fromLogged'$ , from the fact that  $pdThis \in fromInEpa$  (because the before purse state is  $epa$ , and  $\Phi BOp$  gives  $pdThis \in authenticFrom$ ), and using lemma 'notLoggedAndIn'.

We have  $pd \notin toLogged'$ :

$$\begin{aligned} ack\ pd \in ether &&& [\text{precondition AckPurseOkay}] \\ \Rightarrow pd \notin toInEpv \cup toLogged' &&& [\text{BetweenWorld constraint B-10}] \\ \Rightarrow pd \notin toLogged' &&& [\text{law}] \end{aligned}$$

Thus we have

$$definitelyLost' = definitelyLost$$

#### 20.6.6 Behaviour of $maybeLost$

$$\begin{aligned} maybeLost' &= (fromInEpa' \cup fromLogged') \cap toInEpv' && [\text{defn.}] \\ &= (fromInEpa \cup (fromLogged' \setminus \{ pdThis \})) \cap toInEpv && [\text{above identities}] \\ &= ((fromInEpa \cup fromLogged') \setminus \{ pdThis \}) \cap toInEpv && [pdThis \notin fromLogged', \text{ as above}] \\ &= (fromInEpa \cup fromLogged') \cap (toInEpv \setminus \{ pdThis \}) && [\text{algebra}] \\ &= (fromInEpa \cup fromLogged') \cap toInEpv && [pdThis \notin toInEpv, \text{ see below}] \\ &= maybeLost && [\text{defn.}] \end{aligned}$$

We have  $pdThis \notin toInEpv$ :

$$\begin{aligned} ack\ pd \in ether & && [\text{precondition } AckOkay] \\ \Rightarrow pdThis \notin toInEpv \cup toLogged & && [BetweenWorld \text{ constraint B-10}] \\ \Rightarrow pdThis \notin toInEpv & && [\text{law}] \end{aligned}$$

Thus we have

$$maybeLost' = maybeLost$$

## 20.7 Finishing proof of check-operation

The above shows that none of the three sets *definitelyLost*, *maybeLost* or *chosenLost* changes. As *AckOkay* does not alter any concrete *balance* or *lost*, and given that the abstract values are defined solely in terms of these (unchanging) values, it follows that the abstract values don't change, thus discharging the **check-operation** proof obligation.

- 20.5
- 20

---

## Correctness of *ReadExceptionLog*

### 21.1 Proof obligation

We have to prove the correct refinement of each abstract operation. In section 9.2.4 we give a general simplification of the correctness proof. We use lemma 'multiple refinement' (section 14.2) to split the proof obligation for each  $\mathcal{A}$  operation into one for each individual  $\mathcal{B}$  operation.

This chapter proves the  $\mathcal{B}$  operation.

- We use lemma 'ignore' (see section 14.3) to simplify the proof obligation by proving the correctness of *Ignore* (in section 14.7), and *Abort* (in section 14.8), leaving the *Okay* branch to be proven here.
- Since the *Okay* branch of this operation is expressed as a promotion of *AbortPurseOkay* composed with a simpler *EafromPurseOkay* operation, we use lemma 'abort backward' (section C.5), and prove only that the promotion of the simpler operation is a refinement.
- We use lemma 'deterministic' (section C.1) to reduce the proof obligation to the three cases **exists-pd**, **exists-chosenLost**, and **check-operation**.
- Since this operation leaves the sets *maybeLost* and *definitelyLost* unchanged, we use lemma 'lost unchanged' (section C.2) to discharge the **exists-pd-and exists chosenLost-obligations** automatically.
- Since this operation refines *AbIgnore*, we use lemma '*AbIgnore*' (from section C.3) to simplify **check-operation** to **check-operation-ignore**.

### 21.2 Invoking lemma ‘lost unchanged’

We have the constraint  $\exists \text{ConPurse}$  in the definition of *ReadExceptionLogPurseEafromOkay*. From  $\Phi \text{BOP}$  and  $\exists \text{ConPurse}$ , we know that *archive* and *conAuthPurse* remain unchanged, as do *definitelyLost* and *maybeLost*. Hence we can invoke lemma ‘Lost unchanged’.

### 21.3 check-operation-ignore

$$\begin{aligned} & \Phi \text{BOP}; \text{ReadExceptionLogPurseEafromOkay}; \\ & \quad \text{RabOut}; \text{RabClPd}' [\text{pdThis} / \text{pdThis}']; \\ & \quad \text{AbWorld}; \text{RabClPd}; \text{RabIn} | \\ & \quad \text{chosenLost}' = \text{chosenLost} \\ & \quad \wedge \text{maybeLost}' = \text{maybeLost} \\ & \quad \wedge \text{definitelyLost}' = \text{definitelyLost} \\ & \vdash \\ & \forall n : \text{dom } \text{abAuthPurse} \bullet \\ & \quad (\text{abAuthPurse}' n). \text{balance} = (\text{abAuthPurse } n). \text{balance} \\ & \quad \wedge (\text{abAuthPurse}' n). \text{lost} = (\text{abAuthPurse } n). \text{lost} \end{aligned}$$

**Proof:**

We have that *maybeLost* and *definitelyLost* are unchanged from the hypothesis. Hence the *balance* and *lost* components of all the abstract purses remain unchanged, satisfying our proof requirement.

- 21.3
- 21

## Correctness of *ClearExceptionLog*

### 22.1 Proof obligation

We have to prove the correct refinement of each abstract operation. In section 9.2.4 we give a general simplification of the correctness proof. We use lemma ‘multiple refinement’ (section 14.2) to split the proof obligation for each  $\mathcal{A}$  operation into one for each individual  $\mathcal{B}$  operation.

This chapter proves the  $\mathcal{B}$  operation.

- We use lemma ‘ignore’ (see section 14.3) to simplify the proof obligation by proving the correctness of *Ignore* (in section 14.7), and *Abort* (in section 14.8), leaving the *Okay* branch to be proven here.
- Since the *Okay* branch of this operation is expressed as a promotion of *AbortPurseOkay* composed with a simpler *EafromPurseOkay* operation, we use lemma ‘abort backward’ (section C.5), and prove only that the promotion of the simpler operation is a refinement.
- We use lemma ‘deterministic’ (section C.1) to reduce the proof obligation to the three cases **exists-pd**, **exists-chosenLost**, and **check-operation**.
- Since this operation leaves the sets *maybeLost* and *definitelyLost* unchanged, we use lemma ‘lost unchanged’ (section C.2) to discharge the **exists pd-and exists chosenLost-obligations** automatically.
- Since this operation refines *AbIgnore*, we use lemma ‘AbIgnore’ (from section C.3) to simplify **check-operation** to **check-operation-ignore**.

## 22.2 Invoking lemma ‘Lost unchanged’

The purse’s exception log is cleared, so we cannot use the ‘sufficient conditions’ to invoke lemma ‘lost unchanged’: we need first to show that *fromLogged* and *toLogged* are unchanged.

We have from the operation definition that the exception log details in the purse that are to be cleared match the ones in the *exceptionLogClear* message. We have, from constraint B-15 that the log details in the message are already in the *archive*. So deleting them from the purse will not change *allLogs*. But *fromLogged* and *toLogged* partition *allLogs*, so these do not change either.

Hence we can invoke lemma ‘Lost unchanged’.

## 22.3 check-operation-ignore

$$\begin{aligned} & \Phi BOp; ClearExceptionLogPurseEafromOkay; \\ & \quad RabOut; RabClPd' [pdThis | pdThis']; \\ & \quad AbWorld; RabClPd; RabIn | \\ & \quad chosenLost' = chosenLost \\ & \quad \wedge maybeLost' = maybeLost \\ & \quad \wedge definitelyLost' = definitelyLost \\ & \vdash \\ & \forall n : \text{dom } abAuthPurse \bullet \\ & \quad (abAuthPurse' n).balance = (abAuthPurse n).balance \\ & \quad \wedge (abAuthPurse' n).lost = (abAuthPurse n).lost \end{aligned}$$

### Proof:

We have that *maybeLost* and *definitelyLost* are unchanged from the hypothesis. Hence the *balance* and *lost* components of all the abstract purses remain unchanged.

- 22.3
- 22

# Correctness of *AuthoriseExLogClear*

## 23.1 Proof obligation

We have to prove the correct refinement of each abstract operation. In section 9.2.4 we give a general simplification of the correctness proof. We use lemma ‘multiple refinement’ to split the proof obligation for each  $\mathcal{A}$  operation into one for each individual  $\mathcal{B}$  operation.

This chapter proves the  $\mathcal{B}$  operation.

- We use lemma ‘ignore’ to simplify the proof obligation further to proving the correctness of *Ignore* (section 14.7), leaving the *Okay* branch to be proven.

We cannot use any of the other simplifications directly for *AuthoriseExLogClear*, since it cannot be written as a promotion. So the correctness proof obligation for *AuthoriseExLogClear* is

$$\begin{aligned} & AuthoriseExLogClearOkay; Rab'; RabOut \\ & \vdash \\ & \exists AbWorld; a? : AIN \bullet Rab \wedge RabIn \wedge AbIgnore \end{aligned}$$

## 23.2 Proof

First we choose an input. We argue exactly as in section 14.4.1 to reduce the obligation to:

$$\begin{aligned} & AuthoriseExLogClearOkay; Rab'; RabOut; RabIn \\ & \vdash \\ & \exists AbWorld \bullet Rab \wedge AbIgnore \end{aligned}$$

We [cut] in a before  $AbWorld$  equal to the after  $AbWorld'$  in  $Rab'$  (the side lemma is trivial), and use [consq exists] to remove the quantifier from the consequent.

$$\begin{array}{l} \text{AuthoriseExLogClearOkay; } Rab'; RabOut; RabIn; AbWorld \mid \\ \quad \theta AbWorld = \theta AbWorld' \\ \vdash \\ Rab \wedge AbIgnore \end{array}$$

$AbIgnore$  is certainly satisfied by the equal abstract before and after worlds.

It remains to show that  $Rab$  is satisfied. The only difference between the concrete before and after worlds, as given by *AuthoriseExLogClearOkay*, is the addition of an *exceptionLogClear* message in the *ether*. But  $Rab$  does not depend on *exceptionLogClear* messages, and so we can deduce  $Rab$  directly from  $Rab'$

- 23.2
- 23

---

## Correctness of *Archive*

### 24.1 Proof obligation

We have to prove the correct refinement of each abstract operation. In section 9.2.4 we give a general simplification of the correctness proof. We use lemma ‘multiple refinement’ to split the proof obligation for each  $\mathcal{A}$  operation into one for each individual  $\mathcal{B}$  operation.

This chapter proves the  $\mathcal{B}$  operation.

We cannot use any more of the usual simplifications directly for *Archive*, since it cannot be written as a promotion. So the correctness proof obligation for *Archive* is

$$\text{Archive; } Rab'; RabOut \vdash \exists AbWorld; a? : AIN \bullet Rab \wedge RabIn \wedge AbIgnore$$

### 24.2 Proof

First we choose an input. We argue exactly as in section 14.4.1 to reduce the obligation to:

$$\text{Archive; } Rab'; RabOut; RabIn \vdash \exists AbWorld \bullet Rab \wedge AbIgnore$$

We [cut] in a before  $AbWorld$  equal to the after  $AbWorld'$  in  $Rab'$  (the side lemma is trivial), and use [consq exists] to remove the quantifier from the consequent.

$$\begin{array}{l} \text{Archive; } Rab'; RabOut; RabIn; AbWorld \mid \\ \quad \theta AbWorld = \theta AbWorld' \\ \vdash \\ Rab \wedge AbIgnore \end{array}$$

*Abignore* is certainly satisfied by the equal abstract before and after worlds.

It remains to show that *Rab* is satisfied. The only difference between the concrete before and after worlds, as given by *Archive*, is the inclusion of some log details in the *archive*. We have, from *BetweenWorld* constraint B-14, that the log details added to the archive from the *exceptionLogResult* message are already in *allLogs*. So, although the *archive* grows, the operation does not add any new logs to the *world*. Thus *fromLogged* and *toLogged* don't change. Hence *maybeLost* and *definitelyLost* don't change. Therefore, nothing that *Rab* relies upon changes in the concrete world, and so we can deduce *Rab* directly from *Rab'*.

- 24.2
- 24

## Part III

### Second Refinement: *B* to *C*

## Refinement Proof Rules

### 25.1 Security of the implementation

We prove the concrete model  $C$  is secure with respect to the between model  $B$  by showing that every concrete operation correctly refines a between operation. The concrete and between operations are similarly-named.

The full list of refinements is:

$StartTo \sqsubseteq CStartTo$

$StartFrom \sqsubseteq CStartFrom$

$Req \sqsubseteq CReq$

$Val \sqsubseteq CVal$

$Ack \sqsubseteq CAck$

$ReadExceptionLog \sqsubseteq CReadExceptionLog$

$ClearExceptionLog \sqsubseteq CClearExceptionLog$

$AuthoriseExLogClear \sqsubseteq CAuthoriseExLogClear$

$Archive \sqsubseteq CArchive$

$Abort \sqsubseteq CAbort$

$Increase \sqsubseteq CIncrease$

$Ignore \sqsubseteq CIgnore$

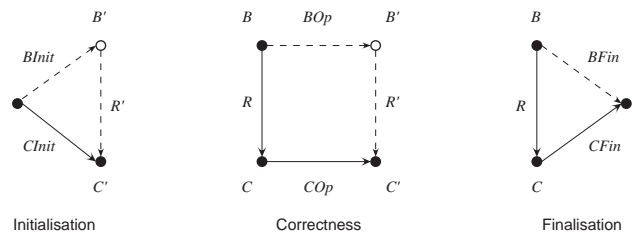


Figure 25.1: A summary of the forward proof rules. The hypothesis is the existence of the lower (solid) path. The proof obligation is to demonstrate the existence of an upper (dashed) path.

