

Propos de banc de touche

Guy Laffitte

May 9, 2025

1 Au stade de Vertou

1.1 Premier matin

Le vent était favorable. L'usine de la BN (Biscuiterie Nantaise) nous offrait de bonnes odeurs de biscuits. Et Guy a répondu à nos questions alors que le petit-fils était à l'entraînement de foot à la française.

- H.H. : Tu as connu J.R. Abrial lorsque tu as suivi un stage au CEPIA sur le Domaine de Voluceau à Rocquencourt. C'était en quelle année ?
- G.L. : En octobre 1985.
- H.H. : J'y étais aussi en octobre et au printemps. On aurait pu s'y rencontrer. Mais on ne se connaissait pas encore. Qu'est-ce qui t'a alors plu ?
- G.L. : Point fort : au lieu d'essayer vainement de faire une preuve sur un programme quelconque, on commence par faire une spécification que l'on peut prouver, puis on ne s'intéresse qu'aux programmes implémentant la spécification.
 - H.H. : J.R. Abrial te remercie dans le B-Book pour ton apport. Tu me racontes.
 - G.L. : Je travaillais à l'INSEE boulevard Adolphe-Pinard dans le 14^e.
 - H.H. : Adolphe Pinard ! ma mère m'a légué un livre d'Adolphe Pinard ! Revenons à la population. Mais avec Adolphe Pinard nous y sommes. C'est à Nantes que nous avons le fichier de la population, et le NNI me servait d'exercice pour l'apprentissage de B ! Quand j'étais au service informatique de la mairie, je me souviens avoir appris qu'à la naissance, quand le sexe est indéterminé (on attend la chute des testicules. A-t-on pris en compte la propriété de fatalité ?) le code sexe est mis égal à 1. A mon époque, la seule modification était le passage à 1.)
 - G.L. : et ce n'était pas loin de chez lui qui habitait à l'adresse qui apparaissait dans ses articles, au 26 rue des Plantes{indexrue des Plantes, un immeuble style Art déco, composé d'ateliers d'artistes en duplex avec l'atelier en partie

basse, chambre et cuisine, séjour en mezzanine, avec des baies de double hauteur. Max Ernst y a vécu. Marx Ernst c'est celui qui a illustré mon "Logique sans peine" (édition de 1966) de Lewis Carroll, publié par Hermann, l'éditeur du premier Bourbaki. Tu me rappelles des souvenirs. Si ma mémoire est bonne, il y a une plaque à la mémoire de Jean Moulin qui y avait loué un studio.

- G.L. : Oui. Je pouvais aller à pied de l'INSEE à la rue des plantes, Nous avons pu ainsi discuter.
- H.H. : Quels ont été tes apports ?
- G.L. : Apports théoriques.
 - * Obligation de preuve de l'initialisation.
 - * Boucle Introduction p. 377 et 378 du B-Book. Version initiale (duale) du Th. 9.2.1 p. 379 avec des unions à la place des intersections : simplification drastique des hypothèses.
- B-Tool.
 - * Amélioration de la machine de suites.
 - * Expertise de non plagiat entre la version initiale (appartenant à BP) et la nouvelle version (STERIA à l'époque).
 - * Analyse d'une nouvelle version de l'analyseur syntaxique, un automate à pile d'inspiration LR remplaçant une descente récursive. Subtilités : génération de polonaise inverse saturée et insertion d'opérateurs implicites (substitution et évaluation).
- H.H. : Tu pourras nous en parler lors de la journée ? Et de ton application de B au recensement de la population. Tu en avais fait une présentation aux étudiants. Je me souviens de l'étude de la géographie administrative.
- G. L.: D'accord.
 - * Outils pour le Recensement de la Population 1990 ¹
 - * Utilisation systématique du B-Tool pour l'analyse syntaxique des outils et la génération de code (Pascal).
 - * TRANS_xx . Outil de stockage de données au moyen de mémoires virtuelles rémanentes et de machines de suites sur une idée initiale de JRA.
 - * Notions de base, de système et d'application.
 - * Notion de base miroir.
 - * Développement sur Unix, portable sur IBM OS et DPS7.

