Program Verification

Radu Iosif (CR1,CNRS)

Joint work with:

- ➡ Marius Bozga (IR1,CNRS)
- ➡ Filip Konecny (PhD 2008-2012, now at EPFL, Lausanne)
- ➡ Jiri Simacek (PhD 2008-2012, now at NetSuite, Brno)
- ➡ Florent Garnier (PostDoc 2010-2012, now at MathWorks, Paris)

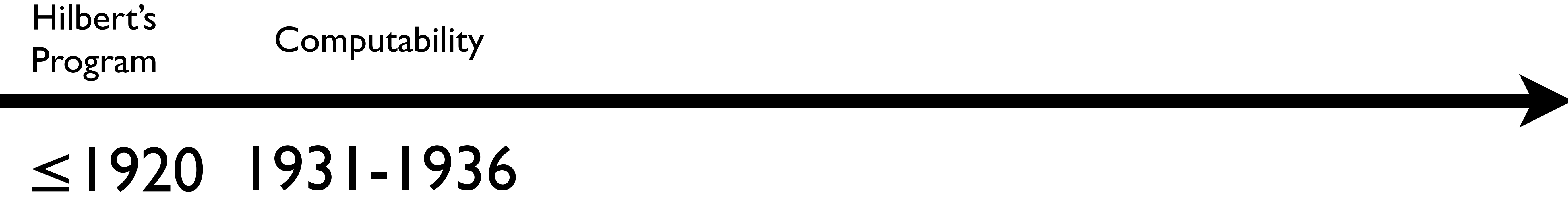
Program Verification Timeline

Program Verification Timeline

Hilbert's
Program

≤1920

Program Verification Timeline



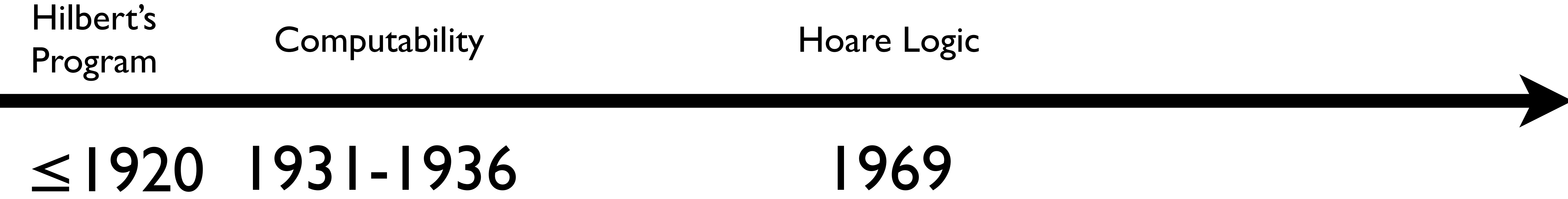
Hilbert's Program

≤1920

Computability

1931-1936

Program Verification Timeline



Hilbert's Program

≤1920

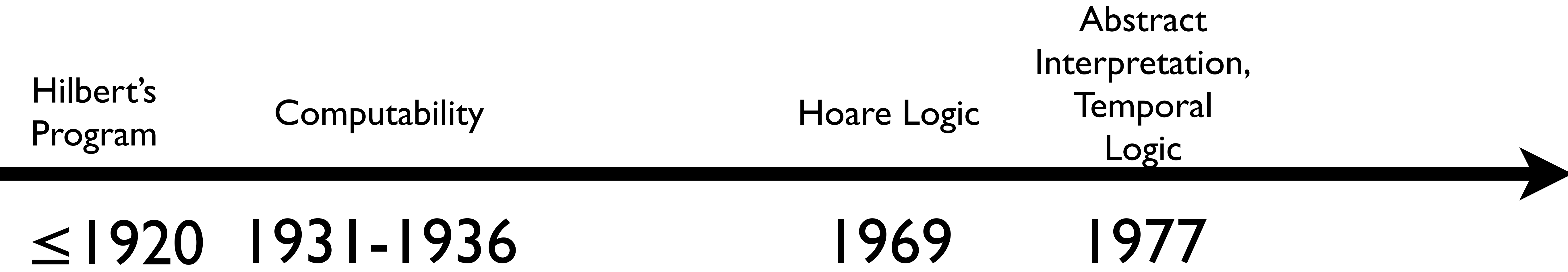
Computability

1931-1936

Hoare Logic

1969

Program Verification Timeline



Hilbert's Program

≤1920

Computability

1931-1936

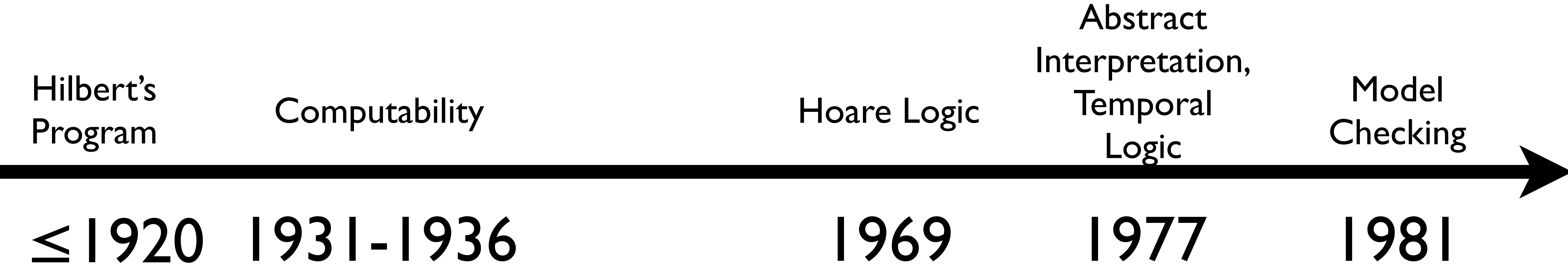
Hoare Logic

1969