## 25.2 Forwards rules proof obligations

Each of these refinements must be proved correct. [Spivey 1992b, Chapter 5] presents the theorems that need to be proved for the most commonly-occurring case of non-determinism, sometimes called ‘downward’ or ‘forward’ conditions, where the abstract and concrete inputs and outputs are identical. These, augmented with a finalisation proof, are appropriate for the  $\mathcal{B}$  to  $\mathcal{C}$  refinement proofs.

The forward rules are summarised in figure 25.1. Note how the paths are different from the backward case (figure 9.1) because of the direction of the  $R$  arrows.

### 25.2.1 Retrieve

The retrieve relation has one part that links the abstract and concrete states.

### 25.2.2 Initialisation

$$CInit \vdash \exists B' \bullet BInit \wedge R'$$

### 25.2.3 Finalisation

$$R; CFIn \vdash BFin$$

### 25.2.4 Applicability

$$R; BIn \mid \text{pre } BOp \vdash \text{pre } COp$$

### 25.2.5 Correctness

$$R; COp \mid \text{pre } BOp \vdash \exists B' \bullet R' \wedge BOp$$

We can simplify the correctness condition because we know that all the between operations are total, i.e.

$$\text{pre } BOp = \text{true}$$

This was proved earlier, in section 8.3.2.

We can therefore simplify the correctness condition to

$$R; COp \vdash \exists B' \bullet R' \wedge BOp$$



---

## $\mathcal{B}$ to $\mathcal{C}$ retrieve relation

### 26.1 Retrieve state

The  $\mathcal{B}$  and  $\mathcal{C}$  worlds are identical, except that the  $\mathcal{C}$  world can 'lose' *ether* messages.

<i>Rbc</i>
<i>BetweenWorld</i>
<i>ConWorld</i> <sub>0</sub>
$conAuthPurse_0 = conAuthPurse$
$ether_0 \sqsubseteq ether$
$archive_0 = archive$

The subscript zero on the concrete world serves to distinguish like-named between and concrete components.

---

## Initialisation, Finalisation, and Applicability

### 27.1 Initialisation proof

$$\text{ConInitState} \vdash \exists \text{BetweenWorld}' \bullet \text{BetweenInitState} \wedge \text{Rbc}'$$

**Proof:**

We expand  $\text{ConInitState}$  in the hypothesis according to its definition.

$$\begin{aligned} & \text{ConWorld}'_0 \mid \\ & (\exists \text{BetweenWorld}' \mid \text{BetweenInitState} \bullet \\ & \quad \text{conAuthPurse}'_0 = \text{conAuthPurse}' \\ & \quad \wedge \text{archive}' = \text{archive}' \\ & \quad \wedge \{\perp\} \subseteq \text{ether}'_0 \subseteq \text{ether}') \\ & \vdash \\ & \exists \text{BetweenWorld}' \bullet \text{BetweenInitState} \wedge \text{Rbc}' \end{aligned}$$

From the definition of  $\text{Rbc}'$ , we can see that the consequent follows directly from the hypothesis.

■ 27.1

### 27.2 Finalisation proof

$$\text{Rbc}; \text{ConFinState} \vdash \text{BetwFinState}$$

**Proof:**

We have defined  $\text{ConFinState}$  and  $\text{BetwFinState}$  to have the same mathematical form.

$Rbc$  in the hypothesis requires the concrete and between purse states and archives to be identical, and allows the between  $ether$  to be bigger than the concrete  $ether$ .

Finalisation of the purses depends only on the purse states (identical by hypothesis) and on the sets  $definitelyLost$  and  $maybeLost$ . These sets themselves depend only on purse states and on the archive (also identical for concrete and between worlds by the retrieve in the hypothesis). As result,  $gAuthPurse$  for between finalisation is identical to that for concrete finalisation.

■ 27.2

### 27.3 Applicability proofs

Applicability follows automatically from the totality of the concrete operations as shown in section 8.4.

■ 27.3

---

## Lemmas for the $\mathcal{B}$ to $\mathcal{C}$ correctness proofs

### 28.1 Specialising the proof rules

For each concrete operation  $COp$  and corresponding between operation  $BOP$  we have to show

$$Rbc; COp \vdash \exists \textit{BetweenWorld}' \bullet Rbc' \wedge BOP$$

Many operations are defined as the disjunction of other operations. A  $COp$  will have the same branches as a corresponding  $BOP$ : a  $CIgnore$  branch, and either a  $CAbort$  or  $COpOkay$  branch, or both. We split the proof obligation into  $CIgnore$ ,  $CAbort$  and  $COpOkay$  branches, as we did in section 14.3. This gives some or all of the following proof requirements, depending on which branches are in  $COp$ :

$$Rbc; CIgnore \vdash \exists \textit{BetweenWorld}' \bullet Rbc' \wedge CIgnore$$

$$Rbc; CAbort \vdash \exists \textit{BetweenWorld}' \bullet Rbc' \wedge CAbort$$

$$Rbc; COpOkay \vdash \exists \textit{BetweenWorld}' \bullet Rbc' \wedge COpOkay$$

The correctness of the  $CIgnore$  branch is dealt with below in section 28.2. We then develop the correctness proof for the  $CAbort$  and  $COpOkay$  branches, and introduce a lemma applicable to certain operations. Following this, we present the proof of correctness of two common branches —  $CIncrease$  and  $CAbort$ .

## 28.2 Correctness of *CIgnore*

The correctness of the *CIgnore* branch follows trivially by choosing

$$\theta_{BetweenWorld'} = \theta_{BetweenWorld}$$

■ 28.2

## 28.3 Correctness of a branch of the operation

### 28.3.1 Choosing *BetweenWorld'*

In choosing *BetweenWorld'*, we base our choice of the *conAuthPurse'* and *archive'* components on *Rbc'*, and our choice of the *ether'* component on *BOP-Okay'*.

We have *conAuthPurse'\_0* and *archive'\_0* in the hypothesis, and we use this to provide the value for *conAuthPurse'* and *archive'*, respectively (this satisfies the constraint on *conAuthPurse'* and *archive'* in *Rbc'*).

$$\begin{aligned} conAuthPurse' &= conAuthPurse'_0 \\ archive' &= archive'_0 \end{aligned}$$

*m!* and *ether* are declared in the hypothesis, and *ether'* can be constructed deterministically from these (note that the following construction satisfies the relevant constraint in *BOPOkay* — either in  $\Phi BOP$  or explicitly as in *Archive*).

$$ether' = ether \cup \{m!\}$$

We need to show that the chosen *BetweenWorld'* and *m!* satisfy each of the conjuncts in the consequent (retrieve *Rbc'* and operation *BOPOkay*).

We also need to show that this choice is indeed an after *BetweenWorld'* (that it satisfies the constraints on *BetweenWorld* specified in section 5.3).

### 28.3.2 Case *BOPOkay*

From the choice of *ether'* above, the relevant constraint on *ether'* in *BOPOkay* is satisfied by construction.

At most one purse changes in *COPOkay*. Let us call this new purse value *p*. This gives

$$\begin{aligned} conAuthPurse'_0 &= conAuthPurse_0 \oplus \{p\} \\ conAuthPurse'_0 &= conAuthPurse \oplus \{p\} && [Rbc] \\ conAuthPurse' &= conAuthPurse \oplus \{p\} && [\text{choice of } conAuthPurse'] \end{aligned}$$

This satisfies the constraint on *conAuthPurse'* in *BOPOkay* (where at most one purse changes in an identical manner to *COPOkay*).

*archive'* is a function of *archive* and *m!*, defined in *BOPOkay*. Call this function *f*:

$$| f : Logbook \times MESSAGE \rightarrow Logbook$$

Because *COPOkay* is defined in an analogous way, *f* also relates *archive'\_0* to *archive\_0* and *m!*.

From the hypothesis we have *COPOkay* and *Rbc*, and with our choice of *archive'* we have, respectively

$$\begin{aligned} archive'_0 &= f(archive_0, m!) \\ \wedge archive &= archive_0 \\ \wedge archive' &= archive'_0 \end{aligned}$$

Substituting the latter two equations into the first gives the predicate in *BOP-Okay*.

Thus, the *BOPOkay* constraints on all the components of our chosen *BetweenWorld'* are satisfied under the correctness hypothesis and choice of *BetweenWorld'*.

■ 28.3.2

### 28.3.3 Case *Rbc'*

Both the *conAuthPurse'* and *archive'* components of *BetweenWorld'* satisfy *Rbc'* from the choice of *BetweenWorld'*.

All *COPOkay* operations constrain *ether'* as

$$ether'_0 \subseteq ether_0 \cup \{m!\}$$

either through  $\Phi COP$ , or explicitly in *CArchive*. Hence for *ether'* we have

$$\begin{aligned} ether' & \\ &= ether \cup \{m!\} && [\text{choice of } ether'] \\ &\supseteq ether_0 \cup \{m!\} && [Rbc] \\ &\supseteq ether'_0 && [COPOkay] \end{aligned}$$

This satisfies the constraint on *ether'* in *Rbc'*.

### 28.3.4 Case ‘obey constraints’

We know from the hypothesis that the before *BetweenWorld* satisfies the constraints, so we need check only that the chosen message *m*!, and any change of purse state during the operation, maintains this constraint.

**Lemma 28.1** (constraint) If an operation obeys the following properties, then it preserves the *BetweenWorld* constraints:

- it does not change purse status or current transaction details (*pdAuth*)
- it does not change *allLogs*
- it does not change the payment detail messages, exception log read messages or exception log clear messages in the *ether* (either by not emitting such a message, or by emitting an already existing message)
- no sequence number decreases (all concrete operations have the property, so it is automatically satisfied)

■

#### Proof:

The *BetweenWorld* constraints refer only to certain *ether* messages (*req*, *val*, *ack*, *exceptionLogResult* and *exceptionLogClear*), and relate their presence or absence to purse status (*status*, *pdAuth* and *nextSeqNo*) and *allLogs*. From the hypothesis we can invoke lemma ‘logs unchanged’ (section C.7) to say that, as *allLogs* does not change, not does *allLogs*. So operations that do not change the purse status, do not change *allLogs*, and do not emit any relevant new messages, will automatically preserve the constraints.

■ 28.3.4

Even when lemma ‘constraint’ does not apply, we know from the form of the operation that at most one purse changes, and one message is emitted. As at most one purse changes, the proof that the *BetweenWorld* constraints are preserved need refer only to this purse; the constraints hold on the other purses before the operation by hypothesis, and so they hold afterward, too.

### 28.3.5 Summary of *ConOkay* proof obligation

For each operation, we have to show that either lemma ‘constraint’ holds or that the choice of *BetweenWorld*’ obeys the constraints (see section 5.3).

## 28.4 Correctness of *CIncrease*

*CIncrease* does not change *status* or *pdAuth*, does not log, and no relevant message is emitted to the *ether*, so lemma ‘constraint’ (section C.6) is applicable.

■ 28.4

## 28.5 Correctness of *CAbort*

Lemma ‘constraint’ is not applicable, because *CAbort* moves one purse into *eaFrom*, and it may not have been in this state before, and it may log a pending transaction. Therefore we have to show that our chosen *BetweenWorld*’ obeys the constraints.

One  $\perp$  message is emitted, and (possibly) one log is recorded.

B-1 *req*  $\Rightarrow$  authentic to purse. No new *req* messages.

B-2 No future *reqs*. No new *req* messages.

B-3 No future *vals*. No new *val* messages.

B-4 No future *acks*. No new *ack* messages.

B-5 No future *from* logs. The purse moves into *eaFrom*, possibly logging a transaction, and possibly increasing *nextSeqNo*. This does not invalidate this constraint for any previous logs. To create a new *from* log, the purse would have had to have been in *epa* (from *LogIfNecessary*). Hence, using *ConPurse* constraint P-??, we have

$$pdAuth.fromSeqNo < nextSeqNo$$

From *AbortPurse*, we also have

$$nextSeqNo \leq nextSeqNo'$$

This gives

$$pdAuth.fromSeqNo < nextSeqNo'$$

The *pdAuth* is logged when the pre-state purse is in *epa*, and thus the new log obeys the constraint.

B-6 No future *to* logs. The purse moves into *eaFrom*, possibly logging a transaction, and possibly increasing *nextSeqNo*. This does not invalidate this constraint for any previous logs. To create a new *to* log, the purse would

have had to have been in  $epv$  (from *LogIfNecessary*). Hence, using *ConPurse* constraint P-??, we have

$$pdAuth.toSeqNo < nextSeqNo$$

From *AbortPurse*, we also have

$$nextSeqNo \leq nextSeqNo'$$

This gives

$$pdAuth.toSeqNo < nextSeqNo'$$

The  $pdAuth$  is logged when the pre-state purse is in  $epv$ , and thus the new log obeys the constraint.

B-7  $from$  in  $\{epr, epa\}$ , so no future  $from$  logs. The purse moves into  $eaFrom$ , so no new purses in  $epr$  or  $epa$ .

B-8  $to$  in  $\{epv, eaTo\}$ , so no future  $to$  logs. The purse moves into  $eaFrom$ , so no new purses in  $epv$  or  $eaTo$ .

B-9  $epr \Rightarrow \neg val \wedge \neg ack$ . The purse moves into  $eaFrom$ , and so does not move into  $epr$ .

B-10  $req \wedge \neg ack \Leftrightarrow toInEpv \vee toLogged$ .

