



Đặc tả Z (5)



Giới thiệu

- được đề xuất bởi Jean René Abrial ở Đại học Oxford
- ngôn ngữ đặc tả hình thức được sử dụng rộng rãi nhất
- dựa trên lý thuyết tập hợp
- ký hiệu toán học
- sử dụng các sơ đồ (schema)
 - dễ hiểu



Giới thiệu

- Gồm bốn thành phần cơ bản
 - các kiểu dữ liệu (types)
 - dựa trên khái niệm tập hợp
 - các sơ đồ trạng thái (state schemas)
 - mô tả các biến và ràng buộc trên các biến
 - các sơ đồ thao tác (operation schemas)
 - mô tả các thao tác (thay đổi trạng thái)
 - các toán tử sơ đồ (schema operations)
 - định nghĩa các sơ đồ mới từ các sơ đồ đã có

3



Kiểu dữ liệu

- mỗi kiểu dữ liệu là một **tập hợp** các phần tử
- Ví dụ
 - {true, false} : kiểu lô-gíc
 - N: kiểu số tự nhiên
 - Z: kiểu số nguyên
 - R: kiểu số thực
 - {red, blue, green}

4



Kiểu dữ liệu

- Các phép toán trên tập hợp

- Hợp: $A \cup B$
- Giao: $A \cap B$
- Hiệu: A / B
- Tập con: $A \subseteq B$
- Tập các tập con: $P A$
 - ví dụ: $P \{a, b\} = \{\{\}, \{a\}, \{b\}, \{a, b\}\}$

5



Kiểu dữ liệu

- một số kiểu dữ liệu cơ bản đã được định nghĩa trước

- kiểu số nguyên Z
- kiểu số tự nhiên N
- kiểu số thực R
- ...

- có thể định nghĩa các kiểu dữ liệu mới

- ANSWER == yes | no
- [PERSON]
 - sử dụng cặp ký hiệu [và] để định nghĩa kiểu cơ bản mới

6



Kiểu dữ liệu

- Khai báo kiểu

- $x : T$

- x là phần tử của tập T

- Ví dụ

- $x : R$

- $n : N$

- $3 : N$

- $\text{red} : \{\text{red, blue, green}\}$

7



Vị từ

- Một vị từ (predicate) được sử dụng để định nghĩa các tính chất của biến/giá trị

- Ví dụ

- $x > 0$

- $\pi \in R$

8



Ví từ

- Có thể sử dụng các toán tử lô-gíc để định nghĩa các ví từ phức tạp

- Và: $A \wedge B$
- Hoặc: $A \vee B$
- Phủ định: $\neg A$
- Kéo theo: $A \Rightarrow B$

- Ví dụ

- $(x > y) \wedge (y > 0)$
- $(x > 10) \vee (x = 1)$
- $(x > 0) \Rightarrow x/x = 1$
- $(\neg(x \in S)) \vee (x \in T)$

9



Ví từ

- Các toán tử khác

- $(\forall x : T \bullet A)$
 - A đúng với **mọi** x thuộc T
 - Ví dụ: $(\forall x : N \bullet x - x = 0)$

- $(\exists x : T \bullet A)$
 - A đúng với **một số** giá trị x thuộc T
 - Ví dụ: $(\exists x : R \bullet x + x = 4)$

- $\{x : T \mid A\}$
 - biểu diễn các phần tử x của T thỏa mãn A
 - Ví dụ: $N = \{x : Z \mid x \geq 0\}$

10



Sơ đồ trạng thái

- Cấu trúc sơ đồ trạng thái gồm
 - tên sơ đồ
 - khai báo biến
 - định nghĩa vị từ

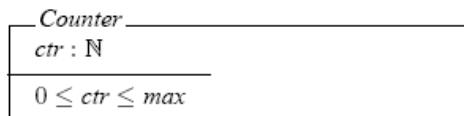


11



Sơ đồ trạng thái

- Đặc tả Z chứa
 - các biến trạng thái
 - khởi gán biến
 - các thao tác trên các biến
 - biến trạng thái có thể có các bất biến
 - điều kiện mà luôn đúng, biểu diễn bởi các vị từ

