



Spécification formelle avec B

Henri Habrias

Hermes

Lavoisier

2-005-310-1

Spécification formelle avec B



Henri Habrias

avec la collaboration de

Jean-Yves Lafaye

Marie-Laure Potet

hermes
Science
— publications —

Table des matières

Avant-propos	13
Chapitre 1. Les services de B	19
Chapitre 2. Rerédaction d'un cahier des charges et introduction au concept de machine abstraite en B	31
2.1. Une nouvelle rédaction de la définition des besoins.	31
2.1.1. La définition informelle de besoins	31
2.1.2. Questions au demandeur.	32
2.2. La spécification en B	36
2.3. Le raffinement et implantation	41
2.4. Le processus de construction d'une application.	44
Chapitre 3. Introduction au développement d'un logiciel en B par un exemple.	45
3.1. La démarche de développement.	45
3.2. Le cahier des charges informel	46
3.3. L'architecture du projet.	46
3.4. La spécification	48
3.5. Retour sur la structuration de notre logiciel.	61
Chapitre 4. Logique et preuve.	65
4.1. La notion de séquent.	67
4.2. Règles d'inférence	68
4.3. Les trois règles de base du raisonnement mathématique.	71
4.3.1. Hypothèse (HYP).	71
4.3.2. Monotonie (MON).	72

4.3.3. Coupure (CUT)	72
4.4. Les deux stratégies de preuve d'un séquent : stratégie par l'avant et stratégie par l'arrière	73
4.4.1. Stratégie par l'arrière (ou dirigée par le but)	73
4.4.2. Stratégie par l'avant	73
4.5. Le calcul des propositions	74
4.6. Calcul des prédicats	83
4.6.1. Substitution	83
4.6.2. Quantification universelle	84
4.6.3. Occurrences libres et occurrences liées	85
4.6.4. Prédicat et expression	86
4.6.5. Test de (non-) liberté	87
4.6.6. Les règles de calcul pour la substitution	88
4.6.7. Règles dérivées pour la substitution	89
4.6.8. Règles d'inférence du calcul des prédicats	89
4.6.9. Quantificateur existentiel	92
Chapitre 5. Ensembles	99
5.1. Une approche syntaxique	99
5.2. B et les axiomes de la théorie des ensembles	101
5.2.1. Les axiomes de la théorie des ensembles	101
5.2.2. Les axiomes de la théorie des ensembles de B	104
5.2.3. Deux symboles essentiels : P et \times	105
5.3. L'inclusion ensembliste	108
5.4. La vérification du typage	110
5.5. Constructions dérivées : Union, Intersection, Différence	113
5.6. Ensembles de base	114
5.7. Intersection et Union généralisées	117
5.8. Pourquoi utiliser la théorie des ensembles ?	118
Chapitre 6. Relations et fonctions	121
6.1. Relation, Source, Cible, Domaine, Codomaine	122
6.1.1. Relation	122
6.1.2. Ensemble de départ (source), ensemble d'arrivée (cible), domaine et codomaine, couple	124
6.1.3. Relation inverse	126
6.2. Les 16 cas d'associations binaires entre ensembles	126
6.2.1. Le principe de la symbolisation en B	127
6.2.2. Les 16 cas et le paraphrasage en français	129
6.3. Opérations sur les relations et les fonctions	147
6.3.1. La restriction	147
6.3.2. L'image relationnelle, $rr[]$ et application de fonction, $ff ()$	149

