

1. Introduction à B

- B pour Bourbaki
- 1978 : notation Z (Jean-Raymond Abrial)
- 1991 : les premiers pas de la méthode B (J-R Abrial)
- 1995 : industrialisation de la méthode B
L'exemple industriel Météor
 - RER
 - Plus de 1000 composants B (>100 000 lignes de B)
 - 87 000 lignes de code ADA générées
 - 29 000 preuves (dont plus de 80% automatique)
 - Opérationnel depuis 1998, aucune anomalie depuis !

Fondements mathématiques avec un cadre homogène pour tout le cycle de développement (analyse, conception et réalisation)

Approche :

Raffiner le modèle initial d'une machine abstraite (sa spécification) en un module exécutable (son code).

Validation basée sur des preuves :

- Preuve de la spécification de chaque opération.
- Preuve du raffinement d'une machine en une autre.

Langage de modélisation :

- Abstraction du système
- Changement d'états du système
- Spécification des invariants du système (à vérifier)

Exemple de machine abstraite

MACHINE

réserve(*max_siège*)

VARIABLES

siège

INVARIANT

$siège \in 0..max_siège$

INITIALISATION

siège := *max_siège*

OPERATIONS

réserver \triangleq

PRE *siège* > 0

THEN *siège* := *siège* - 1

END ;

annuler \triangleq

PRE *siège* < *max_siège*

THEN *siège* := *siège* + 1

END ;

END

2. Éléments de bases de la méthode B

Ensemble, Relation & Fonction, Entier, Suite,
Substitution (simple / multiple)

Ensemble (notation ASCII)

$e1$ et en représentent des expressions quelconques (entiers, ensembles,...)

Id représente un identificateur

$n1$ et $n2$ sont des expressions qui représentent des entiers

$\{\}$ Ensemble vide

NAT Ensemble des entiers

$NAT1$ Ensemble des entiers non nuls

$\{e1, \dots, en\}$ Ensemble des éléments $e1, \dots, en$ (définition par extension)

$\{Id \mid \text{Prédicats}\}$ Ensemble défini par compréhension

$(n1..n2)$ Ensemble des entiers compris entre $n1$ et $n2$

Ensemble (notation ASCII)

E , $E1$ et $E2$ représentent des ensembles.

$POW(E)$ Ensemble des parties de E

$POW1(E)$ Ensemble des parties non vides de E

$E1 * E2$ Produit cartésien

$E1 \vee E2$ Union des ensembles $E1$ et $E2$

$E1 \wedge E2$ Intersection des ensembles $E1$ et $E2$

$E1 - E2$ Ensemble des éléments de $E1$ qui ne sont pas dans $E2$

Formule élémentaire (notation ASCII)

$e, e1$ et $e2$ représentent des expressions quelconques (entiers, ensembles,...)

$n1$ et $n2$ sont des expressions qui représentent des entiers

$E, E1$ et $E2$ représentent des ensembles.

$e1=e2$ $n1>n2$ $n1<n2$ $e1 \neq e2$ $n1 \geq n2$ $n1 \leq n2$ No comment !

$e:E$ L'expression e est un objet de l'ensemble E (appartenance)

$e!:E$ L'expression e n'est pas un objet de l'ensemble E

$E1 \subset: E2$ $E1$ est un sous-ensemble de $E2$ (inclusion)

$E1 \not\subset: E2$ $E1$ n'est pas un sous-ensemble de $E2$.

$E1 \subset\subset: E2$ $E1$ est un sous-ensemble strict de $E2$ (inclusion stricte).

$E1 \not\subset\subset: E2$ $E1$ n'est pas un sous-ensemble strict de $E2$.

Formule composée (notation ASCII)

F, F1 et F2 représentent des formules.

$\text{not}(F)$	négation
$F1 \ \& \ F2$	conjonction
$F1 \ \text{or} \ F2$	disjonction
$F1 \Rightarrow F2$	implication
$F1 \Leftrightarrow F2$	équivalence
$\# \text{ var} . F$	quantification existentielle
$! \text{ var} . F$	quantification universelle

Relation (notation ASCII)

$E, E1, E2$ et $E3$ représentent des ensembles.

$R, R1$ et $R2$ représentent des relations.

