Đặc tả Z (5)

Nguyễn Thanh Bình
Khoa Công nghệ Thông tin
Trường Đại học Bách khoa
Đại học Đà Nẵng

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
  - Hội: $A \cup B$
  - 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
    - red : {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

Vị từ

- Có thể sử dụng các toán tử lô-gíc để định nghĩa các vị 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

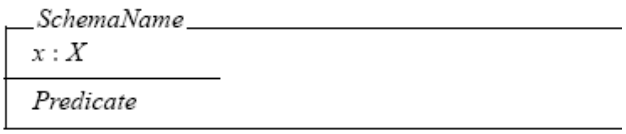
Vị từ

- 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

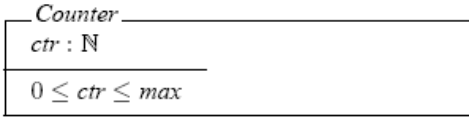
- Cấu trúc sơ đồ trạng thái gồm
  - tên sơ đồ
  - khai báo biến
  - định nghĩa vị từ



11

Sơ đồ trạng thái

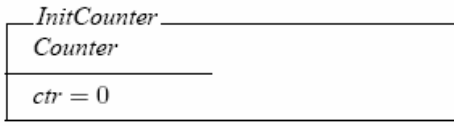
- Đặc tả Z chứa
  - các biến trạng thái
  - khởi gán biến
  - các thao tác trên các biến
  - biến trạng thái có thể có các bất biến
    - điều kiện mà luôn đúng, biểu diễn bởi các vị từ



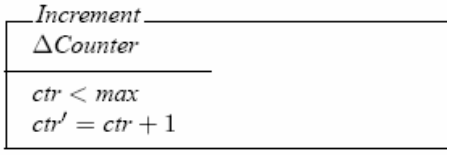
12

Sơ đồ thao tác

- Khởi gán biến



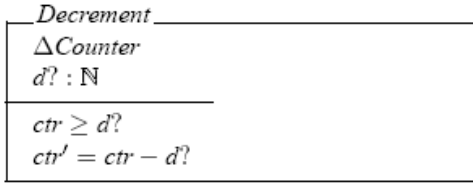
- Khai báo thao tác trên biến
  - kí hiệu Δ biểu diễn biến trạng thái bị thay đổi bởi thao tác
  - kí hiệu ‘ (dấu nháy đơn) biểu diễn giá trị mới của biến



13

Sơ đồ thao tác

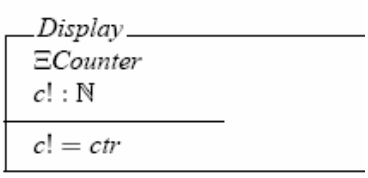
- Thao tác có thể có các tham số vào và ra
  - tên tham số vào kết thúc bởi kí tự “?”
  - tên tham số ra kết thúc bởi kí tự “!”



14

Sơ đồ thao tác

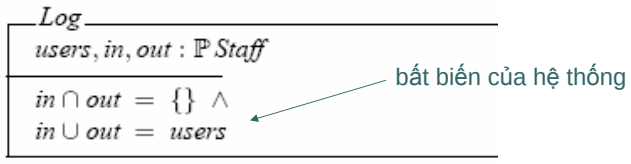
- Kí hiệu Ξ mô tả thao tác không thể thay đổi biến trạng thái



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*



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

$name? : Staff$

$name? \in in$

$out' = out \cup \{name?\}$

$in' = in \setminus \{name?\}$

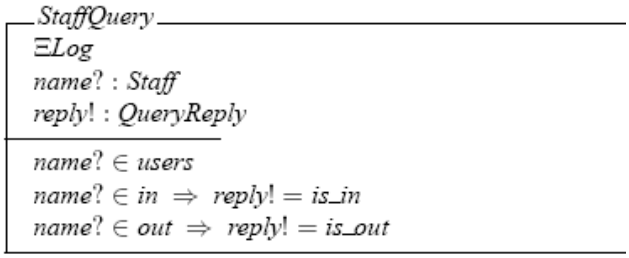
$users' = users$

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

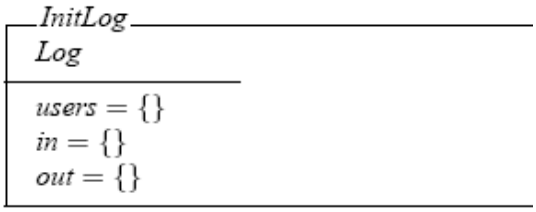
    QueryReply == is_in | is_out
  - Đặc tả thao tác