Abstract Interpretation, Temporal Logic

1977

Program Verification Timeline



Hilbert's Program

Computability

Hoare Logic

Abstract Interpretation, Temporal Logic

Model Checking

≤1920

1931-1936

1969

1977

1981

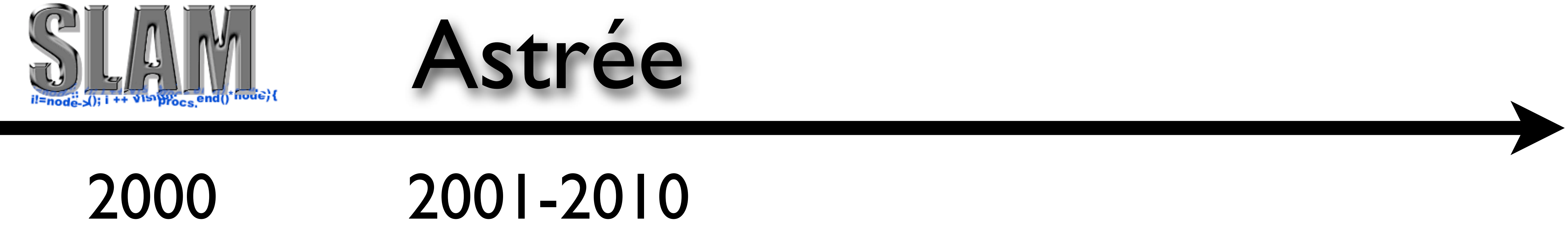
Program Verification Timeline

Program Verification Timeline

Program Verification Timeline

2000

Program Verification Timeline



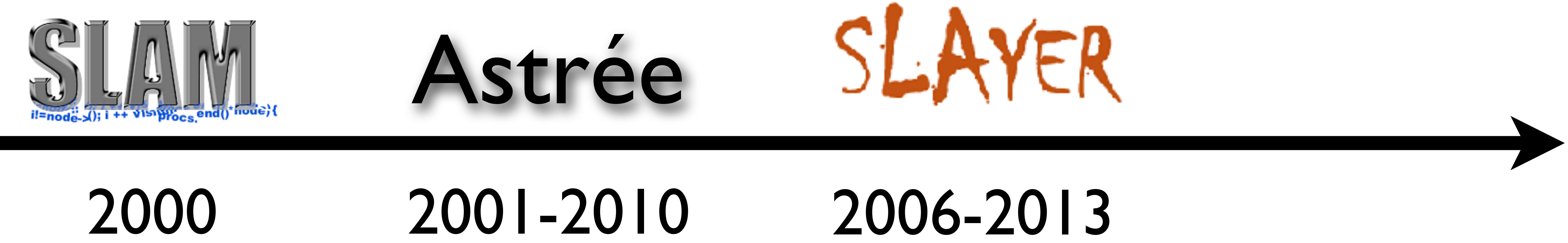
SLAM

Astrée

2000

2001-2010

Program Verification Timeline



SLAM

Astrée

SLAYER

2000

2001-2010

2006-2013

Program Verification Timeline

SLAM

Astrée

SLAYER

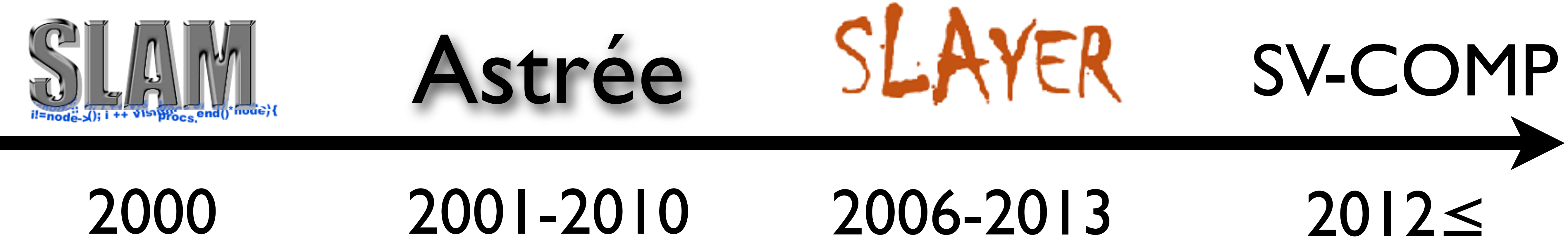
2000

2001-2010

2006-2013

Reports of 100K to 10 million lines of verified code!

Program Verification Timeline



SLAM — 2000

Astrée — 2001-2010

SLAYER — 2006-2013

SV-COMP — 2012≤

Reports of 100K to 10 million lines of verified code!

Program Verification Status

Static Analysis

- Lots of false positives
- No automatic refinement

Model Checking

- Infinite state spaces
- No guarantee of termination

What’s wrong ?

- The success criteria are wrong
- The size of a program gives no indication on the complexity of its verification problems
- Empirical success stories (deadly bug found in device driver) are almost impossible to reproduce and trust

What's wrong ?

- The success criteria are wrong
- The size of a program gives no indication on the complexity of its verification problems
- Empirical success stories (deadly bug found in device driver) are almost impossible to reproduce and trust

We need better measures of problem complexity than the # of lines, or the # of variables, etc ...