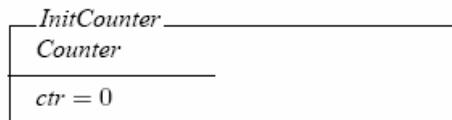


12



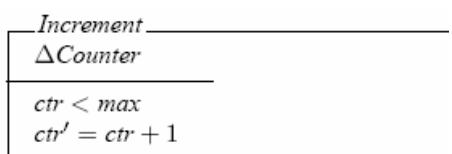
Sơ đồ thao tác

- Khởi gán biến



- Khai báo thao tác trên biến

- kí hiệu Δ biểu diễn biến trạng thái bị thay đổi bởi thao tác
- kí hiệu ‘ (dấu nháy đơn) biểu diễn giá trị mới của biến



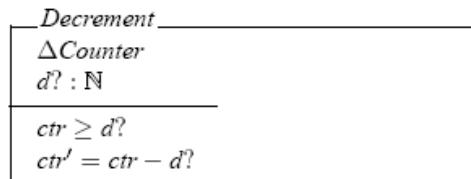
13



Sơ đồ thao tác

- Thao tác có thể có các tham số vào và ra

- tên tham số vào kết thúc bởi kí tự “?”
- tên tham số ra kết thúc bởi kí tự “!”



14



Sơ đồ thao tác

- Kí hiệu \exists mô tả thao tác không thể thay đổi biến trạng thái

Display _____
 $\exists Counter$
 $c! : \mathbb{N}$
 $c! = ctr$

15



Ví dụ 1

- ĐẶC TẢ HỆ THỐNG GHI NHẬN CÁC NHÂN VIÊN VÀO/RA TÒA NHÀ LÀM VIỆC
 - Kiểu dữ liệu $[Staff]$ là kiểu cơ bản mới của hệ thống
 - Trạng thái của hệ thống bao gồm
 - tập hợp các người sử dụng hệ thống $user$
 - tập hợp các nhân viên đang vào in
 - tập hợp các nhân viên đang ra out

Log _____
 $users, in, out : \mathbb{P} Staff$
 $in \cap out = \{\} \wedge$
 $in \cup out = users$

bất biến của hệ thống

16



Ví dụ 1

- Đặc tả thao tác ghi nhận một nhân viên vào

CheckIn _____
 ΔLog
 $name? : Staff$

 $name? \in out$
 $in' = in \cup \{name?\}$
 $out' = out \setminus \{name?\}$
 $users' = users$

17



Ví dụ 1

- Đặc tả thao tác ghi nhận một nhân viên ra

CheckOut _____
 ΔLog
 $name? : Staff$

 $name? \in in$
 $out' = out \cup \{name?\}$
 $in' = in \setminus \{name?\}$
 $users' = users$

18



Ví dụ 1

- Đặc tả thao tác kiểm tra một nhân viên vào hay ra

- Thao tác này cho kết quả là phần tử của kiểu

$QueryReply == is_in | is_out$

- Đặc tả thao tác

```
StaffQuery
└ Log
  name? : Staff
  reply! : QueryReply
  _____
  name? ∈ users
  name? ∈ in ⇒ reply! = is_in
  name? ∈ out ⇒ reply! = is_out
```

19



Ví dụ 1

- Khởi tạo hệ thống

```
InitLog
└ Log
  users = {}
  in = {}
  out = {}
```

20



Ví dụ 1

- Tóm lại

- **Sơ đồ trạng thái:** các thành phần/đối tượng của hệ thống
- **Bắt biến:** ràng buộc giữa các đối tượng
- **Các sơ đồ thao tác**
 - Điều kiện trên các tham số vào
 - Quan hệ giữa trạng thái trước và sau
 - Tham số kết quả
- **Khởi gán**

21



Ví dụ 1

- Hãy đặc tả các thao tác

- Register: thêm vào một nhân viên mới
- QueryIn: cho biết những nhân viên đang vào/làm việc

22



Toán tử sơ đồ

- Các sơ đồ có thể được kết hợp để tạo ra các sơ đồ mới
- Các toán tử sơ đồ
 - Và: \wedge
 - Hoặc: \vee