- case  $\Rightarrow$ :  
No new  $req$  messages; no  $ack$  messages removed from the  $ether$ .  
The purse may have moved out of  $epv$ , but in such a case *LogIfNecessary* says that it logs, hence re-establishing the condition.
- case  $\Leftarrow$ :  
No purses newly in  $epv$ .  
There might be a new  $to$  log, in which case we must show there was a  $req$ , but no  $ack$  before. A  $to$  log can be made only by a purse moving out of  $epv$ . Then the *BetweenWorld* constraint B-10, on  $toInEpv$ , before the operation gives us the required  $req$  and lack of  $ack$ .

B-11  $epv \wedge val \Rightarrow fromInEpa \vee fromLogged$ . No purses newly in  $epv$ ; no new  $val$  messages.

The purse may have moved out of  $epa$ . But in such a case *LogIfNecessary* says that it logs, hence re-establishing the condition.

B-12  $fromInEpa \vee fromLogged \Rightarrow req$ . No purses newly in  $epa$ .

There might be a new  $from$  log, in which case we must show there was a  $req$  before. A  $from$  log can be made only by a purse moving out of

$epa$ . Then the *BetweenWorld* constraint B-12, on  $fromInEpa$ , before the operation gives us the required  $req$ .

B-13  $toLogged$  finite. At most one  $to$  log written, so finite before gives finite after.

B-14  $exceptionLogResults$  in  $allLogs$ . No new exception log result messages.

B-15 Cleared logs archived. No  $exceptionLogClear$  messages are added, and the archive is unchanged.

B-16  $req$  for each log. If there are no new logs, then the constraint holds from the pre-state.

If a transaction exception is logged, then the purse status must have been either  $epv$  or  $epa$ . From constraints B-10 and B-12, there was a  $req$  in the pre-state  $ether$  for the transaction which was logged. This  $req$  will also be in the post-state  $ether$ .

■ 28.5

## 28.6 Lemma 'logs unchanged'

**Lemma 28.2** (logs unchanged) When the *archive* and the individual purse logs do not change, and when no new  $req$  messages are added to the  $ether$ , the set of *PayDetails* representing all the logs does not change either.

$$\begin{aligned} BOpOkay \mid archive' &= archive \\ \wedge req \triangleright ether' &= req \triangleright ether \\ \wedge \forall n : \text{dom } conAuthPurse &\bullet \\ & (conAuthPurse' n).exLog = (conAuthPurse n).exLog \end{aligned}$$

⊢

$$\begin{aligned} allLogs' &= allLogs \\ \wedge toLogged' &= toLogged \\ \wedge fromLogged' &= fromLogged \end{aligned}$$

■

**Proof:**

$$\begin{aligned}
\text{allLogs} &= \text{archive} \\
&\quad \cup \{ n : \text{dom } \text{conAuthPurse}; ld : \text{PayDetails} \mid \\
&\quad \quad ld \in (\text{conAuthPurse } n).\text{exLog} \} \\
& \hspace{15em} [\text{defn}] \\
&= \text{archive}' \\
&\quad \cup \{ n : \text{dom } \text{conAuthPurse}'; ld : \text{PayDetails} \mid \\
&\quad \quad ld \in (\text{conAuthPurse}' n).\text{exLog} \} \\
& \hspace{15em} [\text{assumption and } \Phi BOp] \\
&= \text{allLogs}' \\
& \hspace{15em} [\text{defn}] \\
\text{allLogs} &= \{ n : \text{dom } \text{conAuthPurse}; pd : \text{PayDetails} \mid \\
&\quad n \mapsto pd \in \text{allLogs} \wedge \text{req } pd \in \text{ether} \} \\
& \hspace{15em} [\text{defn}] \\
&= \{ n : \text{dom } \text{conAuthPurse}'; pd : \text{PayDetails} \mid \\
&\quad n \mapsto pd \in \text{allLogs}' \wedge \text{req } pd \in \text{ether}' \} \\
& \hspace{15em} [\text{assumption and above}] \\
&= \text{allLogs}' \\
& \hspace{15em} [\text{defn}]
\end{aligned}$$

The arguments for *toLogged* and *fromLogged* follow in exactly the same way.

■ 28.6

### 28.7 Lemma ‘abort forward’: operations that first abort

Some concrete operations are written as a composition of *Abort* and a simpler operation starting from *eaFrom* (*StartFrom*, *StartTo*, *ReadExceptionLog*, *ClearExceptionLog*, etc.).

**Lemma 28.3** (abort forward) Where a *C* operation is written as a composition of *CAbort* and a simpler operation starting from *eaFrom*, and the corresponding *B* operation is structured analogously, it is sufficient to prove that the simpler *C* operation refines the corresponding *B* operation.

$$\begin{aligned}
&(\text{CAbort} \circlearrowleft \text{COpEafrom}); \text{Rbc}; \\
&\quad (\forall \text{COpEafrom}'; \text{Rbc} \bullet \exists \text{BetweenWorld}' \bullet \text{Rbc}' \wedge \text{BOPeafrom}) \\
&\vdash \\
&\quad \exists \text{BetweenWorld}' \bullet \text{Rbc}' \wedge (\text{Abort} \circlearrowleft \text{BOPeafrom})
\end{aligned}$$

■

**Proof** We have already proved in section 28.5 that *CAbort* refines *Abort*. Adding this to our hypothesis, we get

$$\begin{aligned}
&(\text{CAbort} \circlearrowleft \text{COpEafrom}); \text{Rbc}; \\
&\quad (\forall \text{CAbort}; \text{Rbc} \bullet \exists \text{BetweenWorld}' \bullet \text{Rbc}' \wedge \text{Abort}); \\
&\quad (\forall \text{COpEafrom}; \text{Rbc} \bullet \exists \text{BetweenWorld}' \bullet \text{Rbc}' \wedge \text{BOPeafrom}) \\
&\vdash \\
&\quad \exists \text{BetweenWorld}' \bullet \text{Rbc}' \wedge (\text{Abort} \circlearrowleft \text{BOPeafrom})
\end{aligned}$$

The hypothesis is now in precisely the form required to use lemma ‘compose forward’, (section C.10) and we do so to prove the consequent.

■ 28.7

## Correctness proofs

### 29.1 Introduction

Many of the following arguments are about constraints of the form

$$\textit{antecedent} \Rightarrow \textit{consequent}$$

The correctness arguments are of three kinds:

- B-1 Argue that the operation leaves the truth values of both antecedent and consequent unaltered, so that the truth before the operation establishes the truth afterwards.
- B-2 The operation might make the antecedent true after when it was false before, by adding a new message to a set, or moving a purse into a set. In this case it is necessary to show that the consequent is true after.
- B-3 The operation might make the consequent false after when it was true before, by moving a purse out of a set. In this case it is necessary to show that the antecedent is false after.

Note that we do not need to argue that a constraint cannot be changed by *removing* a message: messages stay in the *ether* once there.

### 29.2 Correctness of *CStartFrom*

*StartFromOkay* comprises *AbortPurse* followed by *StartFromEafromPurseOkay* at the unpromoted level. As a result, we can apply lemma 'abort forward' (section C.8), leaving us to prove the correctness of *StartFromEafromPurseOkay*.



Lemma 'constraint' is not applicable, because *StartFromEafromPurseOkay* changes status: it moves the purse from *eaFrom* into *epr*. Therefore we have to show that our chosen *BetweenWorld'* obeys the constraints.

One  $\perp$  message is emitted, and no logs are recorded.

We can invoke lemma 'logs unchanged', section C.7, because no new *req* messages are produced, no new purse logs are produced, and the *archive* does not change. Therefore, the sets *allLogs*, *fromLogged* and *toLogged* remain unchanged.

B-1 *req*  $\Rightarrow$  authentic to purse. No new *req* messages.

B-2 No future *reqs*. No new *req* messages.

B-3 No future *vals*. No new *val* messages.

B-4 No future *acks*. No new *ack* messages.

B-5 No future *from* logs. No new logs.

B-6 No future *to* logs. No new logs.

B-7 *from* in  $\{epr, epa\} \Rightarrow$  no future *from* logs. There are no new logs, but the purse moves into *epr*, so we must prove that the constraint for this purse holds (for all other purses in *epr*, the constraint holds beforehand, and so holds afterwards). In *StartFrom*, the post-state *pdAuth'.fromSeqNo* is equal to pre-state *nextSeqNo*. Coupling this with constraint B-5 we have

$$\forall pd : fromLogged \mid pd.from = name? \bullet \\ pd.fromSeqNo < (conAuthPurse' pd.from).pdAuth.fromSeqNo$$

Since the logs don't change we have

$$\forall pd : fromLogged' \mid pd.from = name? \bullet \\ pd.fromSeqNo < (conAuthPurse' pd.from).pdAuth.fromSeqNo$$

which proves the constraint for purse *name?*.

B-8 *to* in  $\{epv, eaTo\} \Rightarrow$  no future *to* logs. No new logs, and the purse moves into *epr*.

B-9 *epr*  $\Rightarrow \neg val \wedge \neg ack$ . The purse moves into *epr*, so it is necessary to show there was no *val* or *ack* before.

The *pd* we are considering is given by

$$pd == (conAuthPurse' name?).pdAuth$$

Noting that *pd.from = name?*, the definition of *StartFrom* then gives us that

$$\begin{aligned} & (conAuthPurse name?).nextSeqNo \\ & = (conAuthPurse' name?).pdAuth.fromSeqNo \\ \Rightarrow & (conAuthPurse pd.from).nextSeqNo = pd.fromSeqNo \\ \Rightarrow & val pd \notin ether \quad [BetweenWorld \text{ constraint B-3}] \\ & \wedge ack pd \notin ether \quad [BetweenWorld \text{ constraint B-4}] \end{aligned}$$

B-10 *req*  $\wedge \neg ack \Leftrightarrow toInEpv \vee toLogged$ .

• case  $\Rightarrow$ :

No new *req* messages. The purse moved from *eaFrom* to *epr* without generating new logs. Hence, true before implies true after.

• case  $\Leftarrow$ :

No purses newly in *epv* and no new logs. No *acks* added to the *ether*.

B-11 *epv*  $\wedge val \Rightarrow fromInEpa \vee fromLogged$ . No purses newly in *epv*; no new *val* messages. The purse did not move out of *epa*.

B-12 *fromInEpa*  $\vee fromLogged \Rightarrow req$ . No purses newly in *epa*; no new logs.

B-13 *toLogged* finite. No new logs.

B-14 *exceptionLogResults* in *allLogs*. No new log result messages.

B-15 Cleared logs archived. No new *exceptionLogClear* messages.

B-16 *req* for each log. No new elements added to *fromLogged* or *toLogged*.

■ 29.2

### 29.3 Correctness of CStartTo

*StartToOkay* is composed of *AbortPurse* followed by *StartToEafromPurseOkay* at the unpromoted level. As a result, we can apply lemma 'abort forward' (section C.8), leaving us to prove the correctness of *StartToEafromPurseOkay*.

Lemma 'constraint' is not applicable, because *StartToEafromPurseOkay* moves one purse into *epv*, and it was not in this state before. Therefore we have to show that our chosen *BetweenWorld'* obeys the constraints.

One *req* message is emitted, and no new logs are recorded. We cannot invoke lemma 'logs unchanged' because we do have a new *req* message, but constraint B-16 gives us the same result. This is not a circular argument.

- B-1  $req \Rightarrow$  authentic  $to$  purse. One new  $req$ , which refers to the  $name?$  purse as the  $to$  purse.  $\Phi BOp$  states that this purse is authentic.
- B-2 No future  $reqs$ .  $StartToPurseEafromOkay$  emits one  $req$  message, which has its  $nextSeqNo$  in it by construction. It also increases  $nextSeqNo$ . The  $req$  message meets the constraints because the referenced  $to$  purse (itself) has a larger  $nextSeqNo$  after the operation.
- B-3 No future  $vals$ . No new  $val$  messages.
- B-4 No future  $acks$ . No new  $ack$  messages.
- B-5 No future  $from$  logs. No new logs.
- B-6 No future  $to$  logs. No new logs.
- B-7  $from$  in  $\{epr, epa\} \Rightarrow$  no future  $from$  logs. There are no new logs and the purse moves into  $epv$ , so this constraint does not apply to this purse.
- B-8  $to$  in  $\{epv, eaTo\} \Rightarrow$  no future  $to$  logs. There are no new logs, but the purse moves into  $epv$ , so we must prove that the constraint for this purse holds (for all other purses in  $epv$ , the constraint holds beforehand, and so holds afterwards). In  $StartTo$ , the post-state  $pdAuth'.toSeqNo$  is equal to pre-state  $nextSeqNo$ . Coupling this with constraint B-6 we have

$$\forall pd : toLogged \mid pd.to = name? \bullet \\ pd.toSeqNo < (conAuthPurse' pd.to).pdAuth.toSeqNo$$

Since the logs don't change, we have

$$\forall pd : toLogged' \mid pd.to = name? \bullet \\ pd.toSeqNo < (conAuthPurse' pd.to).pdAuth.toSeqNo$$

which proves the constraint for purse  $name?$ .