$E1 \leftrightarrow E2$ Ensemble des relations entre éléments de $E1$ et de $E2$

$dom(R)$ Le domaine de la relation R

$ran(R)$ L'image de la relation R (codomaine ou range)

$R[E]$ L'image de l'ensemble E par la relation R

$R1 ; R2$ Composition des relations $R1$ et $R2$

$id(E)$ Relation identité sur l'ensemble E

$R\sim$ Relation inverse de R

Exemple :

$E1 = \{a, b, c\}$ $E2 = \{A, B, C\}$ $R1: E1 \leftrightarrow E2$ $R1 = \{(a, A), (a, B), (b, B)\} = \{a \rightarrow A, a \rightarrow B, b \rightarrow B\}$
 $E3 = \{x, y, z\}$ $R2: E2 \leftrightarrow E3$ $R2 = \{(A, x), (A, y), (B, y), (C, z)\}$

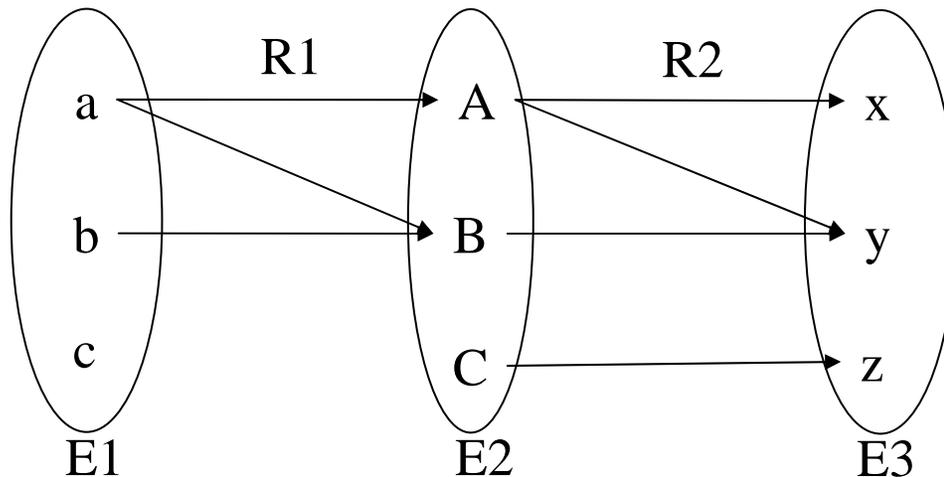
Donnez $dom(R1)$, $ran(R1)$, $R1[\{b, c\}]$, $R1;R2$ et $R1\sim$.

Exemple (solution)

$E1 = \{a, b, c\}$ $E2 = \{A, B, C\}$ $E3 = \{x, y, z\}$

$R1: E1 \leftrightarrow E2$ $R1 = \{(a, A), (a, B), (b, B)\} = \{a \mapsto A, a \mapsto B, b \mapsto B\}$

$R2: E2 \leftrightarrow E3$ $R2 = \{(A, x), (A, y), (B, y), (C, z)\}$



$\text{dom}(R1) = \{a, b\}$

$\text{ran}(R1) = \{A, B\}$

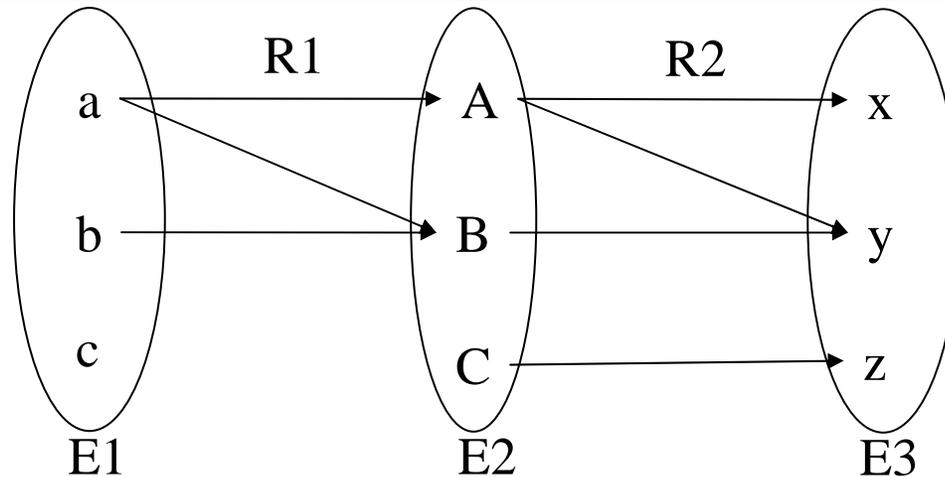
$R1[\{b, c\}] = \{B\}$

$R1; R2 = \{(a, x), (a, y), (b, y)\}$

$R1 \sim = \{(A, a), (B, a), (B, b)\}$

Donnez $\text{dom}(R2)$, $\text{ran}(R2)$, $R2[\{A\}]$ et $(R2 \sim); (R1 \sim)$.