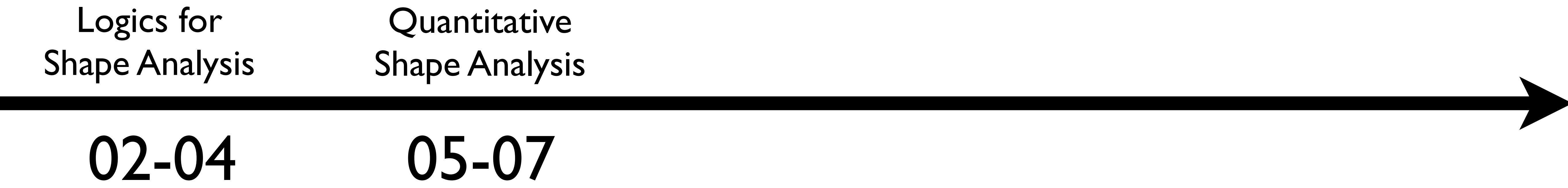
A Personal Timeline

A Personal Timeline

Logics for Shape Analysis

02-04

A Personal Timeline



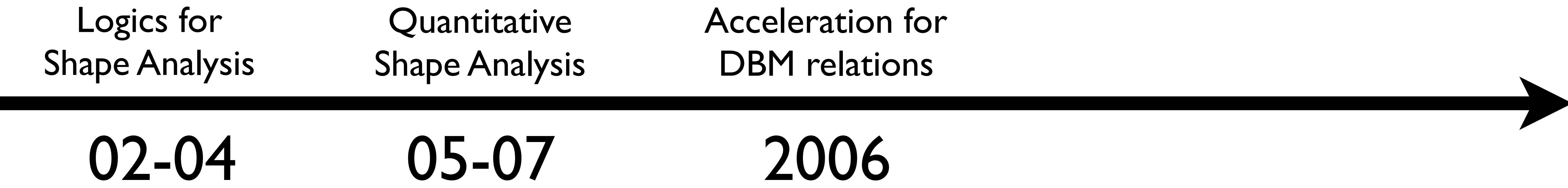
Logics for Shape Analysis

02-04

Quantitative Shape Analysis

05-07

A Personal Timeline



Logics for Shape Analysis

02-04

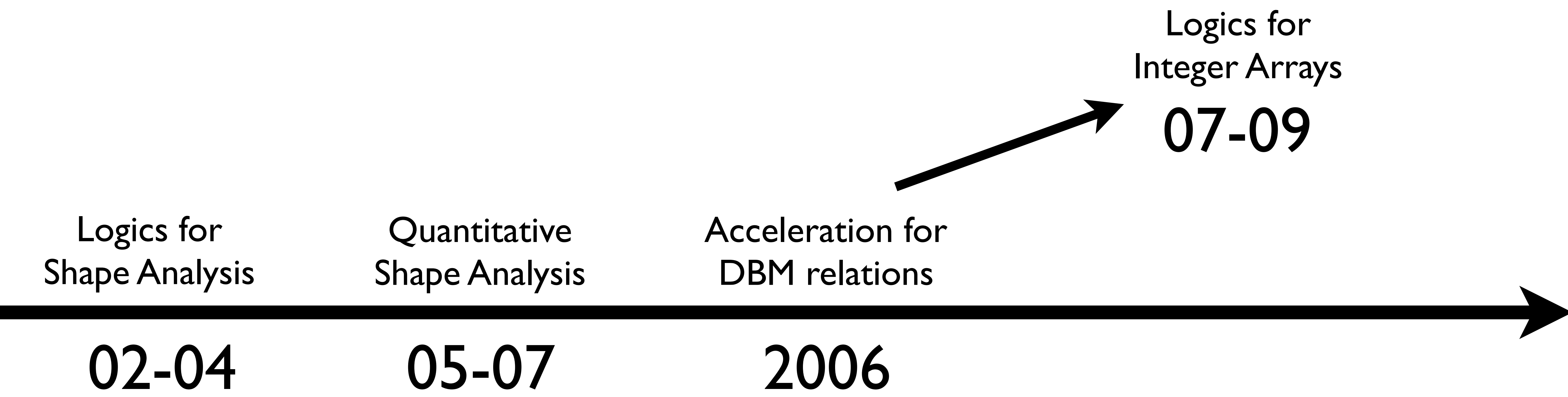
Quantitative Shape Analysis

05-07

Acceleration for DBM relations

2006