¹Bernard, P., Laffitte, G. (1995). *The French population census for 1990*. In: Bowen, J.P., Hinchey, M.G. (eds) ZUM '95: The Z Formal Specification Notation. ZUM 1995. Lecture Notes in Computer Science, vol 967. Springer, Berlin, Heidelberg

1.2 Deuxième mercredi matin au stade de Vertou

- H.H. : Je t'ai apporté le livre B événementiel.
- G.L. : Merci je ne connais pas le B événementiel. J'ai fouillé dans mes archives et j'ai trouvé des choses.
- H.H. : Pour le B événementiel, je comprends bien qu'à l'INSEE ce n'était pas un domaine d'application. Ce serait bien de nous présenter ça.
- H.H. : Ce serait bien de nous présenter ça.
- G.L. : J'ai traité un sujet qu'on ne trouve pas dans les livres. Le voici :

Une ménagère possède une pile de torchons dans un placard. Les torchons sont tous identiques. En fonction de ses besoins, la ménagère prend un ou plusieurs torchons sur le dessus de la pile. De temps à autre, elle fait sa lessive. Les torchons lavés, séchés puis pliés sont mis en une pile qu'elle range EN DESSOUS de la pile des torchons non utilisés. Cette manière de faire semble clairement meilleure que de les ranger par dessus afin répartir au mieux l'usure des torchons. Que pouvez-vous en dire ?
Indications :

- l'approche statistique semble vouée à l'échec dès le départ au vu des problèmes de combinatoire,
- une approche de type "invariant" permet d'arriver à un résultat non trivial.

Depuis la dernière fois j'ai retrouvé ça dans mes archives.

MODEL

 fifo.1 (Max, XX)

CONSTRAINTS

 Max : NAT &

 Max ≥ 2 &

 XX $\neq \{\}$

VARIABLES

 in1, out1, tab1

INVARIANT

 in1 : NATURAL1 &

 out1 : NATURAL1 &

 out1 \leq in1 &

 in1 \leq out1 + Max &

 tab1 : (1 .. (in1 - 1)) \rightarrow XX

INITIALISATION

```

in1 := 1 ||
out1 := 1 ||
tab1 := {}
OPERATIONS
  ll ← long ≐
  BEGIN
    ll := in1 - out1
  END ;
  add ( xx ) ≐
  PRE
    xx : XX &
    in1 + 1 ≤ out1 + Max
  THEN
    tab1(in1) := xx ||
    in1 := in1 + 1
  END ;
  xx ← rmv ≐
  PRE
    out1 + 1 ≤ in1
  THEN
    xx := tab1(out1) ||
    out1 := out1 + 1
  END
END

REFINEMENT
  fifo_2 (Max, XX)
REFINES
  fifo_1
VARIABLES
  in2, out2, tab2
INVARIANT
  in2 = in1 &
  out2 = out1 &
  tab2 : (0 .. Max - 1) → XX &
  ! adr · (adr : (out1 .. in1 - 1) ⇒ tab1(adr) = tab2(adr mod Max))
INITIALISATION
  in2 := 1 ||
  out2 := 1 ||
  tab2 :: (0 .. Max - 1) → XX

```

OPERATIONS

```
ll  $\leftarrow$  long  $\hat{=}$ 
BEGIN
  ll := in2 - out2
END ;
add ( xx )  $\hat{=}$ 
BEGIN
  tab2(in2 mod Max) := xx ||
  in2 := in2 + 1
END ;
xx  $\leftarrow$  rmv  $\hat{=}$ 
BEGIN
  xx := tab2(out2 mod Max) ||
  out2 := out2 + 1
END
```

END

REFINEMENT

```
fifo_3 (Max, XX)
```

REFINES

```
fifo_2
```

VARIABLES

```
in3, out3, tab3
```

INVARIANT

```
out3 = out2 mod Max &
in3 = out3 + in2 - out2 &
tab3 = tab2
```

INITIALISATION

```
in3 := 1 ;
out3 := 1 ;
tab3 :: (0 .. Max - 1)  $\rightarrow$  XX
```

OPERATIONS

```
ll  $\leftarrow$  long  $\hat{=}$ 
BEGIN
  ll := in3 - out3
END ;
add ( xx )  $\hat{=}$ 
BEGIN
  IF in3 < Max THEN
```

```

        tab3(in3) := xx
    ELSE
        tab3(in3 - Max) := xx
    END ;
    in3 := in3 + 1
END ;
xx  $\longleftarrow$  rmv  $\hat{=}$ 
BEGIN
    xx := tab3(out3) ;
    out3 := out3 + 1 ;
    IF out3 = Max THEN
        in3 := in3 - Max ;
        out3 := out3 - Max
    END
END
END

