

Teaching Formal Methods for 10 Years: Reflections on Theories, Tools, Materials, and Communities

Gustavo Carvalho
(ghpc@cin.ufpe.br)

Universidade Federal de Pernambuco
Centro de Informática, 50740-560, Brazil



Centro de
Informática
UFPE



UNIVERSIDADE
FEDERAL
DE PERNAMBUCO

Motivation

The Role of Formal Methods in Computer Science Education¹

... every computer scientist needs to know Formal Methods [4], since the skills and knowledge acquired ... provide the indispensable solid foundation that forms the backbone of CS practice.

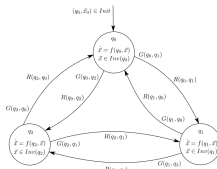
Impressions from teaching FMs for 10 years in Brazil

- Theories
- Tools
- Materials
- Communities

¹[Link to the paper](#)



A reinterpretation of SE with rigour



Formal Model

enables

Animation

Random
User guided

Verification

Testing
Manual proof
Mechanised proof
Model checking

Translation

Other models
Code generation

Visualisation

View x Model

Teaching experience

Focus: a broad overview as depicted before
(conversely, a module with a focus on proof development using Coq)

Period: from 2014–nowadays

Level: undergraduate students

Grouped into three distinct phases

- **Phase 1:** teaching with Z and CSP#
- **Phase 2:** teaching with Event-B and CSP_M
- **Phase 3:** teaching with B



Centro de
Informática
UFPE



UNIVERSIDADE
FEDERAL
DE PERNAMBUCO

General information

	Phase 1	Phase 2	Phase 3
Period	2014–2015	2015–2017	2017–now
Institution	UPE (BR)	UPE (BR)	UFPE (BR)
Course	Comp. Engineering	Comp. Engineering	Comp. Engineering Comp. Science Inf. Systems
Level	Undergraduate	Undergraduate	Undergraduate
Module	Formal Methods	Formal Methods	Critical Systems
Curriculum	Mandatory	Mandatory	Optional
Prerequisites	SW Analysis and Design	SW Analysis and Design	SW Engineering

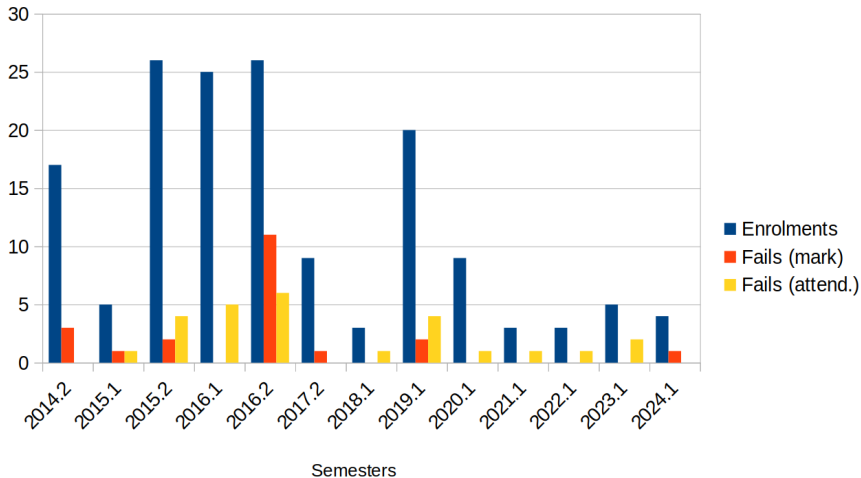


**Centro de
Informática**
UFPE



UNIVERSIDADE
FEDERAL
DE PERNAMBUCO

Enrolments and fails



Phase 1 = 2014.2 .. 2015.1
Phase 2 = 2015.2 .. 2016.2
Phase 3 = 2017.2 .. 2024.1

Teaching and assessment dynamics

	Phase 1	Phase 2	Phase 3
Delivery mode	In person	In person	In person (mostly)
Methodology	Traditional	Traditional	Flipped classroom
Teaching	Classroom Lab. sessions Seminars	Classroom Lab. sessions Seminars	Lab. sessions
Assessment	Project (2 parts) Written exams (2)	Project (2 parts) Written exams (2)	Project (3 parts) Exam at the lab.
Marking	Manual	Manual	Manual