A Personal Timeline



Logics for Integer Arrays

07-09

Logics for Shape Analysis

02-04

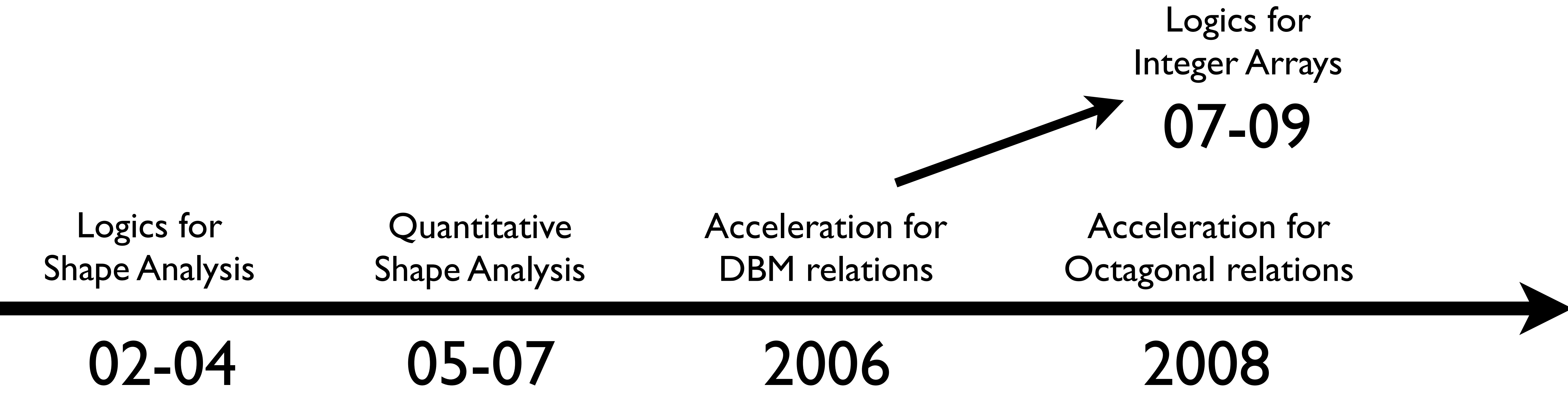
Quantitative Shape Analysis

05-07

Acceleration for DBM relations

2006

A Personal Timeline



Logics for Integer Arrays

07-09

Logics for Shape Analysis

02-04

Quantitative Shape Analysis

05-07

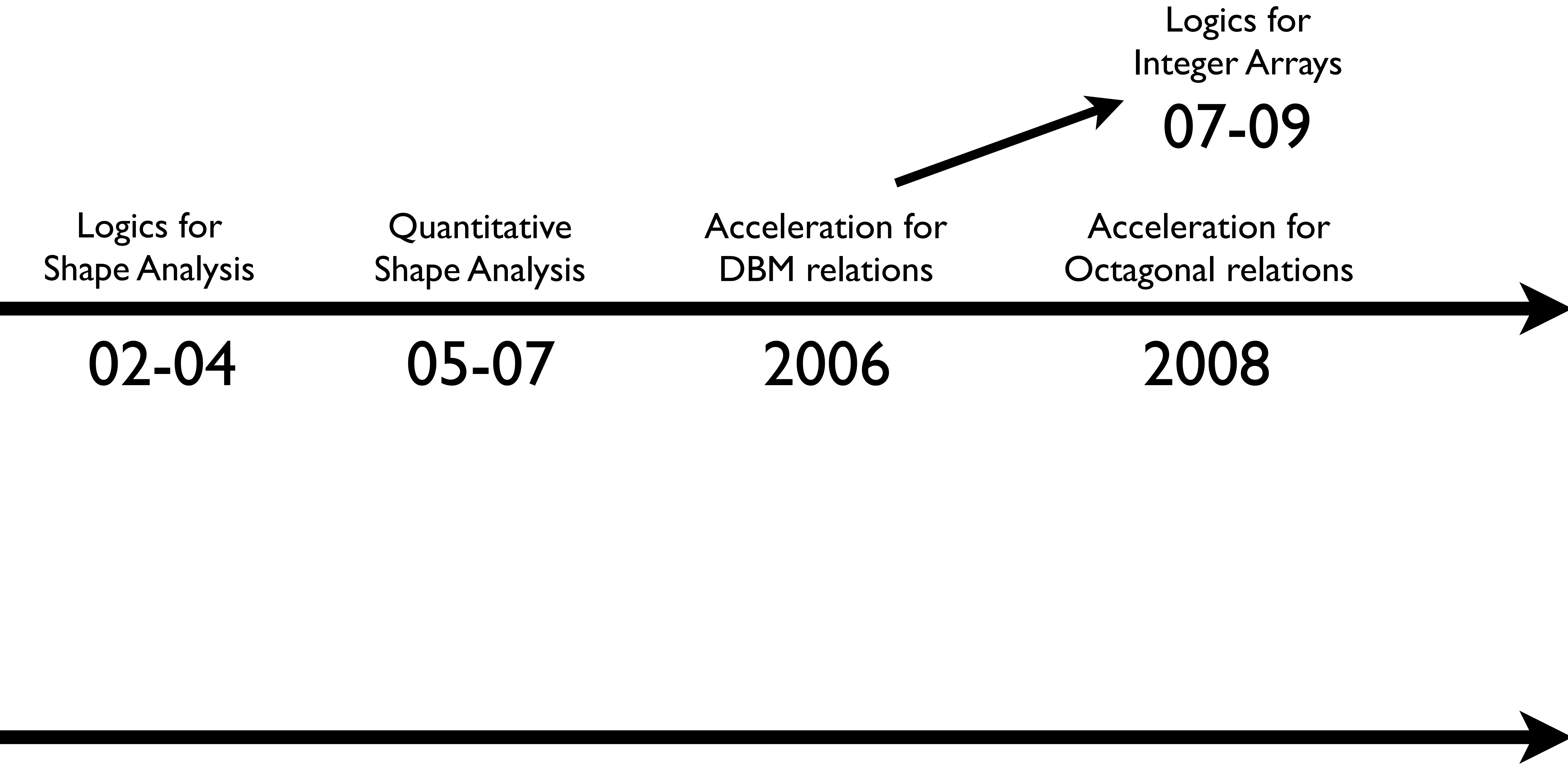
Acceleration for DBM relations

2006

Acceleration for Octagonal relations

