# Plan

**Méthode B.**

# 1. Introduction

# Historique

- 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 !

# Méthode

Fondements mathématiques :

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 raffinage 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**
*réservation(max_siège)*

**VARIABLES**

*siège*

**INVARIANT**

*siège* ∈ *0..max_siège*

**INITIALISATION**

*siège:=max_siège*

**OPERATIONS**
*réserver* ≙

PRE *siège* > *0*

THEN *siège := siège-1*

END;

*annuler* ≙

PRE *siège* < *max_siège*

THEN *siège := siège+1*

END;

**END**

# 2. Eléments de bases de la méthode B

Ensemble, Relation & Fonction, Entier, Suite, substitution

# 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 |
| {*e*1,...,*en*} | Ensemble des éléments *e*1,...,*en* (définition par extension) |
| {Id \| Prédicats} | Ensemble défini par compréhension |
| (*n*1..*n*2) | Ensemble des entiers compris entre *n*1 et *n*2 |

# 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* |
| *E*1 * *E*2 | Produit cartésien |
| *E*1 \/ *E*2 | Union des ensembles *E*1 et *E*2 |
| *E*1 /\ *E*2 | Intersection des ensembles *E*1 et *E*2 |
| *E*1 - *E*2 | Ensemble des éléments de *E*1 qui ne sont pas dans *E*2 |

# 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 /= e2 n1 >= n2 n1 <= 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* |
| *E*1 <: *E*2 | *E*1 est un sous-ensemble de *E*2 (inclusion) |
| *E*1 /<: *E*2 | *E*1 n'est pas un sous-ensemble de *E*2. |
| *E*1 <<: *E*2 | *E*1 est un sous-ensemble strict de *E*2 (inclusion stricte). |
| *E*1 /<<: *E*2 | *E*1 n'est pas un sous-ensemble strict de *E*2. |

# Formule composée (notation ASCII)

*F, F1 et F2 représentent des formules.*

| | |
|---|---|
| not(F) | négation |
| F1 & F2 | conjonction |
| F1 or F2 | disjonction |
| F1 => F2 | implication |
| F1 <=> F2 | équivalence |
| # var . F | quantification existentielle |
| ! var . F | quantification universelle |

# Relation (notation ASCII)

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

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

| | |
|---|---|
| *E1 <-> 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~* | *Relation inverse de R* |

# Exemple

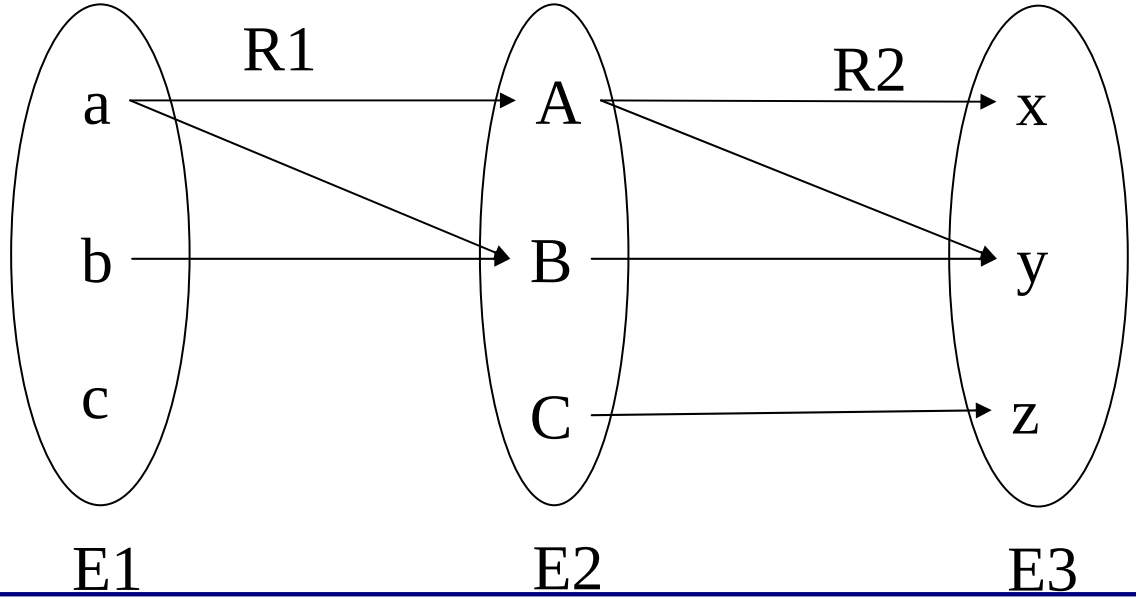
R1:E1<->E2 R1={(a,A),(a,B),(b,B)} = {a|->A,a|->B,b|->B}

R2:E2<->E3 R2={(A,x), (A,y), (B,y), (C,z)}

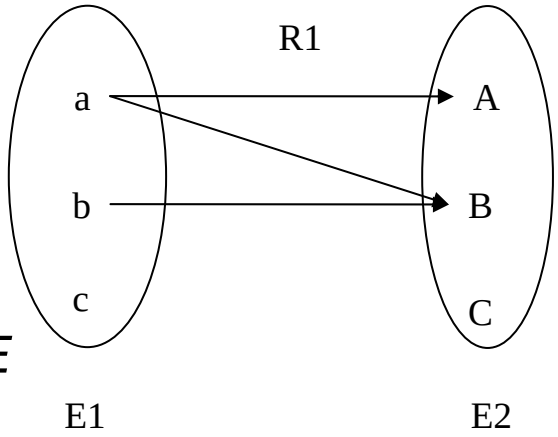
dom(R1)={a,b} ran(R1)={A,B} R1[{b,c}]={B}

R1;R2={(a,x),(a,y),(b,y)} R1~={(A,a),(B,a),(B,b)}

Donnez dom(R2), ran(R2), R2[{A}] et (R2~);(R1~).



# 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|->B}*

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

*Exemple: R1|>{B,C}={a|->B , b|->B}*

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

*Exemple: {b,c}<<|R1={a|->A , a|->B}*

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

*Exemple: R1|>>{B,C}={a|->A }*

# Fonction (notation ASCII)

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

*E1 +-> E2* *l'ensemble des fonctions partielles de E1 dans E2*

- {R | R ∈ E1 <-> E2 ∧ ∀ x,y,z • (((x ↦ y) ∈ R ∧ (x ↦ z) ∈ R) ⇒ y = z)}

*E1 --> E2* *l'ensemble des fonctions totales de E1 dans E2*

- {R | R ∈ E1 +-> E2 ∧ dom(R) = E1}

*E1 >+> E2* *l'ensemble des fonctions partielles injectives de E1 dans E2*

- {R | R ∈ E1 +-> E2 ∧ $R^{-1}$ ∈ E2 +-> E1}

*E1 >-> E2* *l'ensemble des fonctions totales injectives de E1 dans E2*

- (E1 >+> E2) ∩ (E1 --> E2)

# Fonction (notation ASCII)

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

*E1 +->> E2* *l'ensemble des fonctions partielles surjectives de E1 dans E2*

- {R | R ∈ E1 +-> E2 ∧ ran(R) = E2}

*E1 -->> E2* *l'ensemble des fonctions totales surjectives de E1 dans E2*

- (E1 +->> E2) ∩ (E1 --> E2)

*E1 >+>> E2* *l'ensemble des fonctions totales bijectives de E1 dans E2*

- (E1 >-> E2) ∩ (E1 -->> E2)

*E1 >->> E2* *l'ensemble des fonctions partielles bijectives de E1 dans E2*

- (E1 >+> E2) ∩ (E1 +->> E2)