- B-9  $epr \Rightarrow \neg val \wedge \neg ack$ . No purses newly in  $epr$ ; no new  $vals$  or  $acks$ .
- B-10  $req \wedge \neg ack \Leftrightarrow toInEpv \vee toLogged$ . We claim that there is a new  $req$  for which there is no  $ack$  in the ether, and the purse moves into  $epv$ . As a result, we prove the consequent for each implication direction.
- case  $\Rightarrow$ :  
We must prove  $toInEpv \vee toLogged$ . The purse moves into  $epv$ , thus establishing the consequent.
  - case  $\Leftarrow$ :  
The purse moves into  $epv$ , so we must show that there is a  $req$ , but no  $ack$ , for the purse's  $pdAuth'$ . From  $StartTo$ , we have  $m! = req\ pdAuth'$ ,

so the  $req$  is in the ether. It is then necessary to show there is no  $ack$  before. The  $pd$  we are considering is given by

$$pd == (conAuthPurse' name?).pdAuth$$

Noting that  $pd.to = name?$ , the definition of  $StartTo$  gives us that

$$\begin{aligned} & (conAuthPurse\ name?).nextSeqNo \\ & = (conAuthPurse' name?).pdAuth.toSeqNo \\ & \Rightarrow (conAuthPurse\ pd.to).nextSeqNo = pd.toSeqNo \\ & \Rightarrow ack\ pd \notin ether \quad [BetweenWorld\ constraint\ B-4] \end{aligned}$$

Hence, we have the corresponding  $req$  but no  $ack$ .

- B-11  $epv \wedge val \Rightarrow fromInEpa \vee fromLogged$ . To prove this constraint, we demonstrate that the antecedent is false: the purse moves into  $epv$ , so we must show that there is no  $val$  before. The  $pd$  we are considering is given by

$$pd == (conAuthPurse' name?).pdAuth$$

Noting that  $pd.to = name?$ , the definition of  $StartTo$  gives us that

$$\begin{aligned} & (conAuthPurse\ name?).nextSeqNo \\ & = (conAuthPurse' name?).pdAuth.toSeqNo \\ & \Rightarrow (conAuthPurse\ pd.to).nextSeqNo = pd.toSeqNo \\ & \Rightarrow val\ pd \notin ether \quad [BetweenWorld\ constraint\ B-3] \end{aligned}$$

Hence, there is no  $val$  before, and no  $val$  is emitted by this operation.

- B-12  $fromInEpa \vee fromLogged \Rightarrow req$ . No purses newly in  $epa$ ; no new logs.
- B-13  $toLogged$  finite. No new logs.
- B-14 Read exception record messages are logged. No new log result messages.
- B-15 Cleared logs archived. No new  $exceptionLogClear$  messages.
- B-16  $req$  for each log. No new elements added to  $fromLogged$  or  $toLogged$ .

■ 29.3

### 29.4 Correctness of $CReq$

Lemma ‘constraint’ is not applicable, because a purse moves from  $epr$  to  $epa$  and emits a  $val$  message. Therefore we have to show that our chosen *BetweenWorld* obeys the constraints.

We can invoke lemma ‘logs unchanged’, section C.7, because no new  $req$  messages are produced, no new purse logs are produced, and the *archive* does not change. Therefore, the sets *allLogs*, *fromLogged* and *toLogged* remain unchanged.

B-1  $req \Rightarrow$  authentic to purse. No new  $req$  messages.

B-2 No future  $reqs$ . No new  $req$  messages.

B-3 No future  $vals$ .  $Req$  puts a  $val$  in the *ether*. Let  $pd$  be the pay details of the  $val$ . Hence,

$$\begin{aligned} pd &== (conAuthPurse\ name?).pdAuth \\ m? &= req\ pd \\ m! &= val\ pd \end{aligned}$$

To show that the new  $val$  message upholds this constraint, we have to demonstrate that this is not a future message with respect to purse  $name?$ :

$$\begin{aligned} pd.toSeqNo &< (conAuthPurse'\ pd.to).nextSeqNo \\ pd.fromSeqNo &< (conAuthPurse'\ pd.from).nextSeqNo \end{aligned}$$

Since  $req\ pd$  is in the ether, from B-2 we can then satisfy the requirement for the  $to$  sequence number. Since the pre-state *status* was  $epr$ , using purse constraint P-2c we know that

$$pd.fromSeqNo < nextSeqNo$$

Since  $Req$  does not alter  $nextSeqNo$ , we thus have

$$pd.fromSeqNo < (conAuthPurse'\ pd.from).nextSeqNo$$

B-4 No future  $acks$ . No new  $ack$  messages.

B-5 No future  $from$  logs. No new logs.

B-6 No future  $to$  logs. No new logs.

B-7  $from$  in  $\{epr, epa\} \Rightarrow$  no future  $from$  logs. No new logs.

The  $from$  purse moves from  $epr$  into  $epa$ . *BetweenWorld* constraint B-7 held on  $epr$ .

B-8  $to$  in  $\{epv, eaTo\} \Rightarrow$  no future  $to$  logs. No new logs; no purses newly in  $epv$  or  $eaTo$ .

B-9  $epr \Rightarrow \neg val \wedge \neg ack$ . No purses newly in  $epr$ ; no new  $acks$ .

We need to show the emitted  $val$  does not have the same  $pd$  as the stored  $pdAuth$  of any purse currently in  $epr$ . It has the same  $pd$  as the  $pdAuth$  stored in the purse from which it was emitted, which moved from  $epr$  and is now in  $epa$ . No other purse can also have this  $pdAuth$ , because  $pdAuth$  includes the *name* of the purse (*ConPurse* constraint P-2a), and purse names are unique.

B-10  $req \wedge \neg ack \Leftrightarrow toInEpv \vee toLogged$ .

- case  $\Rightarrow$ : No new  $req$  or  $ack$  messages.
- case  $\Leftarrow$ : No purses newly in  $epv$ ; no new logs.

B-11  $epv \wedge val \Rightarrow fromInEpa \vee fromLogged$ . The  $from$  purse emits a  $val$ . It also moves into  $epa$ , thereby establishing the constraint.

B-12  $fromInEpa \vee fromLogged \Rightarrow req$ . The purse moves into  $epa$ . The operation precondition gives the presence of the required  $req$ .

B-13  $toLogged$  finite. No new logs.

B-14 Read exception record messages are logged. No new log result messages.

B-15 Cleared logs archived. No new *exceptionLogClear* messages.

B-16  $req$  for each log. No new elements added to *fromLogged* or *toLogged*.

■ 29.4

### 29.5 Correctness of $CVal$

Lemma ‘constraint’ is not applicable, because a purse moves from  $epv$  to  $eaPayee$  and emits an  $ack$  message. Therefore we have to show that our chosen *BetweenWorld* obeys the constraints.

We can invoke lemma ‘logs unchanged’, section C.7, because no new  $req$  messages are produced, no new purse logs are produced, and the *archive* does not change. Therefore, the sets *allLogs*, *fromLogged* and *toLogged* remain unchanged.

B-1  $req \Rightarrow$  authentic to purse. No new  $req$  messages.

B-2 No future  $reqs$ .  $Val$  emits no new  $req$  messages.

B-3 No future  $vals$ .  $Val$  emits no new  $val$  messages.

- B-4 No future *acks*. *ValOkay* puts an *ack* in the *ether'*, but it has the same *pd* as the *val* read from the *ether*, which obeys *BetweenWorld* constraint B-3. So the *ack's pd* obeys the constraint.
- B-5 No future *from* logs. No new logs.
- B-6 No future *to* logs. No new logs.
- B-7 *from* in  $\{epr, epa\} \Rightarrow$  no future *from* logs. No new logs; no purses newly in *epr* or *epa*.
- B-8 *to* in  $\{epv, eaTo\} \Rightarrow$  no future *to* logs. No new logs.  
The *to* purse moves from *epv* into *eaTo*. *BetweenWorld* constraint B-8 held on *epv*.
- B-9  $epr \Rightarrow \neg val \wedge \neg ack$ . No purses newly in *epr*.  
We need to show the emitted *ack* does not have the same *pd* as any purse currently in *epr*. It has the same *pd* as the *val* message, and so *BetweenWorld* constraint B-9 on *val* gives us the required condition.
- B-10  $req \wedge \neg ack \Leftrightarrow toInEpv \vee toLogged$ .
- case  $\Rightarrow$ : *ValOkay* emits an *ack*, making the antecedent false.
  - case  $\Leftarrow$ : From lemma 'notLoggedAndIn', section C.12, the purse cannot be in *toLogged*. *ValOkay* moves the purse out of *epv* without logging, making the antecedent false.
- B-11  $epv \wedge val \Rightarrow fromInEpa \vee fromLogged$ . No purses newly in *epv*; no new *val* messages; no purses leaving *epa*, no changing logs.
- B-12  $fromInEpa \vee fromLogged \Rightarrow req$ . No purses newly in *epa*; no new logs.
- B-13 *toLogged* finite. No new logs.
- B-14 Read exception record messages are logged. No new log result messages.
- B-15 Cleared logs archived. No new *exceptionLogClear* messages.
- B-16 *req* for each log. No new elements added to *fromLogged* or *toLogged*.

■ 29.5

## 29.6 Correctness of *Cack*

Lemma 'constraint' is not applicable, because a purse moves from *epa* to *eaPayer*. Therefore we have to show that our chosen *BetweenWorld'* obeys the constraints.

It emits a  $\perp$  message. We can invoke lemma 'logs unchanged', section C.7, because no new *req* messages are produced, no new purse logs are produced,

and the *archive* does not change. Therefore, the sets *allLogs*, *fromLogged* and *toLogged* remain unchanged.

- B-1 *req*  $\Rightarrow$  authentic *to* purse. No new *req* messages.
- B-2 No future *reqs*. No new *req* messages.
- B-3 No future *vals*. No new *val* messages.
- B-4 No future *acks*. No new *ack* messages.
- B-5 No future *from* logs. No new logs.
- B-6 No future *to* logs. No new logs.
- B-7 *from* in  $\{epr, epa\} \Rightarrow$  no future *from* logs. No purses newly in *epr* or *epa*.
- B-8 *to* in  $\{epv, eaTo\} \Rightarrow$  no future *to* logs. No purses newly in *epv* or *eaTo*.
- B-9  $epr \Rightarrow \neg val \wedge \neg ack$ . No purses newly in *epr*; no new *vals* or *acks*.
- B-10  $req \wedge \neg ack \Leftrightarrow toInEpv \vee toLogged$ .
- case  $\Rightarrow$ : No new *reqs*; no new *acks*; no purses moving out of *epv*, no logs lost.
  - case  $\Leftarrow$ : No purses newly in *epv*; no new logs.
- B-11  $epv \wedge val \Rightarrow fromInEpa \vee fromLogged$ . No purses newly in *epv*; no new *vals*.  
The purse moves out of *epa* without logging, so we need to show that the antecedent is false for this purse. It is sufficient to show the antecedent is false before the operation (since the operation does not change it). There is an *ack* message, *AckOkay's* input, so *BetweenWorld* constraint B-10 gives us  $pd \notin toInEpv$ .
- B-12  $fromInEpa \vee fromLogged \Rightarrow req$ . No purses newly in *epa*; no new logs.
- B-13 *toLogged* finite. No new logs.
- B-14 Read exception record messages are logged. No new log result messages.
- B-15 Cleared logs archived. No new *exceptionLogClear* messages.
- B-16 *req* for each log. No new elements added to *fromLogged* or *toLogged*.

■ 29.6

### 29.7 Correctness of *CReadExceptionLog*

*ReadExceptionLogOkay* is composed of *AbortPurse* followed by *ReadExceptionLogEafromPurseOkay* at the unpromoted level. As a result, we can apply lemma ‘abort forward’ (section C.8), leaving us to prove the correctness of *ReadExceptionLogEafromPurseOkay*.

This operation does not change any purse, but it does emit an *exceptionLogResult* message. As a result, lemma ‘constraint’ is not applicable.

We can invoke lemma ‘logs unchanged’, section C.7, because no new *req* messages are produced, no new purse logs are produced, and the *archive* does not change. Therefore, the sets *allLogs*, *fromLogged* and *toLogged* remain unchanged.

- B-1 *req*  $\Rightarrow$  authentic *to* purse. No new *req* messages.
- B-2 No future *reqs*. No new *req* messages.
- B-3 No future *vals*. No new *val* messages.
- B-4 No future *acks*. No new *ack* messages.
- B-5 No future *from* logs. No new logs.
- B-6 No future *to* logs. No new logs.
- B-7 *from* in  $\{epr, epa\} \Rightarrow$  no future *from* logs. No purses newly in *epr* or *epa*.
- B-8 *to* in  $\{epv, eaTo\} \Rightarrow$  no future *to* logs. No purses newly in *epv* or *eaTo*.
- B-9 *epr*  $\Rightarrow \neg val \wedge \neg ack$ . No purses newly in *epr*; no new *vals* or *acks*.
- B-10  $req \wedge \neg ack \Leftrightarrow toInEpv \vee toLogged$ .
  - case  $\Rightarrow$ : No new *reqs*; no new *acks*; no purses moving out of *epv*, no logs lost.
  - case  $\Leftarrow$ : No purses newly in *epv*; no new logs.
- B-11  $epv \wedge val \Rightarrow fromInEpa \vee fromLogged$ . No purses newly in *epv*; no new *vals*; no purse moves out of *epa*; no logs lost.
- B-12  $fromInEpa \vee fromLogged \Rightarrow req$ . No purses newly in *epa*; no new logs.
- B-13 *toLogged* finite. No new logs.
- B-14 Read exception record messages are logged. There may be a new *exceptionLogResult* message. If this is so, then we must show that this refers to a stored exception log record. From *ReadExceptionLogPurseEafromOkay*, we have

$$m! \in \{\perp\} \cup \{ld : exLog' \bullet exceptionLogResult(name, ld)\}$$

Hence, if there is an *exceptionLogResult* message, it refers to an exception record which is in the log of purse *name?*, and so is in *allLogs*'. This upholds the constraint.

B-15 Cleared logs archived. No new *exceptionLogClear* messages.

B-16 *req* for each log. No new elements added to *fromLogged* or *toLogged*.