2008

A Personal Timeline



Logics for Integer Arrays 07-09

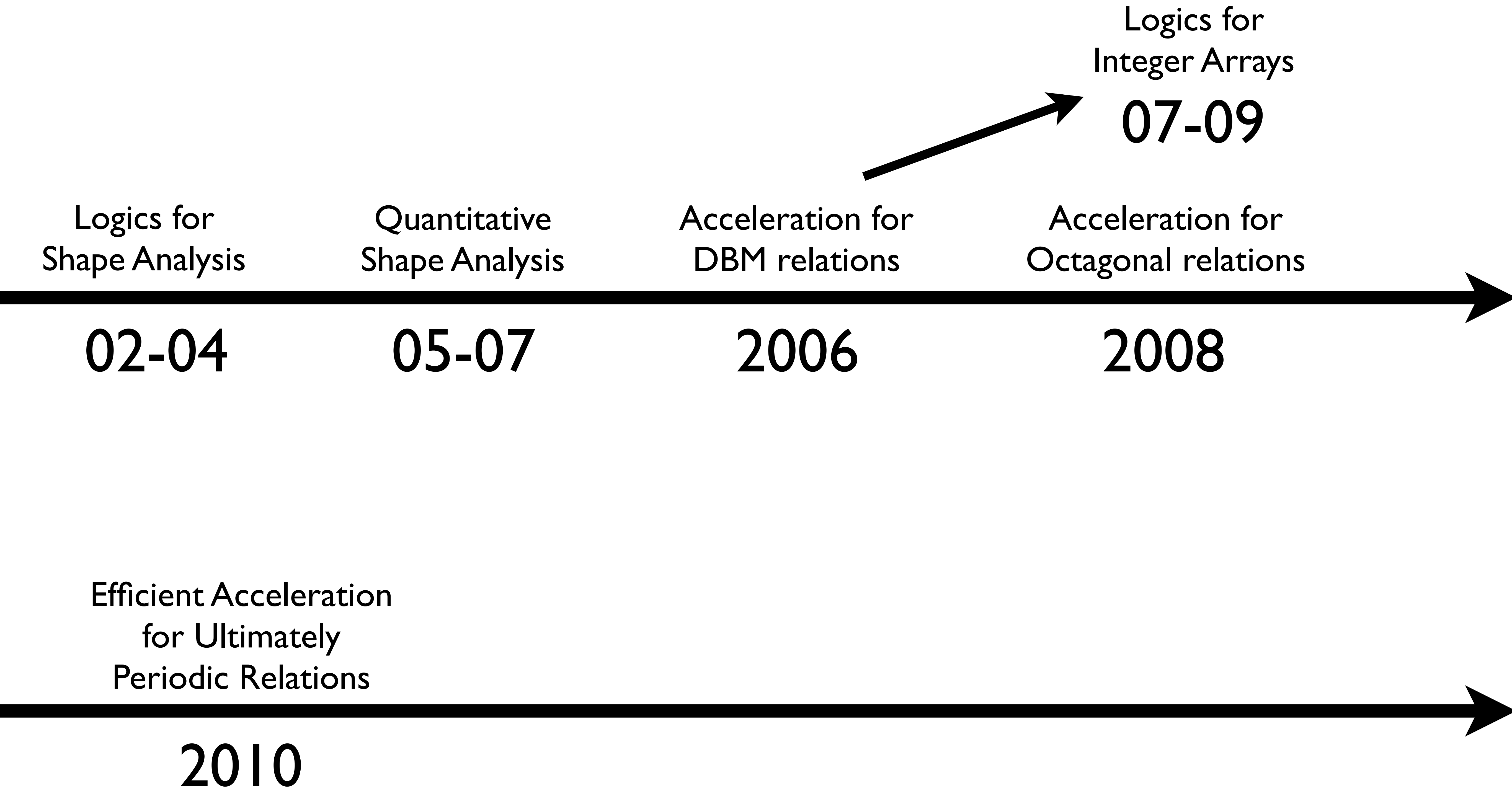
Logics for Shape Analysis 02-04

Quantitative Shape Analysis 05-07

Acceleration for DBM relations 2006

Acceleration for Octagonal relations 2008

A Personal Timeline



Logics for
Integer Arrays

07-09

Logics for
Shape Analysis

02-04

Quantitative
Shape Analysis

05-07

Acceleration for
DBM relations

2006

Acceleration for