Centro de
Informática
UFPE



UNIVERSIDADE
FEDERAL
DE PERNAMBUCO

Phase 1: from 2014 to 2015

	Phase 1
Approach	Fragmented overview
Theories	Z CSP#
Tools	CZT Z-Eves PAT
Materials	Book by Woodcock & Davies Tools documentation
Communities	Scarce
Impressions	<ul style="list-style-type: none">- Loose connection- Tools (Z)- Scarce community- Shallow seminars



**Centro de
Informática**
UFPE



UNIVERSIDADE
FEDERAL
DE PERNAMBUCO

Phase 2: from 2015 to 2017

	Phase 2
Approach	Fragmented overview
Theories	Event-B CSP _M
Tools	Rodin ProB BMotion Studio FDR3
Materials	Tools documentation Book by Roscoe
Communities	Scarce
Impressions	<ul style="list-style-type: none">- Loose connection+ Tools (Event-B)- Scarce community- Shallow seminars

R



FDR3



Centro de
Informática
UFPE



UNIVERSIDADE
FEDERAL
DE PERNAMBUCO

Phase 3: from 2017 to nowadays

	Phase 3
Approach	Unified overview
Theories	B
Tools	Atelier B ProB BMotionWeb
Materials	MOOC of B Tools documentation
Communities	Scarce
Impressions	+ Integrated applications of FMs + Tools (B) - Scarce community

ATELIER B



Centro de
Informática
UFPE



UNIVERSIDADE
FEDERAL
DE PERNAMBUCO

Phase 3: from 2017 to nowadays



Project presented in
2024.1: revisiting the
lift example

Module's website:

sites.google.com/a/cin.ufpe.br/if721



Centro de
Informática
UFPE



UNIVERSIDADE
FEDERAL
DE PERNAMBUCO

Summary of our thoughts

Curriculum

- Thinking about **correctness** is crucial
- Should be an **integral** part of CS education
- Start the discussion **early** (e.g., Discrete Mathematics, Logic)

Module's scope

- First, a mandatory module “Formal Methods” (**unified overview**)
- Then, optional modules (focus on **specific techniques**)



Centro de
Informática
UFPE



UNIVERSIDADE
FEDERAL
DE PERNAMBUCO

Summary of our thoughts

Theories, tools, materials, and communities

- First, be **more practical** than theoretical
- Then, get into the underlying **details** and theories
- Choose appropriate **languages** (materials and communities)
- Choose appropriate **tools** (documentation and user-friendliness)



Centro de
Informática
UFPE



UNIVERSIDADE
FEDERAL
DE PERNAMBUCO

Demonstration @ FM Teaching Expo

```

1  /* Stack
2     * Author: @gpc
3     * Creation date: 02/09/24
4     */
5
6  MACHINE
7  Stack
8  CONSTANTS
9  PROPERTIES
10 MAX_SIZE : NAT
11 & MAX_SIZE > 0
12 VARIABLES
13 stack_data
14 INVARIANT
15 stack_data : seq(NAT)
16 // seq(s) = 0 n . (n : NAT | 1..n -> E)
17 INITIALISATION
18 stack_data := ()
19 OPERATIONS
20 stack_push(value) =
21   PRE
22     value : NAT
23     & size(stack_data) < MAX_SIZE