■ 29.7

### 29.8 Correctness of *CClearExceptionLog*

*ClearExceptionLogOkay* is composed of *AbortPurse* followed by *ClearExceptionLogEafromPurseOkay* at the unpromoted level. As a result, we can apply lemma ‘abort forward’ (section C.8), leaving us to prove the correctness of *ClearExceptionLogEafromPurseOkay*.

The operation changes only one purse, and emits a  $\perp$  message. The only change to the purse is that its exception log is cleared. However, we have the pre-condition that the input message matches the the exception log (*exLog*). The input message comes from the ether, and hence from constraint B-15 we know that the purse’s exception log must have already been recorded in the archive. In this way, clearing the purse’s log does not affect *allLogs*. So lemma ‘constraint’ (section C.6) is applicable.

■ 29.8

### 29.9 Correctness of *CAuthoriseExLogClear*

Lemma ‘constraint’ is not applicable, because an *exceptionLogClear* message is emitted to the ether. So, we must show that the constraints hold afterwards.

No purses are changed.

We can invoke lemma ‘logs unchanged’, section C.7, because no new *req* messages are produced, no new purse logs are produced, and the *archive* does not change. Therefore, the sets *allLogs*, *fromLogged* and *toLogged* remain unchanged.

- B-1 *req*  $\Rightarrow$  authentic *to* purse. No new *req* messages.
- B-2 No future *reqs*. No new *req* messages.
- B-3 No future *vals*. No new *val* messages.
- B-4 No future *acks*. No new *ack* messages.
- B-5 No future *from* logs. No new logs.

- B-6 No future *to* logs. No new logs.
- B-7 *from* in  $\{epv, epa\} \Rightarrow$  no future *from* logs. No purses newly in *epv* or *epa*.
- B-8 *to* in  $\{epv, eaTo\} \Rightarrow$  no future *to* logs. No purses newly in *epv* or *eaTo*.
- B-9  $epv \Rightarrow \neg val \wedge \neg ack$ . No purses newly in *epv*; no new *vals* or *acks*.
- B-10  $req \wedge \neg ack \Leftrightarrow toInEpv \vee toLogged$ .
- case  $\Rightarrow$ : No new *reqs*; no new *acks*; no purses moving out of *epv*; no logs lost.
  - case  $\Leftarrow$ : No purses newly in *epv*; no new logs.
- B-11  $epv \wedge val \Rightarrow fromInEpa \vee fromLogged$ . No purses newly in *epv*; no new *vals*; no purse moves out of *epa*; no logs lost.
- B-12  $fromInEpa \vee fromLogged \Rightarrow req$ . No purses newly in *epa*; no new logs.
- B-13 *toLogged* finite. No new logs.
- B-14 Read exception record messages are logged. No new exception log read messages.
- B-15 Cleared logs archived. There is a new *exceptionLogClear* message. However, the operation contains the pre-condition that the log records for which the message is generated must be in the archive. Hence, the constraint is upheld.
- B-16 *req* for each log. No new elements added to *fromLogged* or *toLogged*.

### 29.10 Correctness of *CArchive*

This operation archives the contents of some of the *exceptionLogResult* messages in the ether. It does not change any purse, or change the ether.

From B-14, we know that those exception records referred to by the *exceptionLogResult* messages are already in *allLogs*. As a result, adding them to *archive* does not change *allLogs*. This operation does not change any purse, and does not emit a payment details message. So lemma ‘constraint’ is applicable.

- 29.10
- 29

---

## Summary

The proofs presented in this report constitute a proof that the architectural design given by the *C* model is *secure* with respect to the security properties as described in the Formal Security Policy Model (the *A* model) and the Security Properties.

We have presented the proofs in a logical sequence, but even so, it can be hard to be sure that no steps have been missed. The following table gives a hierarchical view of the proof, showing at each level how a proof goal is satisfied by a number of subgoals. Each line in the table is one proof goal, together with a section reference for where that proof goal is addressed.

If the proof goal has child goals (goals one level of indent deeper) then the section reference explains how it is that the goal can be satisfied by its collection of subgoals. For example, goal 1.4 (AbTransfer upholds properties) is proved by proving three subgoals: 1.4.1 (SP 1), 1.4.2 (SP 2.1) and 1.4.3 (SP 6.2). The reference for goal 1.4 is to section 2.4, where it is argued that we have only to prove the three SPs 1, 2.1 and 6.2 because all other SPs can be proved trivially.

If a goal has no further subgoals, its section reference is the proof of this goal directly.

It can be seen that all proof goals have section references, and all steps have been addressed.

System secure	by definition
1. Abstract preserves security properties	by definition
1.1. AbIgnore upholds properties	2.4
1.2. AbTransfer upholds properties	2.4
1.2.1. SP 1	2.4
1.2.1.1. Okay	2.4.1
1.2.1.2. Lost	2.4.3
1.2.2. SP 2.1	2.4
1.2.2.1. Okay	2.4.2
1.2.2.2. Lost	2.4.4
2. Concrete preserves security properties	by definition
2.1. Each concrete operation upholds properties	2.4
3. Abstract operations are total	8.2.2
4. A is refined by B	by definition
4.1. Init	by definition
4.1.1. state initialisation	11.2
4.1.2. input initialisation	11.3
4.2. Applicability	9.2.3
4.2.1. pre AOp = true	8.2.2
4.2.2. simpler applicability	by definition
4.2.2.1. pre BOp = true	8.3.2
4.3. Correctness	9.2.4
4.3.1. pre AOp = true	8.2.2
4.3.2. simpler correctness	by definition
4.3.2.1. AbTransfer	9 and 14.3
4.3.2.1.1. Ignore	14.7
4.3.2.1.2. Okay and Lost	C.1
4.3.2.1.2.1. exists-pd	18.4
4.3.2.1.2.2. exists-chosenLost	18.5
4.3.2.1.2.3. check-operation	18.6
4.3.2.2. AbIgnore	9 and 14.2
4.3.2.2.1. StartFrom	14.3
4.3.2.2.1.1. Ignore	14.7
4.3.2.2.1.2. Abort	14.8
4.3.2.2.1.3. Okay	C.5
4.3.2.2.1.3.1. Abort	14.8

4.3.2.2.1.3.2. EaPayer operation	C.1
4.3.2.2.1.3.2.1. exists-pd	16.4
4.3.2.2.1.3.2.2. exists-chosenLost	16.5
4.3.2.2.1.3.2.3. check-operation	C.3
4.3.2.2.1.3.2.3.1. check-operation-ignore	16.6
4.3.2.2.2. StartTo	14.3
4.3.2.2.2.1. Ignore	14.7
4.3.2.2.2.2. Abort	14.8
4.3.2.2.2.3. Okay	C.5
4.3.2.2.2.3.1. Abort	14.8
4.3.2.2.2.3.2. EaPayer operation	C.1
4.3.2.2.2.3.2.1. exists-pd	17.4
4.3.2.2.2.3.2.2. exists-chosenLost	17.5
4.3.2.2.2.3.2.3. check-operation	C.3
4.3.2.2.2.3.2.3.1. check-operation-ignore	17.6
4.3.2.2.3. Val	14.3
4.3.2.2.3.1. Ignore	14.7
4.3.2.2.3.2. Okay	C.1 and 19.2
4.3.2.2.3.2.1. exists-pd	19.3
4.3.2.2.3.2.2. exists-chosenLost	19.4
4.3.2.2.3.2.3. check-operation	C.3
4.3.2.2.3.2.3.1. check-operation-ignore	19.5 and on
4.3.2.2.4. Ack	14.3
4.3.2.2.4.1. Ignore	14.7
4.3.2.2.4.2. Okay	C.1 and 20.2
4.3.2.2.4.2.1. exists-pd	20.3
4.3.2.2.4.2.2. exists-chosenLost	20.4
4.3.2.2.4.2.3. check-operation	C.3
4.3.2.2.4.2.3.1. check-operation-ignore	20.5 and on

4.3.2.2.5.	ReadExceptionLog	14.3
4.3.2.2.5.1.	Ignore	14.7
4.3.2.2.5.2.	Okay	C.5
4.3.2.2.5.2.1.	Abort	14.8
4.3.2.2.5.2.2.	EaPayer operation	C.1 and 21
4.3.2.2.5.2.2.1.	lemma lost unchanged	C.2
4.3.2.2.5.2.2.2.	check-operation	C.3
4.3.2.2.5.2.2.2.1.	check-operation-ignore	21.3
4.3.2.2.6.	ClearExceptionLog	14.3
4.3.2.2.6.1.	Ignore	14.7
4.3.2.2.6.2.	Abort	14.8
4.3.2.2.6.3.	Okay	C.5
4.3.2.2.6.3.1.	Abort	14.8
4.3.2.2.6.3.2.	EaPayer operation	C.1 and 22
4.3.2.2.6.3.2.1.	lemma lost unchanged	C.2
4.3.2.2.6.3.2.2.	check-operation	C.3
4.3.2.2.6.3.2.2.1.	check-operation-ignore	22.3
4.3.2.2.7.	AuthoriseExLogClear	14.3
4.3.2.2.7.1.	Ignore	14.7
4.3.2.2.7.2.	Okay	23.2
4.3.2.2.8.	Archive	24.2
4.3.2.2.9.	Ignore	14.7
4.3.2.2.10.	Increase	15.3
4.3.2.2.11.	Abort	14.8
4.4.	Finalisation	by definition
4.4.1.	output finalisation	12.2
4.4.2.	state finalisation	12.3
5.	B is refined by C	established rules 25.2
5.1.	Init	27.1
5.2.	Applicability	27.3
5.2.1.	pre COP = true	8.4.2
5.3.	Correctness	25.2.5
5.3.1.	Simpler correctness	25
5.3.1.1.	StartTo is refined	28.1
5.3.1.1.1.	Okay branch	29.3 and C.10
5.3.1.1.1.1.	Eafrom branch	29.3
5.3.1.1.1.2.	Abort branch	28.5

5.3.1.1.2.	Cignore branch	28.2
5.3.1.1.3.	CAbort branch	28.5
5.3.1.2.	StartFrom is refined	28.1
5.3.1.2.1.	Okay branch	29.2 and C.10
5.3.1.2.1.1.	Eafrom branch	29.2
5.3.1.2.1.2.	Abort branch	28.5
5.3.1.2.2.	Cignore branch	28.2
5.3.1.2.3.	CAbort branch	28.5
5.3.1.3.	Req is refined	28.1
5.3.1.3.1.	Okay branch	29.4
5.3.1.3.2.	Cignore branch	28.2
5.3.1.4.	Val is refined	28.1
5.3.1.4.1.	Okay branch	29.5
5.3.1.4.2.	Cignore branch	28.2
5.3.1.5.	Ack is refined	28.1
5.3.1.5.1.	Okay branch	29.6
5.3.1.5.2.	Cignore branch	28.2
5.3.1.6.	ReadExceptionLog is refined	28.1
5.3.1.6.1.	Okay branch	29.7 and C.10
5.3.1.6.1.1.	Eafrom branch	29.7
5.3.1.6.1.2.	Abort branch	28.5
5.3.1.6.2.	Cignore branch	28.2
5.3.1.7.	ClearExceptionLog is refined	28.1
5.3.1.7.1.	Okay branch	29.8 and C.10
5.3.1.7.1.1.	Eafrom branch	29.8
5.3.1.7.1.2.	Abort branch	28.5
5.3.1.7.2.	Cignore branch	28.2
5.3.1.7.3.	CAbort branch	28.5
5.3.1.8.	AuthoriseExLogClear is refined	28.1
5.3.1.8.1.	Okay branch	29.9
5.3.1.8.2.	Cignore branch	28.2
5.3.1.9.	Archive is refined	29.10
5.3.2.	Totality of BOp	8.3.2
5.4.	Finalisation	27.2



**Part IV**  
**Appendices**

## Proof Layout

### A.1 Notation

The notation

$$Abs \sqsubseteq Conc$$

says the the *Abs* operation is refined by the *Conc* operation.

In order to prove that *Abs* is indeed validly refined by *Conc*, we need to prove various 'correctness conditions', expressed as theorems (section 9).

That the predicate

$$\forall D \mid P \bullet Q$$

is always true is expressed as the theorem

$$\vdash \forall D \mid P \bullet Q$$

which is equivalent to

$$D \mid P \vdash Q$$

This can be read as a theorem that states that, under hypothesis  $D \mid P$  (declarations  $D$  constrained by predicates  $P$ ), consequent  $Q$  (a predicate) has been proved to hold.  $D \mid P$  is usually written as a schema text, and  $Q$  may be written using a schema as predicate.

### A.2 Labelling proof steps

In labelling various steps of the proofs below, we use the following notation.

- [defn  $P$ ]: from the definition of the schema predicate  $P$
- [hyp]: from the hypothesis of the theorem
- [prop  $x$ ]: from a property of the  $Z$  operator  $x$
- [ $name$ ]: use of inference rule  $name$

---

## Inference rules

The proofs presented are rigorous, but informal, in that they have not been checked by a machine proof-checker.

We present below the sort of inference rules we have used. Such explicit use of inference rules improves the readability of the proofs by showing exactly what steps of mathematical reasoning are being made. These inference rules are not intended as a definition of the logic being used, but as guidance about the reasoning steps.

The inference rule

$$\frac{P_1 \quad P_2 \quad \dots \quad P_n}{C} \quad [ \text{rulename} ]$$

says that conclusion  $C$  can be inferred if every premiss  $P_i$  can be proved. (The rule name is used for labelling proof steps.)

The inference rule

$$\frac{P_1, P_2, \dots, P_n}{C} \quad [ \text{rulename} ]$$

says that conclusion  $C$  can be inferred if any premiss  $P_i$  can be proved.