6.3.3. Fonctions constantes	150
6.3.4. Transformée en fonction et transformée en relation.	151
6.3.5. Abstraction fonctionnelle (ou abstraction lambda)	151
6.3.6. Composition, identité, itération, fermeture transitive et réflexive, fermeture transitive.	153
6.3.7. Ecrasement	157
6.3.8. Le produit direct	159
6.3.9. Le produit parallèle	160
6.3.10. La projection	160
6.4. Retour sur les opérateurs ensemblistes =, \subseteq , \cap , \cup , card	161
6.5. Les expressions mal définies	162
Chapitre 7. Objets mathématiques : nombres naturels, suites, arbres	165
7.1. La notion de « point fixe » et la construction des objets mathématiques	165
7.2. L'ensemble des sous-ensembles finis d'un ensemble	166
7.3. Nombres naturels (\mathbb{N}) et entiers (\mathbb{Z})	166
7.4. Suites	168
7.4.1. La notion de suite.	168
7.4.2. Opérateurs sur les suites illustrés par des exemples.	169
7.4.3. L'ordre lexicographique sur une suite d'entiers	171
7.5. Les arbres finis.	171
7.5.1. La notion d'arbre	171
7.5.2. Les arbres étiquetés	173
7.5.3. Les arbres binaires	173
Chapitre 8. Structure d'une machine abstraite et preuve d'opération	175
8.1. Le concept de machine abstraite	175
8.1.1. Partie statique	178
8.1.2. Partie dynamique	178
8.1.3. Classification des opérations	179
8.1.4. L'encapsulation	182
8.2. Nommage des opérations, approche offensive vs approche défensive	184
8.2.1. Le nommage des opérations	184
8.2.2. Les deux styles de programmation : généreux (ou offensif) et défensif	186
8.3. Autres clauses'	192
8.3.1. Les clauses CONCRETE_VARIABLES, ABSTRACT_VARIABLES, ABSTRACT_CONSTANTS et CONCRETE_CONSTANTS	192
8.3.2. La clause DEFINITIONS	194
8.3.3. La clause ASSERTIONS	196
8.4. Les clauses de composition de machines	197

8.5. Retour sur l'interdiction du séquençement dans une machine abstraite . . .	197
8.5.1. Utilisation de la substitution skip.	197
8.5.2. Utilisation des préconditions.	197
8.5.3. Utilisation de variables de phase	198
8.5.4. Implantation de « spécification »	199
8.6. La preuve des opérations.	199

Chapitre 9. Les substitutions 203

9.1. Notion de substitution généralisée	203
9.1.1. Modélisation des transitions	203
9.1.2. Transformation de prédicats	206
9.2. Langage des substitutions généralisées (LSG).	211
9.2.1. Substitutions élémentaires	212
9.2.2. Composition de substitutions	212
9.2.3. Raccourcis d'écriture	215
9.2.4. Séquençement et parallélisme	220
9.3. Calcul des substitutions généralisées	222
9.3.1. Simplification des plus faibles préconditions	222
9.3.2. Simplification du séquençement et du parallélisme	223
9.3.3. Calcul de la terminaison et de la faisabilité.	224
9.4. Forme normale des substitutions	225
9.4.1. Forme normale	225
9.4.2. Vue relationnelle des substitutions.	226
9.4.3. Terminaison et prédicat relationnel d'une substitution normalisée	227
9.5. Compléments	228
9.5.1. Sémantique ensembliste	228
9.5.2. Substitution appliquée à une expression	228

Chapitre 10. Choix de modélisations ensemblistes. 231

10.1. Ensembles, Relations ou Fonctions, les clauses SETS et DEFINITIONS	231
10.1.1. Un premier exemple	231
10.1.2. Un deuxième exemple	232
10.1.3. Modélisation de l'inconnu.	234
10.2. Spécification et inclusion ensembliste	236
10.2.1. Spécification avec inclusion ensembliste	236
10.2.2. Spécification sans inclusion	237
10.3. Ensembles et fonctions pour spécifier un automate	238
10.3.1. Avec seulement des ensembles	238
10.3.2. Avec une fonction d'état et des définitions	239
10.4. Une spécification avec des suites	240
10.5. Un automate avec sorties.	241