19

Ví dụ 1

- Khởi tạo hệ thống



20

Ví dụ 1

- Tóm lại
  - **Sơ đồ trạng thái:** các thành phần/đối tượng của hệ thống
  - **Bất 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
    - $name? \notin users$

StaffQuery

$$\Xi Log$$
$$name? : Staff$$
$$reply! : QueryReply$$

$$name? \in users$$
$$name? \in in \Rightarrow reply! = is\_in$$
$$name? \in out \Rightarrow reply! = is\_out$$

25

Ví dụ 1 (tiếp)

- Cải tiến thao tác *StaffQuery*
  - Đặc tả lại kiểu *QueryReply*

QueryReply == is_in | is_out | not_registered

BadStaffQuery

$$\Xi Log$$
$$name? : Staff$$
$$reply! : QueryReply$$

$$name? \notin users$$
$$reply! = not\_registered$$

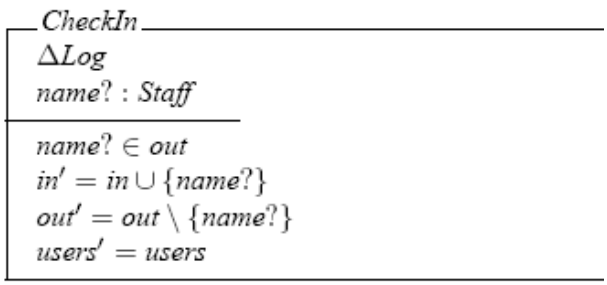
- Khi đó

RobustStaffQuery == StaffQuery ∨ BadStaffQuery

26

Ví dụ 1 (tiếp)

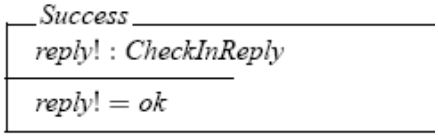
- Cải tiến thao tác *CheckIn*



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

Ví dụ 1 (tiếp)

- Cải tiến thao tác *CheckIn*
  - Mở rộng thao tác cho trường hợp ghi nhận thành công



- Khi đó

  GoodCheckIn == CheckIn ∧ Success

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

$name? : Staff$

$reply! : CheckInReply$

$name? \in in$

$reply! = already\_in$

29

Ví dụ 1 (tiếp)

- Cải tiến thao tác *CheckIn*
  - Xử lý thêm hai trường hợp lỗi

BadCheckIn2

ΞLog

$name? : Staff$

$reply! : CheckInReply$

$name? \notin users$

$reply! = not\_registered$

30

Ví dụ 1 (tiếp)

- Cải tiến thao tác *CheckIn*
  - Khi đó

CheckInReply == ok | already_in | not_registered

RobustCheckIn == GoodCheckIn
∨ BadCheckIn1
∨ BadCheckIn2

31

Quan hệ

- **Cặp phần tử có thứ tự** được biểu diễn
  - *(x, y)*
- **Tích Đề-các** của hai kiểu T1 và T2
  - *T1 x T2*
  - *(x, y) : T1 x T2*

32

Quan hệ

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

$$\begin{aligned} directory \quad = \quad & \{ \, mary \mapsto 287573, \\ & mary \mapsto 398620, \\ & john \mapsto 829483, \\ & jim \mapsto 493028, \\ & jane \mapsto 493028 \, \} \end{aligned}$$

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

33

Quan hệ

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

34

Quan hệ

- **Domain** và **Range**
  - tập hợp các thành phần thứ nhất trong một quan hệ được gọi là **domain** (miền)
    - kí 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**
    - kí hiệu: *ran*
    - ví dụ:
      ran(directory) = {287373, 398620, 829483, 493028}

35

Quan hệ

- Phép trừ miền (domain subtraction)
  - ký hiệu: $\lhd$
  - $S \lhd R$ biểu diễn quan hệ R với các phần tử trong miền S đã bị loại bỏ
  - Nghĩa là:

$$S \lhd R = \{ x \mapsto y \mid (x \mapsto y) \in R \land x \notin S \}$$

36

Quan hệ

- Phép trừ miền (domain subtraction)
  - Ví dụ: $directory = \{ mary \mapsto 287573, mary \mapsto 398620, john \mapsto 829483, jim \mapsto 493028, jane \mapsto 493028 \}$
  - Khi đó: $\{mary\} \lhd directory = \{ john \mapsto 829483, jim \mapsto 493028, jane \mapsto 493028 \}$

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

    Directory

    $dir : Person \leftrightarrow Phone$

38

Ví dụ 2

- Khởi tạo hệ thống

InitDirectory

$Directory$

$dir = \{\}$

- Thêm một số điện thoại

AddEntry

$\Delta Directory$

$name? : Person$

$number? : Phone$

$dir' = dir \cup \{name? \mapsto number?\}$

39

Ví dụ 2

có thể cải tiến ?