### B.1 Universal quantifier becomes hypothesis

$$\frac{S \vdash P}{\vdash \forall S \bullet P} \quad [ \text{uni hyp} ]$$

**B.2 Disjunction in the hypothesis**

Given an hypothesis containing a disjunct, it is sufficient to prove the theorem for each case.

$$\frac{R \vdash P \quad S \vdash P}{R \vee S \vdash P} \quad [ \text{hyp disj} ]$$

**B.3 Disjunction in the consequent**

Given a consequent containing a disjunct, it is sufficient to prove the theorem for only one case (since this is a harder thing to prove).

$$\frac{R \vdash P, R \vdash Q}{R \vdash P \vee Q} \quad [ \text{consq disj} ]$$

**B.4 Conjunction in the consequent**

Given a consequent containing a conjunct, it is sufficient to prove the theorem for each case separately.

$$\frac{R \vdash P \quad R \vdash Q}{R \vdash P \wedge Q} \quad [ \text{consq conj} ]$$

We can add conjuncts to the consequent (since this is a harder thing to prove).

$$\frac{R \vdash P \wedge Q}{R \vdash P} \quad [ \text{strengthen consq} ]$$

**B.5 Cut for lemmas**

Cut is a way to introduce new hypotheses, and discharge them as lemmas.

$$\frac{R; D \mid Q \vdash P \quad R \vdash \exists D \bullet Q}{R \vdash P} \quad [ \text{cut} ]$$

**B.6 Thin**

We can remove assumptions.

$$\frac{\vdash R}{P \vdash R} \quad [ \text{thin} ]$$

**B.7 Universal Quantification**

Universals can be replaced by a particular choice in the hypothesis

$$\frac{x_1 \in X \Rightarrow P(x_1) \vdash R}{\forall x : X \bullet P(x) \vdash R} \quad [ \text{hyp uni} ]$$

**B.8 Negation**

In order to prove something, you can assume its negation.

$$\frac{\neg P \vdash}{\vdash P} \quad [ \text{negation} ]$$

**B.9 Contradiction**

If  $R$  can be proved, assuming its negation allows you to prove anything (because  $\text{false} \Rightarrow \text{anything}$ ).

$$\frac{\vdash R}{\neg R \vdash \text{anything}} \quad [ \text{contradiction} ]$$

**B.10 One Point Rule**

In order to prove there exists a value with a property, it is enough to exhibit such a value.

$$\frac{\vdash P[t/x]}{\vdash \exists x \bullet P \wedge x = t} \quad [ \text{one point} ]$$

provided  $x$  is not free in  $t$ .

### B.11 Derived Rules

We find it useful to derive some compound rules. These make the proofs in the body of the document easier to follow, and can themselves be proved from the inference rules above.

#### B.11.1 One point cut

$$\frac{P \vdash Q}{P \vdash \exists P \bullet Q} \quad [ \text{consq exists} ]$$

and very similarly

$$\frac{P \vdash Q}{P \vdash (\exists P) \wedge Q} \quad [ \text{consq exists} ]$$

#### B.11.2 Existential in the hypothesis

$$\frac{x : X; D \mid P \vdash}{D \mid \exists x : X \bullet P \vdash} \quad [ \text{hyp exists} ]$$

### B.12 Proof of the Derived Rules

We derive each of the derived rules above from the main inference rules.

#### B.12.1 Derivation of One point cut

We can derive the first one-point cut rule (*consq exists*) as follows. First, we expand  $P$  into a declaration  $D$  and a predicate  $p$ .

$$\begin{aligned} D \mid p \vdash \exists D \bullet p \wedge q & \quad [\text{starting point}] \\ D \mid p \vdash \exists D' \bullet p[D'/D] \wedge q[D'/D] & \quad [\text{rename bound declaration}] \\ D \mid p \vdash \exists D' \bullet p[D'/D] \wedge q[D'/D] \wedge D' = D & \quad [\text{strengthen consequent}] \\ D \mid p \vdash p[D'/D][D/D'] \wedge q[D'/D][D/D'] & \quad [\text{one point rule}] \\ D \mid p \vdash p \wedge q & \quad [\text{simplify renaming}] \\ D \mid p \vdash q & \quad [\text{discharge } p \text{ from hyp}] \end{aligned}$$

The second onepoint-cut rule follows exactly the same way, except that  $q$  is not bound by the existential, and so none of the renamings alters it.

#### B.12.2 Derivation of existential in the hypothesis

$$\begin{aligned} D \mid (\exists x : X \bullet P) \vdash & \quad [\text{starting point}] \\ D; x : X \mid P \wedge (\exists x : X \bullet P) \vdash \quad D \mid (\exists x : X \bullet P) \vdash \exists x : X \bullet P & \\ & \quad [\text{cut in } x : X \mid P] \\ D; x : X \mid P \wedge (\exists x : X \bullet P) \vdash & \quad [\text{discharge side lemma from hyp}] \\ D; x : X \mid P \vdash & \quad [\text{thin}] \end{aligned}$$

as required.

---

## Lemmas and their proofs

### C.1 Lemma ‘deterministic’

**Lemma 1** (deterministic) The correctness proof for a general *Okay* branch consists of the following three proof obligations: <sup>1</sup>

**exists-pd:**

$$\begin{array}{l} \Phi BOp; BOpPurseOkay; RabOut; RabCl'; RabIn \\ \vdash \\ \exists pdThis : PayDetails \bullet \mathcal{P} \end{array}$$

**exists-chosenLost:**

$$\begin{array}{l} \Phi BOp; BOpPurseOkay; RabOut; RabClPd'[pdThis/pdThis']; RabIn | \\ \mathcal{P} \\ \vdash \\ \exists chosenLost : \mathbb{P} PayDetails \bullet \mathcal{Q} \wedge chosenLost \sqsubseteq maybeLost \end{array}$$

**check-operation:**

$$\begin{array}{l} \Phi BOp; BOpPurseOkay; RabOut; RabClPd'[pdThis/pdThis']; \\ AbWorld; RabClPd; RabIn | \\ \mathcal{P} \wedge \mathcal{Q} \\ \vdash \\ AOp \end{array}$$

■

---

<sup>1</sup>Used in: lemma ‘*AbIgnore*’, section 14.6; lemma ‘*Ignore*’, section 14.7; lemma ‘*Abort*’ refines *AbIgnore*’, section 14.8; used to simplify every  $\mathcal{A}\text{-}\mathcal{B}$  operation proof.

**Proof:**

See section 14.4.5.

■ C.1

**C.2 Lemma ‘lost unchanged’**

**Lemma 2** (lost unchanged) For  $BOP\Xi Lost$  operations, where we have that  $maybeLost' = maybeLost$  and  $definitelyLost' = definitelyLost$ , the proof obligations **exists-pd** and **exists-chosenLost** are satisfied automatically by the instantiation of the predicates  $P$  and  $Q$  as:<sup>2</sup>

$$P \Leftrightarrow true$$

$$Q \Leftrightarrow chosenLost = chosenLost'$$

■

**Proof:**

See section 14.5

■ C.2

**C.3 Lemma ‘AbIgnore’**

Consider an operation  $BOPlg$  which refines  $AbIgnore$ . The operation should have the following properties.

- $BOPlg$  is a promoted operation, and thus alters only one concrete purse.
- for any purse, the *name* is unchanged.
- the domain of  $conAuthPurse$  is unchanged (by construction of the promotion)
- for any purse, either *nextSeqNo* is unchanged, or increased.

Where these properties hold for  $BOPlg$ , we can apply lemma  $AbIgnore$ .

**Lemma 3** ( $AbIgnore$ ) For a  $BOPlg$  operation, the **check-operation** proof obliga-

<sup>2</sup>Used in *ExceptionLogEnquiry*, chapter 21; *ExceptionLogClear*, chapter 22.

tion reduces to<sup>3</sup>

$$\Phi BOP; BOPlgPurse; RabCIPd'[pdThis/pdThis']; AbWorld; RabCIPd | \\ P \wedge Q$$

⊢

$$\forall n : \text{dom } abAuthPurse \bullet \\ (abAuthPurse' n).lost = (abAuthPurse n).lost \\ \wedge (abAuthPurse' n).balance = (abAuthPurse n).balance$$

■

**Proof:**

See section 14.6.

■ C.3

**C.4 Lemma ‘Abort refines AbIgnore’**

**Lemma 4** (*Abort* refines *AbIgnore*) Concrete *Abort* refines abstract *AbIgnore*.<sup>4</sup>

$$Abort; Rab'; RabOut \vdash \exists AbWorld; a? : AIN \bullet Rab \wedge RabIn \wedge AbIgnore$$

■

**Proof:**

See section 14.8.

■ C.4

**C.5 Lemma ‘abort backward’**

**Lemma 5** (abort backward) Where a concrete operation is written as a composition of *AbortPurseOkay* and a simpler operation starting from *eaFrom*, it is sufficient to prove that the promotion of the simpler operation alone refines

<sup>3</sup>Used in: ‘Ignore’, section 14.7; lemma ‘Abort refines AbIgnore’, section 14.8; used to simplify every  $A-B$  operation proof that refines *AbIgnore*.

<sup>4</sup>Used in: lemma ‘abort backward’, section C.5

the relevant abstract operation.<sup>5</sup>

$$\begin{aligned}
 & (\exists \Delta \text{ConPurse} \bullet \Phi \text{BOP} \wedge (\text{AbortPurseOkay} \S \text{BOPurseEafromOkay}); \\
 & \quad \text{Rab}'; \text{RabOut}; \\
 & \quad (\forall \text{BOPurseEafromOkay}; \text{Rab}'; \text{RabOut} \bullet \\
 & \quad \quad \exists \text{AbWorld}; a? : \text{AIN} \bullet \text{Rab} \wedge \text{RabIn} \wedge \text{AOp}) \\
 & \vdash \\
 & \exists \text{AbWorld}; a? : \text{AIN} \bullet \text{Rab} \wedge \text{RabIn} \wedge \text{AOp}
 \end{aligned}$$

■

**Proof:**

See section 14.9.

■ C.5

### C.6 Lemma 'constraint'

**Lemma 6** (constraint) If an operation does not change purse status and does not change the presence of payment detail messages in the ether (either by not emitting such a message, or by emitting an already existing message), then it preserves the *BetweenWorld* constraints.<sup>6</sup> ■

**Proof:**

See section 28.3.4.

■ C.6

### C.7 Lemma 'logs unchanged'

**Lemma 7** (logs unchanged) When the *archive* and the individual purse logs do not change, and when no new *req* messages are added to the *ether*, the set of

<sup>5</sup>Used in: *StartFrom*, section 16; *StartTo*, section 17; *ClearExceptionLog*, section 22; *ReadExceptionLog*, section 21

<sup>6</sup>Used in: *Increase*, section 28.4; *CClearExceptionLog*, section 29.8; *CArchive*, section 29.10.

*PayDetails* representing all the logs does not change either.<sup>7</sup>

$$\begin{aligned}
 & \text{BOPOkay} \mid \text{archive}' = \text{archive} \\
 & \wedge (\text{ran req}) \cap \text{ether}' = (\text{ran req}) \cap \text{ether} \bullet \\
 & \wedge \forall n : \text{dom conAuthPurse} \bullet \\
 & \quad (\text{conAuthPurse}' n). \text{exLog} = (\text{conAuthPurse } n). \text{exLog} \\
 & \vdash \\
 & \text{allLogs}' = \text{allLogs} \\
 & \wedge \text{toLogged}' = \text{toLogged} \\
 & \wedge \text{fromLogged}' = \text{fromLogged}
 \end{aligned}$$

■

**Proof:**

See section 28.6.

■ C.7

### C.8 Lemma 'abort forward'

**Lemma 8** (abort forward) Where a *C* operation is written as a composition of *CAbort* and a simpler operation starting from *eaFrom*, and the corresponding *B* operation is structured similarly, it is sufficient to prove that the simpler *C* operation refines corresponding *B* operation<sup>8</sup>.

$$\begin{aligned}
 & (\text{CAbort} \S \text{COPeafrom}); \text{Rbc}; \\
 & \quad (\forall \text{COPeafrom}; \text{Rbc} \bullet \exists \text{BetweenWorld}' \bullet \text{Rbc}' \wedge \text{BOPeafrom}) \\
 & \vdash \\
 & \exists \text{BetweenWorld}' \bullet \text{Rbc}' \wedge (\text{Abort} \S \text{BOPeafrom})
 \end{aligned}$$

■

**Proof:**

See section 28.7.

■ C.8

<sup>7</sup>Used in: lemma 'constraint', section 28.3.4; *CStartFrom*, section 29.2; *CReq*, section 29.4; *CVal*, section 29.5; *CAck*, section 29.6; *CReadExceptionLog*, section 29.7; *CAuthoriseExLogClear*, section 29.9.

<sup>8</sup>Used in: *CStartFrom*, section 29.2; *CStartTo*, section 29.3; *CReadExceptionLog*, section 29.7; *CClearExceptionLog*, section 29.8.



### C.9 Lemma ‘compose backward’

**Lemma C.1** (compose backward) If, under the backwards refinement rules, a concrete operation  $COP_1$  is a refinement of abstract operation  $AOP_1$ , and  $COP_2$  is a refinement of  $AOP_2$ , then their composition is a refinement of the abstract composition<sup>9</sup>.

$$\begin{array}{l} (COP_1 \circ COP_2); R'; ROut; \\ (\forall COP_1; R'; ROut \bullet (\exists A; AIn \bullet R \wedge RIn \wedge AOP_1)); \\ (\forall COP_2; R'; ROut \bullet (\exists A; AIn \bullet R \wedge RIn \wedge AOP_2)) \\ \vdash \\ \exists A; AIn \bullet R \wedge RIn \wedge (AOP_1 \circ AOP_2) \end{array}$$

■

**Proof:**

This result is reasonably self-evident, from the definition of refinement in terms of complete programs. We show that the particular form of the theorem holds here.