23



Toán tử sơ đồ

- Các sơ đồ đã có

Schema1
$x : X; \quad y : Y$
$\mathcal{A}(x, y)$

Schema2
$z : Z; \quad x : X$
$\mathcal{B}(z, x)$

- Tạo các sơ đồ mới

- Schema3 == Schema1 \wedge Schema2
- Schema4 == Schema1 \vee Schema2

Schema3
$x : X; \quad y : Y; \quad z : Z$
$\mathcal{A}(x, y) \wedge \mathcal{B}(z, x)$

Schema4
$x : X; \quad y : Y; \quad z : Z$
$\mathcal{A}(x, y) \vee \mathcal{B}(z, x)$

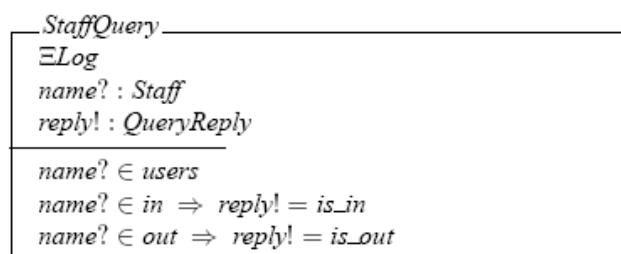
24



Ví dụ 1 (tiếp)

- Cải tiến thao tác *StaffQuery*

- Thao tác *StaffQuery* chưa đặc tả trường hợp lỗi
 - $\text{name}? \notin \text{users}$



25

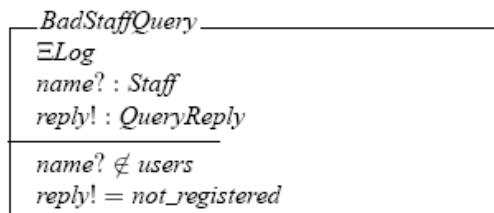


Ví dụ 1 (tiếp)

- Cải tiến thao tác *StaffQuery*

- Đặc tả lại kiểu *QueryReply*

$$\text{QueryReply} == \text{is_in} \mid \text{is_out} \mid \text{not_registered}$$



- Khi đó

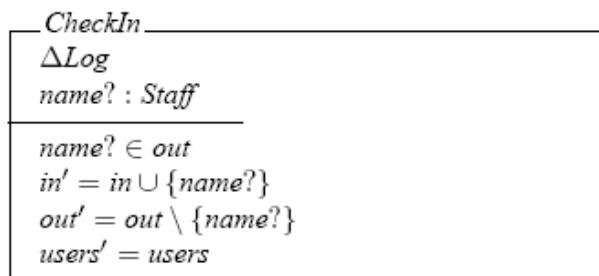
$$\text{RobustStaffQuery} == \text{StaffQuery} \vee \text{BadStaffQuery}$$

26



Ví dụ 1 (tiếp)

- Cải tiến thao tác *CheckIn*



- Mở rộng thao tác cho trường hợp ghi nhận thành công

27



Ví dụ 1 (tiếp)

- Cải tiến thao tác *CheckIn*

- Mở rộng thao tác cho trường hợp ghi nhận thành công



- Khi đó

$$\textit{GoodCheckIn} = \textit{CheckIn} \wedge \textit{Success}$$

28



Ví dụ 1 (tiếp)

- Cải tiến thao tác *CheckIn*

- Xử lý thêm hai trường hợp lỗi
 - 1. name? đã được ghi nhận
 - 2. name? chưa được đăng ký

```
BadCheckIn1 _____  
ΞLog  
name? : Staff  
reply! : CheckInReply  
  
name? ∈ in  
reply! = already_in
```

29



Ví dụ 1 (tiếp)

- Cải tiến thao tác *CheckIn*

- Xử lý thêm hai trường hợp lỗi

```
BadCheckIn2 _____  
ΞLog  
name? : Staff  
reply! : CheckInReply  
  
name? ∉ users  
reply! = not_registered
```

30



Ví dụ 1 (tiếp)

- Cải tiến thao tác *CheckIn*
 - Khi đó

$\text{CheckInReply} == \text{ok} \mid \text{already_in} \mid \text{not_registered}$

