# 5. Raffinement

# Principes du raffinement

Technique utilisée au cours du processus de développement logiciel

But :

Transformer un modèle abstrait d'un système logiciel (la spécification) en un modèle plus concret, c'est-à-dire un modèle plus près d'une implémentation.

Démarche de conception formelle :

- On se donne une spécification formelle SP1 qui exprime en toute abstraction ce que le programme doit réaliser
- Génération progressive du code du programme : SP1 -> SP2 -> … ->SPn
- Correction de chacune des étapes de raffinement

# Exemple de raffinement

Tri par ordre croissant d'un tableau Tab d'entiers de taille n. Le résultat sera dans Tab_Trié.

- **Spécification (ou spécification abstraite)** : on donne les propriétés du tableau trié sans faire allusion à aucun algorithme ou méthode de tri.
  - les éléments de Tab et Tab_Trié sont les mêmes
  - pour chaque indice i (i=2..n): Tab_Trié [i-1] <=Tab_Trié[i]
- **Implémentation (ou spécification concrète)** : mettre en œuvre une des méthodes de tri existantes

# Raffinement et B

Lors d'un raffinement,

- une machine M1 est remplacée par une autre machine M2
- M2 va fournir des opérations de même nom et de même signature
- Les opérations de M2 seront implantées à l'aide de variables d'états différentes

**Conservation de la Cohérence** :

- Si une opération op2 est un raffinement d'une opération op1 alors toute utilisation de op1 doit pouvoir être remplacée par une utilisation de op2, sans changer la cohérence de la machine.

# Exemple de Raffinement en B

```
MACHINE swap
VARIABLES xx,yy
INVARIANT
  xx:NAT & yy:NAT
INITIALISATION
xx::NAT||yy::NAT
OPERATIONS
  echange =
    BEGIN
      xx:=yy||yy:=xx
    END
END
/*Où ‘::’ désigne un choix
   indéterministe d'un
   élément d'un ensemble
   (xx::NAT)*/
```

```
REFINEMENT swapR
REFINES swap
VARIABLES xr, yr, zr
INVARIANT
xr= xx & yr = yy &
zr : NAT
INITIALISATION
  xr,yr,zr:=0,0,0
OPERATIONS
  echange =
    BEGIN
      zr := xr;
      xr := yr;
      yr := zr
    END
END
```

# Contraintes à satisfaire lors d'un raffinement

La machine **swapR** est un raffinement de la machine **swap**

- Les variables abstraites **xx,yy** sont raffinées par les variables concrètes **xr,yr,zr**.
- Les variables concrètes contiennent :
  - Les variables abstraites conservées par le raffinement (**xx,yy**)
  - Des variables concrètes introduites par le raffinement (**xr,yr,zr**)
- L'invariant de collage (**xr=xx&yr=yy&zr:NAT**) permet de :
  - typer les variables concrètes introduites par le raffinement
  - exprimer des propriétés sur les variables concrètes
  - exprimer la relation liant les variables concrètes aux variables abstraites
- L'initialisation concrète (**xr,yr,zr:=0,0,0**) est le raffinement de l'initialisation abstraite (**xx::NAT||yy::NAT**).
- L'opération abstraite **echange** est raffinée par l'opération concrète **echange** de même signature.