Without loss of generality, assume that the concrete and abstract state schemas have a single component,  $c$  and  $a$  respectively. (A multi-component state is isomorphic to a single component state consisting of all the multi-components bundled into a single schema or Cartesian product.)

Expand the compositions, and rename the quantified variables in the hypothesis.

$$\begin{array}{l} (\exists C_0 \bullet COP_1[c_0/c'] \wedge COP_2[c_0/c]); R'; ROut; \\ (\forall COP_1[c_0/c']; R_0; ROut \bullet (\exists A; AIn \bullet R \wedge RIn \wedge AOP_1[a_0/a'])); \\ (\forall COP_2[c_0/c]; R'; ROut \bullet (\exists A_0; AIn \bullet R_0 \wedge RIn \wedge AOP_2[a_0/a])) \\ \vdash \\ \exists A; AIn \bullet R \wedge RIn \wedge (\exists A_0 \bullet AOP_1[a_0/a'] \wedge AOP_2[a_0/a]) \end{array}$$

Use [hyp exists] to drop the  $\exists$  in the hypothesis, then simplify.

$$\begin{array}{l} COP_1[c_0/c']; COP_2[c_0/c]; R'; ROut; \\ (\forall COP_1[c_0/c']; R_0; ROut \bullet \\ (\exists A; AIn \bullet R \wedge RIn \wedge AOP_1[a_0/a'])); \\ (\forall COP_2[c_0/c]; R'; ROut \bullet \\ (\exists A_0; AIn \bullet R_0 \wedge RIn \wedge AOP_2[a_0/a])) \\ \vdash \\ \exists A; AIn \bullet R \wedge RIn \wedge (\exists A_0 \bullet AOP_1[a_0/a'] \wedge AOP_2[a_0/a]) \end{array}$$

<sup>9</sup>Used in: lemma ‘abort backward’, section C.5.

Use  $D \wedge (\forall D \bullet P) \Rightarrow P$  to simplify the second universal quantifier in the hypothesis.

$$\begin{array}{l} COP_1[c_0/c']; COP_2[c_0/c]; R'; ROut; \\ (\forall COP_1[c_0/c']; R_0; ROut \bullet \\ (\exists A; AIn \bullet R \wedge RIn \wedge AOP_1[a_0/a'])) \mid \\ \exists A_0; AIn \bullet R_0 \wedge RIn \wedge AOP_2[a_0/a] \\ \vdash \\ \exists A; AIn \bullet R \wedge RIn \wedge (\exists A_0 \bullet AOP_1[a_0/a'] \wedge AOP_2[a_0/a]) \end{array}$$

Use [hyp exists] to drop the  $\exists$  in the hypothesis, then simplify.

$$\begin{array}{l} COP_1[c_0/c']; COP_2[c_0/c]; R_0; R'; ROut; RIn; AOP_2[a_0/a]; \\ (\forall COP_1[c_0/c']; R_0; ROut \bullet \\ (\exists A; AIn \bullet R \wedge RIn \wedge AOP_1[a_0/a'])) \\ \vdash \\ \exists A; AIn \bullet R \wedge RIn \wedge (\exists A_0 \bullet AOP_1[a_0/a'] \wedge AOP_2[a_0/a]) \end{array}$$

Repeat the previous three steps to simplify the remaining quantifier in the hypothesis.

$$\begin{array}{l} COP_1[c_0/c']; COP_2[c_0/c]; R; R_0; R'; ROut; RIn; \\ AOP_1[a_0/a']; AOP_2[a_0/a] \\ \vdash \\ \exists A; AIn \bullet R \wedge RIn \wedge (\exists A_0 \bullet AOP_1[a_0/a'] \wedge AOP_2[a_0/a]) \end{array}$$

Move the inner  $\exists$  in the consequent outwards.

$$\begin{array}{l} COP_1[c_0/c']; COP_2[c_0/c]; R; R_0; R'; ROut; RIn; \\ AOP_1[a_0/a']; AOP_2[a_0/a] \\ \vdash \\ \exists A; A_0; AIn \bullet R \wedge RIn \wedge AOP_1[a_0/a'] \wedge AOP_2[a_0/a] \end{array}$$

All the terms are in the hypothesis.

■ C.9

### C.10 Lemma ‘compose forward’

**Lemma C.2** (compose forward) If, under the forwards refinement rules, concrete operation  $COP_1$  is a refinement of abstract operation  $AOP_1$ , and  $COP_2$  is a refinement of  $AOP_2$ , then their composition is a refinement of the abstract



combine the schemas across the quantifiers.

$$\begin{aligned}
&= \exists \text{Global}_0 \bullet \\
&\quad (\exists \text{Local}; \text{Local}_a \bullet \\
&\quad \quad [ \text{locals}; \text{locals}_0 : \text{NAME} \mapsto \text{Local} \mid \\
&\quad \quad \quad n? \in \text{dom locals} \\
&\quad \quad \quad \wedge \text{locals } n? = \theta \text{Local} \\
&\quad \quad \quad \wedge \text{locals}_0 = \text{locals} \oplus \{n? \mapsto \theta \text{Local}_a\} ] \\
&\quad \wedge \text{Op}_1[x_a/x']) \\
&\quad \wedge (\exists \text{Local}_b; \text{Local}' \bullet \\
&\quad \quad [ \text{locals}_0; \text{locals}' : \text{NAME} \mapsto \text{Local} \mid \\
&\quad \quad \quad n? \in \text{dom locals}_0 \\
&\quad \quad \quad \wedge \text{locals}_0 n? = \theta \text{Local}_b \\
&\quad \quad \quad \wedge \text{locals}' = \text{locals}_0 \oplus \{n? \mapsto \theta \text{Local}'\} ] \\
&\quad \wedge \text{Op}_2[x_b/x])
\end{aligned}$$

Combine all these as a single schema, putting the quantifications into the predicate.

$$\begin{aligned}
&= [ \text{locals}; \text{locals}' : \text{NAME} \mapsto \text{Local} \mid \\
&\quad \exists \text{local}_0; \text{Local}; \text{Local}'; \text{Local}_a; \text{Local}_b \bullet \\
&\quad \quad n? \in \text{dom locals} \\
&\quad \quad \wedge \text{locals } n? = \theta \text{Local} \\
&\quad \quad \wedge \text{locals}_0 = \text{locals} \oplus \{n? \mapsto \theta \text{Local}_a\} \\
&\quad \quad \wedge n? \in \text{dom locals}_0 \\
&\quad \quad \wedge \text{locals}_0 n? = \theta \text{Local}_b \\
&\quad \quad \wedge \text{locals}' = \text{locals}_0 \oplus \{n? \mapsto \theta \text{Local}'\} \\
&\quad \quad \wedge \text{Op}_1[x_a/x'] \\
&\quad \quad \wedge \text{Op}_2[x_b/x] ]
\end{aligned}$$

We can remove the quantification of  $\text{local}_0$  because we have a full definition of it in terms of other variables. This leaves the following equations relating the remaining variables.

$$\begin{aligned}
&= [ \text{locals}; \text{locals}' : \text{NAME} \mapsto \text{Local} \mid \\
&\quad \exists \text{Local}; \text{Local}'; \text{Local}_a; \text{Local}_b \bullet \\
&\quad \quad n? \in \text{dom locals} \\
&\quad \quad \wedge \text{locals } n? = \theta \text{Local} \\
&\quad \quad \wedge \theta \text{Local}_b = \theta \text{Local}_a \\
&\quad \quad \wedge \text{locals}' = \text{locals} \oplus \{n? \mapsto \theta \text{Local}'\} \\
&\quad \quad \wedge \text{Op}_1[x_a/x'] \\
&\quad \quad \wedge \text{Op}_2[x_b/x] ]
\end{aligned}$$

Using the equation that  $\theta \text{Local}_b = \theta \text{Local}_a$ , rename  $\text{Local}_a$  and  $\text{Local}_b$  both to  $\text{Local}_0$ .

$$\begin{aligned}
&= [ \text{locals}; \text{locals}' : \text{NAME} \mapsto \text{Local} \mid \\
&\quad \exists \text{Local}; \text{Local}'; \text{Local}_0 \bullet \\
&\quad \quad n? \in \text{dom locals} \\
&\quad \quad \wedge \text{locals } n? = \theta \text{Local} \\
&\quad \quad \wedge \text{locals}' = \text{locals} \oplus \{n? \mapsto \theta \text{Local}'\} \\
&\quad \quad \wedge \text{Op}_1[x_0/x'] \\
&\quad \quad \wedge \text{Op}_2[x_0/x] ]
\end{aligned}$$

Redistribute the quantifications

$$\begin{aligned}
&= \exists \text{Local}; \text{Local}' \bullet \\
&\quad [ \text{locals}; \text{locals}' : \text{NAME} \mapsto \text{Local} \mid \\
&\quad \quad n? \in \text{dom locals} \\
&\quad \quad \wedge \text{locals } n? = \theta \text{Local} \\
&\quad \quad \wedge \text{locals}' = \text{locals} \oplus \{n? \mapsto \theta \text{Local}'\} \\
&\quad \quad \wedge (\exists \text{Local}_0 \bullet \text{Op}_1[x_0/x'] \wedge \text{Op}_2[x_0/x]) ]
\end{aligned}$$

and rewrite in terms of composition

$$\begin{aligned}
&= \exists \text{Local}; \text{Local}' \bullet \Phi \wedge (\text{Op}_1 \circ \text{Op}_2) \\
&= \exists \Delta \text{Local} \bullet \Phi \wedge (\text{Op}_1 \circ \text{Op}_2)
\end{aligned}$$

This is the left hand side of the equation, and hence the proof is complete.

■ C.11

## C.12 Lemma 'notLoggedAndIn'

**Lemma C.4** (notLoggedAndIn) If a purse is engaged in a transaction, it does not have a log for that transaction <sup>12</sup>.

*BetweenWorld*

⊢

$(\text{fromInEpr} \cup \text{fromInEpa}) \cap \text{fromLogged} = \emptyset$

$\wedge (\text{toInEpr} \cup \text{toInEapayee}) \cap \text{toLogged} = \emptyset$

■

<sup>12</sup>Used in: *Val*, behaviour of *toLogged*, section 19.6.2; *Ack*, behaviour of *definitelyLost*, section 20.6.5; *CVal*, B-10, section 29.5; lemma 'lost', section C.13; lemma 'not lost before', section C.14.

**Proof:**

Consider the *to* purse case. We consider the *pd* stored in the *to* purse, so

$$\begin{aligned} pd \in (toInEpv \cup toInEapayee) &\Rightarrow \\ pd.toSeqNo = (conAuthPurse pd.to).pdAuth.toSeqNo & \end{aligned}$$

We have, from *BetweenWorld* constraint B-8, that

$$pd \in toLogged \Rightarrow pd.toSeqNo < (conAuthPurse pd.to).pdAuth.toSeqNo$$

Hence there can be no *pd* in both sets.

The arguments for the *from* cases follow similarly, from *BetweenWorld* constraint B-7.

■ C.12

**C.13 Lemma ‘lost’**

**Lemma C.5** (lost) The sets *definitelyLost* and *maybeLost* are disjoint: a *pd* can never be in both. <sup>13</sup>

$$BetweenWorld \vdash definitelyLost \cap maybeLost = \emptyset$$

■

**Proof:**

$$\begin{aligned} definitelyLost \cap maybeLost & \\ = toLogged \cap (fromLogged \cup fromInEpa) & \quad [defn.] \\ \cap (fromInEpa \cup fromLogged) \cap toInEpv & \\ = toLogged \cap toInEpv \cap (fromLogged \cup fromInEpa) & \quad [rearranging] \\ = \emptyset & \quad [Lemma \text{ ‘notLoggedAndIn’ (section C.12)}] \end{aligned}$$

■ C.13

<sup>13</sup>Used in: *Req*, case 1, section 18.7.1; *Req*, case 2, section 18.8.1; *Req*, case 3, section 18.9.1.

**C.14 Lemma ‘not lost before’**

**Lemma C.6** (not lost before) *pdThis* is not lost before the *Req* operation, although it maybe lost after. <sup>14</sup>

$$\begin{aligned} \Phi BOp; ReqPurseOkay; pdThis : PayDetails \mid (req \sim m?) = pdThis & \\ \vdash & \\ definitelyLost = definitelyLost' \setminus \{pdThis\} & \\ \wedge maybeLost = maybeLost' \setminus \{pdThis\} & \end{aligned}$$

■

**Proof:**

From the definition of the way the state changes in *ReqOkay* we can say that the following sets are the same before and afterward:

$$\begin{aligned} fromLogged &= fromLogged' \\ \wedge toLogged &= toLogged' \\ \wedge toInEpv &= toInEpv' \end{aligned}$$

For the set *fromInEpa*, we know from *ReqOkay* that beforehand this *pdThis* was *not* in the set and afterward it was. So

$$\begin{aligned} pdThis \in fromInEpa & \\ \wedge fromInEpa = fromInEpa' \setminus \{pdThis\} & \end{aligned}$$

From Lemma ‘notLoggedAndIn’ (section C.12), we have:

$$pdThis \in fromInEpa \Rightarrow pdThis \notin fromLogged'$$

Reminding ourselves of the definitions of *definitelyLost* and using the identities above, we have

$$\begin{aligned} definitelyLost & \\ = toLogged \cap (fromLogged \cup fromInEpa) & \quad [defn] \\ = toLogged' \cap (fromLogged' \cup fromInEpa' \setminus \{pdThis\}) & \quad [above] \\ = toLogged' \cap (fromLogged' \cup fromInEpa') \setminus \{pdThis\} & \\ & \quad [pdThis \notin fromLogged'] \\ = (toLogged' \cap (fromLogged' \cup fromInEpa')) \setminus \{pdThis\} & \quad [Spivey] \\ = definitelyLost' \setminus \{pdThis\} & \quad [defn] \end{aligned}$$

<sup>14</sup>Used in: *Req*, **exists-chosenLost**, section 18.5; *Req*, **check-operation**, section 18.6.