$\text{RobustCheckIn} == \text{GoodCheckIn}$
 $\quad \vee \text{BadCheckIn1}$
 $\quad \vee \text{BadCheckIn2}$

31



Quan hệ

- **Cặp phần tử có thứ tự** được biểu diễn
 - (x, y)
- **Tích Đè-các** của hai kiểu T_1 và T_2
 - $T_1 \times T_2$
 - $(x, y) : T_1 \times T_2$

32



Quan hệ

- **Quan hệ (relation)** là tập các cặp phần tử có thứ tự

- Ví dụ:

directory = { *mary* \mapsto 287573,
mary \mapsto 398620,
john \mapsto 829483,
jim \mapsto 493028,
jane \mapsto 493028 }

directory : $\mathbb{P}(\text{Person} \times \text{Number})$

33



Quan hệ

- Có thể ký hiệu quan hệ
 - $T \leftrightarrow S = P(T \times S)$
 - *directory* : *Person* \leftrightarrow *Number*
- Ánh xạ
 - cặp phần tử có thứ tự (*x*, *y*) có thể viết $x \mapsto y$
 - Ví dụ *directory* = { *mary* \mapsto 287573,
mary \mapsto 398620,
john \mapsto 829483,
jim \mapsto 493028,
jane \mapsto 493028 }
- Lưu ý
 - Kí hiệu \leftrightarrow dành cho kiểu
 - Kí hiệu \mapsto dành cho giá trị

34



Quan hệ

o Domain và Range

- tập hợp các thành phần thứ nhất trong một quan hệ được gọi là **domain** (miền)
 - ký hiệu: *dom*
 - ví dụ:
 $dom(directory) = \{mary, john, jim, jane\}$
- tập hợp các thành phần thứ hai trong một quan hệ được gọi là **range**
 - ký hiệu: *ran*
 - ví dụ:
 $ran(directory) = \{287373, 398620, 829483, 493028\}$

35



Quan hệ

o Phép trừ miền (domain subtraction)

- ký hiệu: \triangleleft
- $S \triangleleft R$ biểu diễn quan hệ R với các phần tử trong miền S đã bị loại bỏ
- Nghĩa là:

$$S \triangleleft R = \{x \mapsto y \mid (x \mapsto y) \in R \wedge x \notin S\}$$

36



Quan hệ

- Phép trừ miền (domain subtraction)

- Ví dụ: $\text{directory} = \{ \text{mary} \mapsto 287573,$
 $\text{mary} \mapsto 398620,$
 $\text{john} \mapsto 829483,$
 $\text{jim} \mapsto 493028,$
 $\text{jane} \mapsto 493028 \}$

- Khi đó: $\{\text{mary}\} \triangleleft \text{directory} = \{ \text{john} \mapsto 829483,$
 $\text{jim} \mapsto 493028,$
 $\text{jane} \mapsto 493028 \}$

37



Ví dụ 2

- Đặc tả danh bạ điện thoại gồm tên người và số điện thoại

- Sử dụng kiểu cơ bản
 $[Person, Phone]$

- Đặc tả trạng thái hệ thống

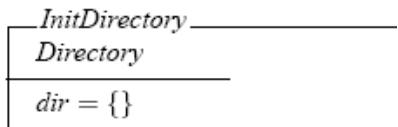
$\boxed{\begin{array}{c} \text{Directory} \\ \hline \text{dir} : \text{Person} \leftrightarrow \text{Phone} \end{array}}$