10.6. Modélisation des objets	243
10.7. Contrainte de sous-ensemble et règle de mise-à-jour	245
Chapitre 11. L'approche bases de données, les contraintes dynamiques, l'hypothèse du déterminisme linguistique de Sapir-Whorf et quelques autres propos	247
11.1. Faits et contraintes (niveau de l'invariant d'état)	247
11.2. Les contraintes « dynamiques »	249
11.2.1. Et si nous avons mal interprété ?	249
11.2.2. Pouvons-nous écrire la contrainte dans l'invariant B ?	250
11.2.3. L'expression des contraintes « dynamiques » et la logique modale	251
11.3. L'hypothèse de Sapir [SAP 63] et Whorf [WHO 56]	252
11.4. Le niveau des fonctions	253
11.4.1. L'exemple	253
11.4.2. Conception des opérations pour un invariant donné et séquences d'opérations	255
11.5. Les bases de données déductives	258
11.6. Contrainte de sous-ensemble, redondance et règle de mise à jour	259
Chapitre 12. Le raffinement	263
12.1. Approche du raffinement	264
12.2. Réduire l'indéterminisme et affaiblir les préconditions	267
12.2.1. Affaiblir les préconditions	267
12.2.2. Réduction de l'indéterminisme	272
12.3. La preuve du raffinement	280
12.4. Les clauses d'un REFINEMENT	283
Chapitre 13. Séquencement et boucle	285
13.1. Le séquencement	286
13.1.1. L'axiome du séquencement	286
13.1.2. Preuve de l'implantation avec un séquencement	287
13.2. La boucle	287
13.2.1. Représentation graphique	287
13.2.2. La substitution de boucle	289
13.2.3. Le théorème de correction	289
13.2.4. Explication du théorème de correction de la boucle	292
13.2.5. Exemple (d'après Le manuel utilisateur de l'Atelier B)	292
13.2.6. L'implantation avec une boucle	296

Chapitre 14. Composition des machines et des raffinements	301
14.1. Composer les invariants	302
14.1.1. Construction incrémentale de spécifications	302
14.1.2. Vérification des appels d'opérations	305
14.1.3. Préservation des invariants par les substitutions généralisées	306
14.1.4. Invariants et variables partagées	307
14.1.5. Les clauses d'assemblage de B	309
14.2. Composer les raffinements	310
14.2.1. Composer les implémentations	310
14.2.2. Vue encapsulée d'une machine	312
14.2.3. Préservation des preuves de raffinement	312
14.3. Les clauses INCLUDES et IMPORTS	316
14.3.1. Utilisation	316
14.3.2. Clauses PROMOTES et EXTENDS	317
14.3.3. Obligations de preuve	317
14.3.4. Clauses INCLUDES et IMPORTS et raffinement	318
14.3.5. Renommage	318
14.4. Clause SEES	319
14.4.1. Utilisation	319
14.4.2. Obligations de preuve	320
14.4.3. Clause SEES et raffinement	320
14.4.4. Exemple	320
14.5. Clause USES	325
14.5.1. Utilisation	325
14.5.2. Un exemple	325
14.5.3. Obligations de preuve	329
14.5.4. Clause USES et raffinement	329
14.6. Conclusion	330
14.6.1. Architectures sans partage	330
14.6.2. Architectures avec partage par la clause SEES	330
14.6.3. Architectures avec partage par la clause USES	331
Chapitre 15. L'implantation finale et la structure d'un projet B	333
15.1. L'IMPLEMENTATION	333
15.1.1. Les clauses d'une IMPLEMENTATION	334
15.1.2. Les primitives de composition de machines	338
15.1.3. Les opérations	346
15.2. Principe général pour architecturer un projet en B	346

Chapitre 16. B événementiel	351
16.1. Interprétation des préconditions et des gardes	351
16.1.1. La précondition	351
16.1.2. La garde	352
16.2. Le contrôleur du pont de l'île.	353
16.2.1. Première vue du système (ou modèle initial).	354
16.2.2. Les obligations de preuve	354
16.2.3. Deuxième vue du système, raffinement par introduction du pont	356
16.2.4. Et ensuite.....	357
 Chapitre 17. B, VDM, Z et spécifications algébriques	359
17.1. Introduction	359
17.2. Une spécification écrite en B, VDM, Z et en spécifications algébriques	360
17.2.1. B	360
17.2.2. VDM	361
17.2.3. Z.	364
17.2.4. Spécification algébrique	367
 Chapitre 18. Glossaire B	373
 Chapitre 19. Notation « mathématique » et notation ASCII pour spécifier B	403
19.1. Prédicats	403
19.2. Ensembles	403
19.3. Relations	404
19.4. Objets mathématiques.	405
19.5. Suites	406
19.6. Substitutions	406
 Bibliographie	407