Similarly for *maybeLost*:

$$\begin{aligned}
\text{maybeLost} &= (\text{fromInEpa} \cup \text{fromLogged}) \cap \text{toInEpv} && \text{[defn]} \\
&= ((\text{fromInEpa}' \setminus \{pdThis\}) \cup \text{fromLogged}') \cap \text{toInEpv}' && \text{[above]} \\
&= ((\text{fromInEpa}' \cup \text{fromLogged}') \setminus \{pdThis\}) \cap \text{toInEpv}' \\
&\quad \text{[}pdThis \notin \text{fromLogged}'\text{]} \\
&= ((\text{fromInEpa}' \cup \text{fromLogged}') \cap \text{toInEpv}') \setminus \{pdThis\} && \text{[prop } \setminus \text{]} \\
&= \text{maybeLost}' \setminus \{pdThis\} && \text{[def]}
\end{aligned}$$

■ C.14

### C.15 Lemma ‘*AbWorld* unique’

**Lemma C.7** (*AbWorld* unique) Given *BetweenWorld* and a choice of which transactions will be lost, there is always exactly one *AbWorld* that retrieves.<sup>15</sup>

$$\begin{aligned}
&\text{BetweenWorld}; \text{chosenLost} : \mathbb{P} \text{ PayDetails}; \text{pdThis} : \text{PayDetails} \mid \\
&\quad \text{chosenLost} \subseteq \text{maybeLost} \\
&\vdash \\
&\exists_1 \text{AbWorld} \bullet \text{RabCLPD}
\end{aligned}$$

■

#### Proof:

Each element of *AbWorld* has an explicit equation in *Rab* defining it uniquely in terms of *BetweenWorld* components. The components are entirely independent, and the only constraint that ties any together is that on *chosenLost* and *maybeLost*, which we have directly in the hypothesis.

The constraints required of any *AbWorld* can be shown to hold as follows:

- *abAuthPurse* : *NAME*  $\leftrightarrow$  *AbPurse*  
*conAuthPurse* is a finite function. From the retrieve *AbstractBetween* the domain of *abAuthPurse* equals the domain of *conAuthPurse*, and so is finite, too.

■ C.15  
 ■ C

<sup>15</sup>Used in: lemma ‘deterministic’, section 14.4.4.

## Auxiliary toolkit definitions

### D.1 Total abstract balance

The function *totalAbBalance* returns the total value held in a finite collection of purses.

$$\begin{array}{|l}
\text{totalAbBalance} : (\text{NAME} \leftrightarrow \text{AbPurse}) \rightarrow \mathbb{N} \\
\text{totalAbBalance } \emptyset = 0 \\
\forall w : \text{NAME} \leftrightarrow \text{AbPurse}; n : \text{NAME}; \text{AbPurse} \mid n \notin \text{dom } w \bullet \\
\quad \text{totalAbBalance}(\{n \mapsto \emptyset \text{AbPurse}\} \cup w) = \\
\quad \text{balance} + \text{totalAbBalance } w
\end{array}$$

This recursive definition is valid, because it is finite, and hence bounded.

### D.2 Total lost value

The function *totalLost* returns the total value lost by a finite collection of purses.

$$\begin{array}{|l}
\text{totalLost} : (\text{NAME} \leftrightarrow \text{AbPurse}) \rightarrow \mathbb{N} \\
\text{totalLost } \emptyset = 0 \\
\forall w : \text{NAME} \leftrightarrow \text{AbPurse}; n : \text{NAME}; \text{AbPurse} \mid n \notin \text{dom } w \bullet \\
\quad \text{totalLost}(\{n \mapsto \emptyset \text{AbPurse}\} \cup w) = \text{lost} + \text{totalLost } w
\end{array}$$

This recursive definition is valid, because it is finite, and hence bounded.

### D.3 Summing values

We define the sum of the values in a set of exception logs, or a set of payment details. This recursive definition is valid, because it is finite, and hence bounded.

$$\begin{array}{|l} \hline \text{sumValue} : \mathbb{F} \text{PayDetails} \rightarrow \mathbb{N} \\ \hline \text{sumValue } \emptyset = 0 \\ \forall \text{ pds} : \mathbb{F} \text{PayDetails}; \text{PayDetails} \mid \emptyset \text{PayDetails} \notin \text{pds} \bullet \\ \text{sumValue}(\{\emptyset \text{PayDetails}\} \cup \text{pds}) = \text{value} + \text{sumValue } \text{pds} \end{array}$$

---

## Bibliography

[Barden *et al.* 1994]

Rosalind Barden, Susan Stepney, and David Cooper. *Z in Practice*. BCS Practitioners Series. Prentice Hall, 1994.

[Flynn *et al.* 1990]

Mike Flynn, Tim Hoverd, and David Brazier. Formaliser—an interactive support tool for Z. In John E. Nicholls, editor, *Z User Workshop: Proceedings of the 4th Annual Z User Meeting, Oxford 1989*, Workshops in Computing, pages 128–141. Springer Verlag, 1990.

[Spivey 1992a]

J. Michael Spivey. *The fuzz Manual*. Computer Science Consultancy, 2nd edition, 1992. <ftp://ftp.comlab.ox.ac.uk/pub/Zforum/fuzz>.

[Spivey 1992b]

J. Michael Spivey. *The Z Notation: a Reference Manual*. Prentice Hall, 2nd edition, 1992.

[Stepney]

Susan Stepney. Formaliser Home Page. <http://public.logica.com/~formaliser/>.

[Woodcock & Davies 1996]

Jim Woodcock and Jim Davies. *Using Z: Specification, Refinement, and Proof*. Prentice Hall, 1996.

---

## Index

$\Phi BOp$ , 31  
 $\Phi COP$ , 37  
 $\perp$ , 20  
  
*abAuthPurse*; *AbWorld*, 16  
*AbFinOut*, 18  
*AbFinState*, 18  
*AbIgnore*, 16  
*AbInitIn*, 18  
*AbInitState*, 17  
*AbOp*, 16  
*Abort*, 32  
*AbortPurseOkay*, 22  
*AbPurse*, 15  
*AbPurseTransfer*, 16  
*AbstractBetween*, 45  
*AbTransfer*, 17  
*AbTransferLost*, 17  
*AbTransferLostTD*, 17  
*AbTransferOkay*, 17  
*AbTransferOkayTD*, 17  
*AbWorld*, 16  
*AbWorldSecureOp*, 16  
*Ack*, 33  
*ack*, 20  
*AckPurseOkay*, 24  
*AIN*, 16  
  
*allLogs*; *AuxWorld*, 28  
*AllValueAccounted*, 13  
*aNullIn*, 16  
*aNullOut*, 16  
*AOUT*, 16  
*Archive*, 34  
*archive*, 27  
*Authentic*, 13  
*AuthenticAckMessage*, 24  
*authenticFrom*; *AuxWorld*, 28  
*AuthenticReqMessage*, 24  
*authenticTo*; *AuxWorld*, 28  
*AuthenticValMessage*, 24  
*AuthoriseExLogClearOkay*, 33  
*AuxWorld*, 28  
  
*balance*; *AbPurse*, 15  
*balance*; *ConPurse*, 20  
*BetweenInitState*, 35  
*BetweenWorld*, 30  
*BetwFinOut*, 36  
*BetwFinState*, 36  
*BetwInitIn*, 36  
  
*CAbort*, 38  
*CAck*, 38  
*CArchive*, 39

*CAuthoriseExLogClear*, 39  
*CClearExceptionLog*, 38  
**check-operation**, 58  
*CIgnore*, 38  
*CIincrease*, 38  
*CLEAR*, 19  
*ClearExceptionLog*, 33  
*ClearExceptionLogEapayerOkay*, 33  
*ClearExceptionLogPurseEapayerOkay*, 26  
*ClearExceptionLogPurseOkay*, 26  
*ConFinState*, 39  
*ConInitState*, 39  
*ConPurse*, 20  
*ConPurseAbort*, 22  
*ConPurseAck*, 22  
*ConPurseClear*, 26  
*ConPurseIncrease*, 21  
*ConPurseReq*, 22  
*ConPurseStart*, 22  
*ConPurseVal*, 22  
*consequent*, 114  
*consqconj*, 116  
*consqdisj*, 116  
*consqexists*, 117  
*contradiction*, 117  
*ConWorld*, 27  
*CounterPartyDetails*, 19  
*cpd*; *StartFromPurseEapayerOkay*, 22  
*cpd*; *StartToPurseEapayerOkay*, 23  
*cpd*; *ValidStartFrom*, 22  
*cpd*; *ValidStartTo*, 23  
*CReadExceptionLog*, 38  
*CReq*, 38  
*CStartFrom*, 38  
*CStartTo*, 38  
*cut*, 116  
*CVal*, 38  
  
*definitelyLost*; *AuxWorld*, 28  
  
*eaPayee*, 18  
*eaPayer*, 18  
*epa*, 18  
*epr*, 18  
*epv*, 18  
*ether*; *ConWorld*, 27  
*exceptionLogClear*, 20  
*exceptionLogResult*, 20  
**exists-chosenLost**, 58  
**exists-pd**, 58  
*exLog*; *ConPurse*, 20  
  
*from*; *TransferDetails*, 16  
*fromInEpa*; *AuxWorld*, 28  
*fromInEpr*; *AuxWorld*, 28  
*fromLogged*; *AuxWorld*, 28  
*fromSeqNo*; *PayDetails*, 19  
  
*GlobalWorld*, 18  
  
*hypdisj*, 116  
*hypexists*, 117  
*hypuni*, 116  
*hypothesis*, 114  
  
*Ignore*, 32, 55  
*image*, 19  
*Increase*, 32  
*IncreasePurseOkay*, 21  
  
lemma '*Abort* refines *AbIgnore*', 61  
lemma '*AbIgnore*', 119  
lemma 'abort backward', 65, 119  
lemma 'abort forward', 120  
lemma '*Abort* refines *AbIgnore*', 119  
lemma '*AbWorld* unique', 125  
lemma 'compose backward', 121  
lemma 'compose forward', 121  
lemma 'constraint', 100, 120  
lemma 'deterministic', 58, 118  
lemma 'ignore', 55  
lemma 'logs unchanged', 120

lemma 'lost unchanged', 59, 119  
 lemma 'lost', 124  
 lemma 'not lost before', 124  
 lemma 'notLoggedAndIn', 124  
 lemma 'promoted composition', 122  
*Logbook*, 27  
*LogIfNecessary*, 13  
*lost*; *AbPurse*, 15  
  
*maybeLost*; *AuxWorld*, 28  
*MESSAGE*, 20  
  
*NAME*, 15  
*name*; *ConPurse*, 20  
*name*; *CounterPartyDetails*, 19  
*negation*, 116  
*nextSeqNo*; *ConPurse*, 20  
*nextSeqNo*; *CounterPartyDetails*, 19  
*NoValueCreation*, 12  
  
*onpoint*, 117  
*OtherPursesRab*, 46  
  
*PayDetails*, 19  
*pdAuth*; *ConPurse*, 20  
*purse*; *ConWorld*, 27  
  
*Rab*, 46  
*RabCl*, 45  
*RabClPd*, 46  
*RabEnd*, 49  
*RabEndClPd*, 48  
*RabHasBeenLost*, 49  
*RabHasBeenLostClPd*, 48  
*RabIn*, 50  
*RabOkay*, 49  
*RabOkayClPd*, 47  
*RabOut*, 50  
*RabWillBeLost*, 49  
*RabWillBeLostClPd*, 47  
*Rbc*, 96  
*ReadExceptionLog*, 33  
  
*readExceptionLog*, 20  
*ReadExceptionLogEapayerOkay*, 33  
*ReadExceptionLogPurseEapayerOkay*,  
 25  
*ReadExceptionLogPurseOkay*, 25  
*Req*, 33  
*req*, 20  
*ReqPurseOkay*, 24  
*RetryAck*, 25  
*RetryReq*, 25  
*RetryVal*, 25  
  
*StartFrom*, 32  
*startFrom*, 20  
*StartFromEapayerOkay*, 33  
*StartFromPurseEapayerOkay*, 22  
*StartFromPurseOkay*, 23  
*StartTo*, 32  
*startTo*, 20  
*StartToEapayerOkay*, 33  
*StartToPurseEapayerOkay*, 23  
*StartToPurseOkay*, 24  
*STATUS*, 18  
*status*; *ConPurse*, 20  
*strengthenconsq*, 116  
*SufficientFundsProperty*, 13  
*sumValue*, 127  
  
*thin*, 116  
*to*; *TransferDetails*, 16  
*toInEapayee*; *AuxWorld*, 28  
*toInEpv*; *AuxWorld*, 28  
*toLogged*; *AuxWorld*, 28  
*toSeqNo*; *PayDetails*, 19  
*totalAbBalance*, 126  
*totalLost*, 126  
*transfer*, 16  
*TransferDetails*, 16  
  
*unihyp*, 115  
  
*Val*, 33

*val*, 20  
*ValidStartFrom*, 22  
*ValidStartTo*, 23  
*ValPurseOkay*, 24  
*value*; *CounterPartyDetails*, 19  
*value*; *TransferDetails*, 16