38

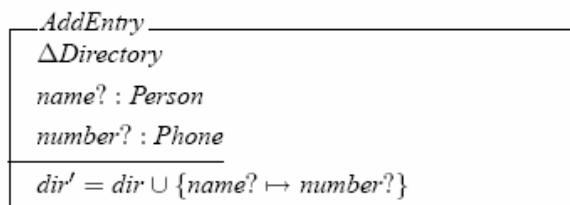


Ví dụ 2

- Khởi tạo hệ thống



- Thêm một số điện thoại

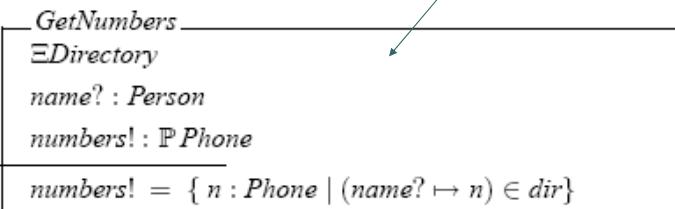


39

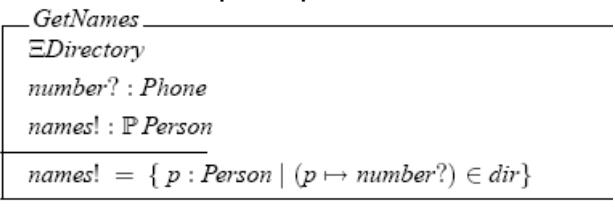


Ví dụ 2

- Tìm số điện thoại của một người



- Tìm tên theo số điện thoại



40



Ví dụ 2

- Xóa số điện thoại của một người

$$\begin{array}{l} RemoveEntry \\ \Delta\text{Directory} \\ name? : \text{Person} \\ number? : \text{Phone} \\ \hline dir' = dir \setminus \{ name? \mapsto number? \} \end{array}$$

41



Ví dụ 2

- Xóa các mục trong danh bạ ứng với một tên

$$\begin{array}{l} RemoveName \\ \Delta\text{Directory} \\ name? : \text{Person} \\ \hline dir' = \{name?\} \triangleleft dir \end{array}$$

- Xóa các mục trong danh bạ ứng với một tập các tên

$$\begin{array}{l} RemoveNames \\ \Delta\text{Directory} \\ names? : \mathbb{P} \text{Person} \\ \hline dir' = names? \triangleleft dir \end{array}$$

42



Partial Function

- là quan hệ mà mỗi phần tử trong domain cho một giá trị duy nhất trong range
- ký hiệu

$$f : X \leftrightarrow Y$$

- nghĩa là

$$\begin{aligned} f : X \leftrightarrow Y | \\ \forall a : X; \quad b_1, b_2 : Y. \\ (a \mapsto b_1) \in f \wedge (a \mapsto b_2) \in f \Rightarrow b_1 = b_2 \end{aligned}$$

43



Partial Function

- Ví dụ

$$\begin{aligned} dir1 &= \{ mary \mapsto 398620, \\ &\quad john \mapsto 829483, \\ &\quad jim \mapsto 493028, \\ &\quad jane \mapsto 493028 \} \end{aligned}$$

- Có thể áp dụng các toán tử hàm

$$\{mary, john\} \triangleleft dir1 = \{jim \mapsto 493028, \\ jane \mapsto 493028\}$$

44



Partial Function

- Toán tử *quá tải hàm* (Function Overriding)

- thay thế một mục vào bởi một mục mới
- ký hiệu

$$f \oplus \{x \mapsto y\}$$

- ví dụ

$$\text{dir1} \oplus \{\text{jim} \mapsto 567325\} = \{ \text{mary} \mapsto 398620, \\ \text{john} \mapsto 829483, \\ \text{jim} \mapsto 567325, \\ \text{jane} \mapsto 493028 \}$$

- lưu ý

$$f \oplus \{x \mapsto y\} = (\{x\} \triangleleft f) \cup \{x \mapsto y\}$$

45



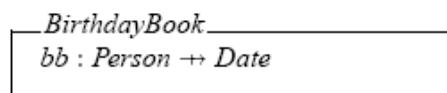
Ví dụ 3

- Đặc tả hệ thống quản lý ngày sinh

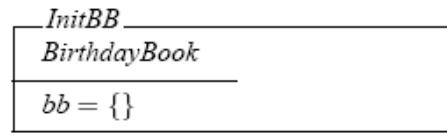
- sử dụng kiểu cơ bản mới

[Person, Date]