- Tìm số điện thoại của một người

GetNumbers

$\Xi Directory$

$name? : Person$

$numbers! : \mathbb{P}\, Phone$

$numbers! = \{ n : Phone \mid (name? \mapsto n) \in dir \}$

- Tìm tên theo số điện thoại

GetNames

$\Xi Directory$

$number? : Phone$

$names! : \mathbb{P}\, Person$

$names! = \{ p : Person \mid (p \mapsto number?) \in dir \}$

40

Ví dụ 2

- Xóa số điện thoại của một người

RemoveEntry

$\Delta Directory$

$name? : Person$

$number? : Phone$

$dir' = dir \setminus \{ name? \mapsto number? \}$

Ví dụ 2

- Xóa các mục trong danh bạ ứng với một tên

RemoveName

$\Delta Directory$

$name? : Person$

$dir' = \{name?\} \lhd dir$

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

RemoveNames

$\Delta Directory$

$names? : \mathbb{P}\, Person$

$dir' = names? \lhd dir$

Partial Function

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

$$f : X \nrightarrow Y$$

- nghĩa là

$$f : X \leftrightarrow Y \mid \\ \forall a : X; \quad b_1, b_2 : Y \cdot \\ (a \mapsto b_1) \in f \land (a \mapsto b_2) \in f \quad \Rightarrow \quad b_1 = b_2$$

43

Partial Function

- Ví dụ

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

- Có thể áp dụng các toán tử hàm

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

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

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

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

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

    BirthdayBook

    $bb : Person \pfun Date$
  - khởi tạo hệ thống

    InitBB

    BirthdayBook

    $bb = \{\}$

46

Ví dụ 3

- Thêm một người vào hệ thống

Add

$\Delta BirthdayBook$

$name? : Person$

$date? : Date$

$name? \notin \mathrm{dom}(bb)$

$bb' = bb \cup \{ name? \mapsto date? \}$

47

Ví dụ 3

Điều gì xảy ra nếu name? ∉ dom(bb)

- Chỉnh sửa ngày sinh

Update

$\Delta BirthdayBook$

$name? : Person$

$date? : Date$

$bb' = bb \oplus \{ name? \mapsto date? \}$

- Xóa một người

Remove

$\Delta BirthdayBook$

$name? : Person$

$bb' = \{ name? \} \lhd bb$

48

Ví dụ 3

- Tìm ngày sinh của một người

Lookup

$\Xi BirthdayBook$

$name? : Person$

$date! : Date$

$name? \in \mathrm{dom}(bb)$

$date! = bb(name?)$

Ví dụ 3

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

BadLookup

$\Xi BirthdayBook$

$name? : Person$

$r! : LookupReply$

$name? \notin \mathrm{dom}(bb)$

$r! = notknown$

$LookupReply == ok \mid notknown$

Ví dụ 3

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

Success

$r! : LookupReply$

$r! = ok$

  - khi đó

$$RobustLookup == (Lookup \land Success) \lor BadLookup$$

51

Ví dụ 3

- Tìm những người cùng ngày sinh

Who

$\Xi BirthdayBook$

$date? : Date$

$names! : \mathbb{P}\, Person$

$$names! = \{ p : Person \mid p \in \mathrm{dom}(bb) \land bb(p) = date? \}$$

52

Total Function

- định nghĩa ánh xạ từ tất cả giá trị của domain đến range
- ký hiệu

$$f : X \rightarrow Y$$

- nghĩa là

$$f : X \nrightarrow Y \mid \mathrm{dom}(f) = X$$

53

Total Function

- Ví dụ

$$square : \mathbb{Z} \rightarrow \mathbb{Z}$$

$$\forall n : \mathbb{Z} \bullet square(n) = n * n$$

$$factorial : \mathbb{N} \rightarrow \mathbb{N}$$

$$\forall i : \mathbb{N} \bullet factorial(0) = 1 \quad factorial(i+1) = (i+1) * factorial(i)$$

54

Total Function

- Sử dụng để định nghĩa hằng số

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

- Ví dụ

$$\frac{min\_count, max\_count : \mathbb{N}}{\begin{array}{l} max\_count = 100 \\ 10 \leq min\_count < max\_count \end{array}}$$

55

Các ký hiệu

Toán tử lô-gíc

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

Tập hợp

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

Quan hệ và Hàm

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

56