```

Item	Name	Value	Previous Value
1	stack_data	(())	(())
2	stack_data	(0,0,0)	(0,0,0)
3	stack_data	(0,0,0,0)	(0,0,0,0)
4	stack_data	(0,0,0,0,0)	(0,0,0,0,0)
5	stack_data	(0,0,0,0,0,0)	(0,0,0,0,0,0)
6	stack_data	(0,0,0,0,0,0,0)	(0,0,0,0,0,0,0)
7	stack_data	(0,0,0,0,0,0,0,0)	(0,0,0,0,0,0,0,0)
8	stack_data	(0,0,0,0,0,0,0,0,0)	(0,0,0,0,0,0,0,0,0)
9	stack_data	(0,0,0,0,0,0,0,0,0,0)	(0,0,0,0,0,0,0,0,0,0)
10	stack_data	(0,0,0,0,0,0,0,0,0,0,0)	(0,0,0,0,0,0,0,0,0,0,0)
11	stack_data	(0,0,0,0,0,0,0,0,0,0,0,0)	(0,0,0,0,0,0,0,0,0,0,0,0)
12	stack_data	(0,0,0,0,0,0,0,0,0,0,0,0,0)	(0,0,0,0,0,0,0,0,0,0,0,0,0)
13	stack_data	(0,0,0,0,0,0,0,0,0,0,0,0,0,0)	(0,0,0,0,0,0,0,0,0,0,0,0,0,0)
14	stack_data	(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0)	(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0)
15	stack_data	(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0)	(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0)
16	stack_data	(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0)	(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0)
17	stack_data	(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0)	(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0)
18	stack_data	(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0)	(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0)
19	stack_data	(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0)	(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0)
20	stack_data	(0,0)	(0,0)
21	stack_data	(0,0)	(0,0)
22	stack_data	(0,0)	(0,0)
23	stack_data	(0,0)	(0,0)

Stack Example

PUSH VALUE	POP VALUE
Push	Pop

Events

Time	Operation	Value
0	INITIALISATION	(())
1	stack_push(0)	(0)
2	stack_push(0)	(0,0)
3	stack_push(0)	(0,0,0)
4	stack_push(0)	(0,0,0,0)
5	stack_push(0)	(0,0,0,0,0)
6	stack_push(0)	(0,0,0,0,0,0)
7	stack_push(0)	(0,0,0,0,0,0,0)
8	stack_push(0)	(0,0,0,0,0,0,0,0)
9	stack_push(0)	(0,0,0,0,0,0,0,0,0)
10	stack_push(0)	(0,0,0,0,0,0,0,0,0,0)
11	stack_push(0)	(0,0,0,0,0,0,0,0,0,0,0)
12	stack_push(0)	(0,0,0,0,0,0,0,0,0,0,0,0)
13	stack_push(0)	(0,0,0,0,0,0,0,0,0,0,0,0,0)
14	stack_push(0)	(0,0,0,0,0,0,0,0,0,0,0,0,0,0)
15	stack_push(0)	(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0)
16	stack_push(0)	(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0)
17	stack_push(0)	(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0)
18	stack_push(0)	(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0)
19	stack_push(0)	(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0)
20	stack_push(0)	(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0)
21	stack_push(0)	(0,0)
22	stack_push(0)	(0,0)
23	stack_push(0)	(0,0)

```

1  stack := ()
2
3  /* Stack
4     * Author: @gpc
5     * Creation date: 02/09/24
6     */
7
8  MACHINE
9  Stack
10 CONSTANTS
11 PROPERTIES
12 MAX_SIZE : NAT
13 & MAX_SIZE > 0
14 VARIABLES
15 stack_data
16 INVARIANT
17 stack_data : seq(NAT)
18 // seq(s) = 0 n . (n : NAT | 1..n -> E)
19 INITIALISATION
20 stack_data := ()
21 OPERATIONS
22 stack_push(value) =
23   PRE
24     value : NAT
25     & size(stack_data) < MAX_SIZE
26   POST
27     stack_data = seq(0, stack_data)
28   END

```



Teaching Formal Methods for 10 Years: Reflections on Theories, Tools, Materials, and Communities

Gustavo Carvalho
(ghpc@cin.ufpe.br)

Universidade Federal de Pernambuco
Centro de Informática, 50740-560, Brazil



Centro de
Informática
UFPE



UNIVERSIDADE
FEDERAL
DE PERNAMBUCO