- mỗi người chỉ có một ngày sinh duy nhất



- khởi tạo hệ thống



46



Ví dụ 3

- Thêm một người vào hệ thống

Add
 $\Delta\text{BirthdayBook}$
 $\text{name?} : \text{Person}$
 $\text{date?} : \text{Date}$
 $\text{name?} \notin \text{dom(bb)}$
 $\text{bb}' = \text{bb} \cup \{ \text{name?} \mapsto \text{date?} \}$

47



Ví dụ 3

Điều gì xảy ra nếu $\text{name?} \notin \text{dom(bb)}$

- Chỉnh sửa ngày sinh

Update
 $\Delta\text{BirthdayBook}$
 $\text{name?} : \text{Person}$
 $\text{date?} : \text{Date}$
 $\text{bb}' = \text{bb} \oplus \{ \text{name?} \mapsto \text{date?} \}$

- Xóa một người

Remove
 $\Delta\text{BirthdayBook}$
 $\text{name?} : \text{Person}$
 $\text{bb}' = \{ \text{name?} \} \triangleleft \text{bb}$

48



Ví dụ 3

- Tìm ngày sinh của một người

```
Lookup _____  
ΞBirthdayBook  
name? : Person  
date! : Date  
  
name? ∈ dom(bb)  
date! = bb(name?)
```

49



Ví dụ 3

- Tìm ngày sinh của một người
 - trường hợp tìm không thấy

```
BadLookup _____  
ΞBirthdayBook  
name? : Person  
r! : LookupReply  
  
name? ∉ dom(bb)  
r! = notknown
```

LookupReply == ok | notknown

50



Ví dụ 3

- Tìm ngày sinh của một người
 - thông báo khi tìm thấy

$$\frac{\begin{array}{c} \text{Success} \\ \hline r! : \text{LookupReply} \end{array}}{r! = \text{ok}}$$

- khi đó

$$\begin{aligned} \text{RobustLookup} &== (\text{Lookup} \wedge \text{Success}) \\ &\vee \text{BadLookup} \end{aligned}$$

51



Ví dụ 3

- Tìm những người cùng ngày sinh

$$\frac{\begin{array}{c} \text{Who} \\ \exists \text{BirthdayBook} \\ \text{date?} : \text{Date} \\ \text{names!} : \mathbb{P} \text{Person} \end{array}}{\begin{array}{l} \text{names!} = \\ \{ p : \text{Person} \mid \\ p \in \text{dom}(bb) \wedge bb(p) = \text{date?} \} \end{array}}$$

52



Total Function

- định nghĩa ánh xạ từ tất cả giá trị của domain đến range
- ký hiệu
 $f : X \rightarrow Y$
- nghĩa là
 $f : X \leftrightarrow Y \mid \text{dom}(f) = X$

53



Total Function

- Ví dụ

$$\frac{\text{square} : \mathbb{Z} \rightarrow \mathbb{Z}}{\forall n : \mathbb{Z} \bullet \quad \text{square}(n) = n * n}$$

$$\frac{\text{factorial} : \mathbb{N} \rightarrow \mathbb{N}}{\forall i : \mathbb{N} \bullet \quad \begin{aligned} \text{factorial}(0) &= 1 \\ \text{factorial}(i + 1) &= (i + 1) * \text{factorial}(i) \end{aligned}}$$

54



Total Function

- Sử dụng để định nghĩa hằng số

$$\frac{c : T}{A}$$

- Ví dụ

$$\frac{\min_count, \max_count : \mathbb{N}}{\max_count = 100 \\ 10 \leq \min_count < \max_count}$$

55



Các ký hiệu

Toán tử lô-gíc

\wedge
 \vee
 \neg
 \Rightarrow
 $(\exists x \bullet P)$
 $(\forall x \bullet P)$

Tập hợp

$\{\dots\}$
 $\{x \mid P\}$
 \in, \notin
 \cup, \cap
 \setminus
 $\mathbb{P}S$
 \mathbb{Z}, \mathbb{N}
 $S \subseteq T$
 $S \times T$

Quan hệ và Hàm

$S \leftrightarrow T$
 $S \leftrightarrow T$
 $S \rightarrow T$
 $x \mapsto y$
 $f(x)$
 $\text{dom } f, \text{ran } f$
 $f \oplus g$
 $S \triangleleft R$

56