```

et ce cas "hybride"

Boucle contenant un corps non-déterministe.

```

Programme HYBRIDE(x : INTEGER)
WHILE x  $\neq$  0 DO
    IF x > 0 THEN
        x := x - 1
    ELSE
        x :: {y | y : INTEGER & y > x }
    ENDIF
INVARIANT
    x : INTEGER
VARIANT
    ?
ENDWHILE

```

```

Programme SYRACUSE(x : NAT1)
WHILE x > 1 DO
    IF pair(x) THEN
        x := x / 2
    ELSE
        x := 3 * x + 1
    ENDIF
ENDWHILE

```

Note 1 : INTEGER désigne les entiers relatifs (Z en maths).

Note 2 : Le symbole "::" désigne l'affectation non-déterministe d'un élément de l'ensemble à sa droite vers la variable à sa gauche.

Avec un choix judicieux du variant, la boucle se termine toujours. Par contre, si la valeur de départ est négative, on ne peut pas borner le nombre d'itérations en fonction de la valeur initiale.

1.3 Citation de G. Laffitte sur le recensement en B

J'avais oublié que j'avais ce texte, pp. 287-288 de *Introduction à la spécification*, H. Habrias, Masson, 1993 !

La méthode et l'outil B ont été utilisés pour la préparation du recensement général de la population de 1990. Les données du recensement ont été organisées en machines abstraites, ou systèmes, eux-mêmes structurés en bases (une base correspond à la notion de fichier en accès direct). Les principaux systèmes réalisés ont été les suivants :

- Le système géographique qui contient toutes les informations relatives aux différents découpages administratifs ou d'étude, y compris les relations qui les unissent et leurs dénominations. Ce système constitue un module par lui-même autonome des données du recensement proprement dit.
- Un système par enquête du recensement : population légale, exhaustif léger, etc.

À ces systèmes propres au recensement s'ajoutent des machines abstraites techniques (lecture et écriture de fichiers séquentiels, entrées-sorties sur écran, acquisition de paramètres). Toutes ces machines et systèmes ont fait l'objet d'une spécification formelle et ont été conçus de façon à être réutilisables et portables. L'outil B a été aussi utilisé comme outil de développement et de mise en œuvre de compilateurs générant du code Pascal 0². Voici quelques uns de ces outils :

- compilateur de bases de données avec compression des champs au niveau du bit, et portabilité assurée par l'utilisation de machines techniques de mémoire virtuelle et de machines de suites ;
- outil de définition de scalaires et tableaux, conçu pour permettre leur stockage dans des bases ;
- outil de définition de structures hiérarchiques des systèmes d'information;
- outil de génération d'automate fini, pilotant le chargement dans les bases de fichiers hiérarchisés contenant les données issues des enquêtes;
- générateur du JCL³ IBM relatif à un système, etc.

²G. Laffitte appelle "Pascal 0" un Pascal sans "record", sans pointeur, avec seulement le type entier.

³JCL (Job-Control-Language) ou "langage de commande" : langage utilisé pour écrire la séquence des commandes qui contrôleront l'exécution d'un travail. Les objets manipulés par le JCL sont des programmes ou des flots d'entrées et de sorties de ces programmes.

Tous ces outils sont interfacés les uns avec les autres par des dictionnaires leur permettant d'échanger des informations. Ces dictionnaires sont des théories stockées sous forme source, donc, consultables sous éditeur de texte.

Index

1985, 1

1990, 7

Adolphe Pinard, 1

analyseur syntaxique, 2

Art déco, style, 1

automate, 7

automate à pile, 2

B-Book, 1

B-Tool, 2

BN, 1

boucle, 2

Bourbaki, 2

BP, 2

Carroll Lewis, 2

CEPIA, 1

compression, 7

DPS7, 2

déterministe, non, 6

Ernst Marx, 2

Event-B, 3

expertise, 2

fatalité, propriété de, 1

géographie administrative, 2

Hermann, 2

hybride, 6

hypothèses, 2

IBM, 2

initialisation, 2

INSEE, 1

intersection, 2

invariant, approche de type, 3

JCL, 7

Moulin Jean, 2

Nantes, 1

NNI, 1

obligation de preuve, 2

Pascal, 2, 7

pile de torchons, 3

polonaise inverse, 2

portabilité, 7

recensement, 2

Rocquencourt, 1

sexe, code, 1

STERIA, 2

suite, machines de, 2

union, 2

Unix, 2