Exemple - solution



Donnez $\text{dom}(R2)$, $\text{ran}(R2)$, $R2[\{A\}]$ et $(R2\sim);(R1\sim)$.

$$\text{dom}(R2) = \{A, B, C\}$$

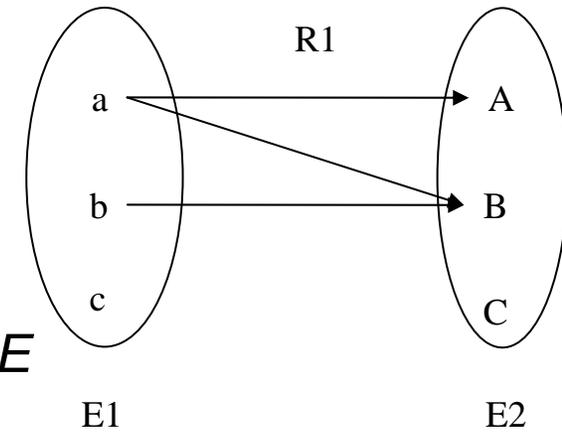
$$\text{ran}(R2) = \{x, y, z\}$$

$$R2[\{A\}] = \{x, y\}$$

$$R1\sim = \{(A, a), (B, a), (B, b)\} \quad R2\sim = \{(x, A), (y, A), (y, B), (z, C)\}$$

$$(R2\sim);(R1\sim) = \{(x, a), (y, a), (y, b)\}$$

Relation (notation ASCII)



E représente un ensemble

R représente une relation

$E <| R$ Restriction de la relation R au domaine E

Exemple: $\{b,c\} <| R1 = \{b \rightarrow B\}$

$R |> E$ Restriction de la relation R à l'image E

Exemple: $R1 |> \{B,C\} = \{a \rightarrow B, b \rightarrow B\}$

$E <<| R$ Anti-restriction de la relation R au domaine E

Exemple: $\{b,c\} <<| R1 = \{a \rightarrow A, a \rightarrow B\}$

$R |>> E$ Anti-restriction de la relation R à l'image E

Exemple: $R1 |>> \{B,C\} = \{a \rightarrow A\}$

Fonction (notation ASCII)

E , $E1$ et $E2$ représentent des ensembles.

$E1 \leftrightarrow E2$ l'ensemble des fonctions partielles de $E1$ dans $E2$

- $\{R \mid R \in E1 \leftrightarrow E2 \wedge \forall x,y,z \cdot ((x \mapsto y) \in R \wedge (x \mapsto z) \in R) \Rightarrow y = z\}$

$E1 \rightarrow E2$ l'ensemble des fonctions totales de $E1$ dans $E2$

- $\{R \mid R \in E1 \leftrightarrow E2 \wedge \text{dom}(R) = E1\}$

$E1 \rightarrow+ E2$ l'ensemble des fonctions partielles injectives de $E1$ dans $E2$

- $\{R \mid R \in E1 \leftrightarrow E2 \wedge R^{-1} \in E2 \leftrightarrow E1\}$

$E1 \rightarrow- E2$ l'ensemble des fonctions totales injectives de $E1$ dans $E2$

- $(E1 \rightarrow+ E2) \cap (E1 \rightarrow- E2)$

Fonction (notation ASCII)

E , $E1$ et $E2$ représentent des ensembles.

$E1 \dashrightarrow E2$ l'ensemble des fonctions partielles surjectives de $E1$ dans $E2$

- $\{R \mid R \in E1 \dashrightarrow E2 \wedge \text{ran}(R) = E2\}$

$E1 \twoheadrightarrow E2$ l'ensemble des fonctions totales surjectives de $E1$ dans $E2$

- $(E1 \dashrightarrow E2) \cap (E1 \twoheadrightarrow E2)$

$E1 \xrightarrow{+} E2$ l'ensemble des fonctions totales bijectives de $E1$ dans $E2$

- $(E1 \xrightarrow{+} E2) \cap (E1 \twoheadrightarrow E2)$

$E1 \xrightarrow{-} E2$ l'ensemble des fonctions partielles bijectives de $E1$ dans $E2$

- $(E1 \xrightarrow{+} E2) \cap (E1 \dashrightarrow E2)$

Substitution simple / multiple

x, x_1, \dots, x_n sont des variables distinctes, et e, e_1, \dots, e_n des expressions quelconques

$x := e$ *Substitution simple (une affectation)*

$x_1, \dots, x_n := e_1, \dots, e_n$ *Substitution multiple*

Suite (ou séquence)

s_1, s_2 représentent des séquences et e, e_1, \dots, e_n des expressions quelconques

$seq(E)$ L'ensemble des séquences finies d'objets de E

$\langle \rangle$ La séquence vide

$[e]$ La séquence réduite à un élément e

$[e_1, \dots, e_n]$ La séquence formée des n éléments e_1, \dots, e_n

$s_1 \wedge s_2$ La concaténation des séquences s_1 et s_2

$e \rightarrow s$ L'ajout de e au début de la séquence s

$s \leftarrow e$ L'ajout de e à la fin de la séquence s

$first(s)$ $last(s)$ Le premier/dernier élément de la séquence non-vide s

$tail(s)$ $front(s)$ La séquence non-vide s privée de son premier/dernier élément

$size(s)$ La taille de la séquence s