Octagonal relations

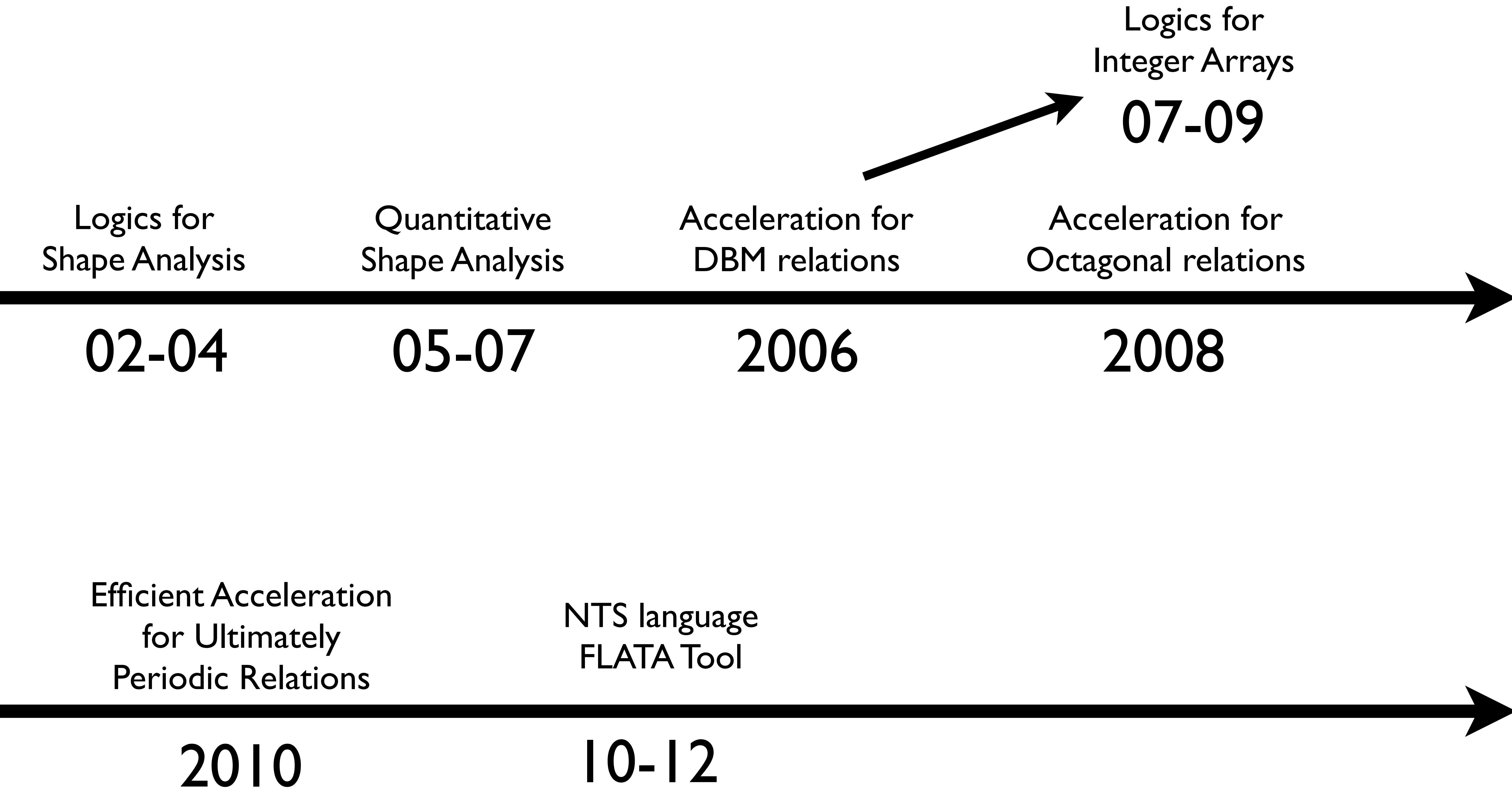
2008

Efficient Acceleration
for Ultimately
Periodic Relations

2010

from 10 var/hour to 10 var/sec

A Personal Timeline



Logics for Integer Arrays

07-09

Logics for Shape Analysis

02-04

Quantitative Shape Analysis

05-07

Acceleration for DBM relations

2006

Acceleration for Octagonal relations

2008

Efficient Acceleration for Ultimately Periodic Relations

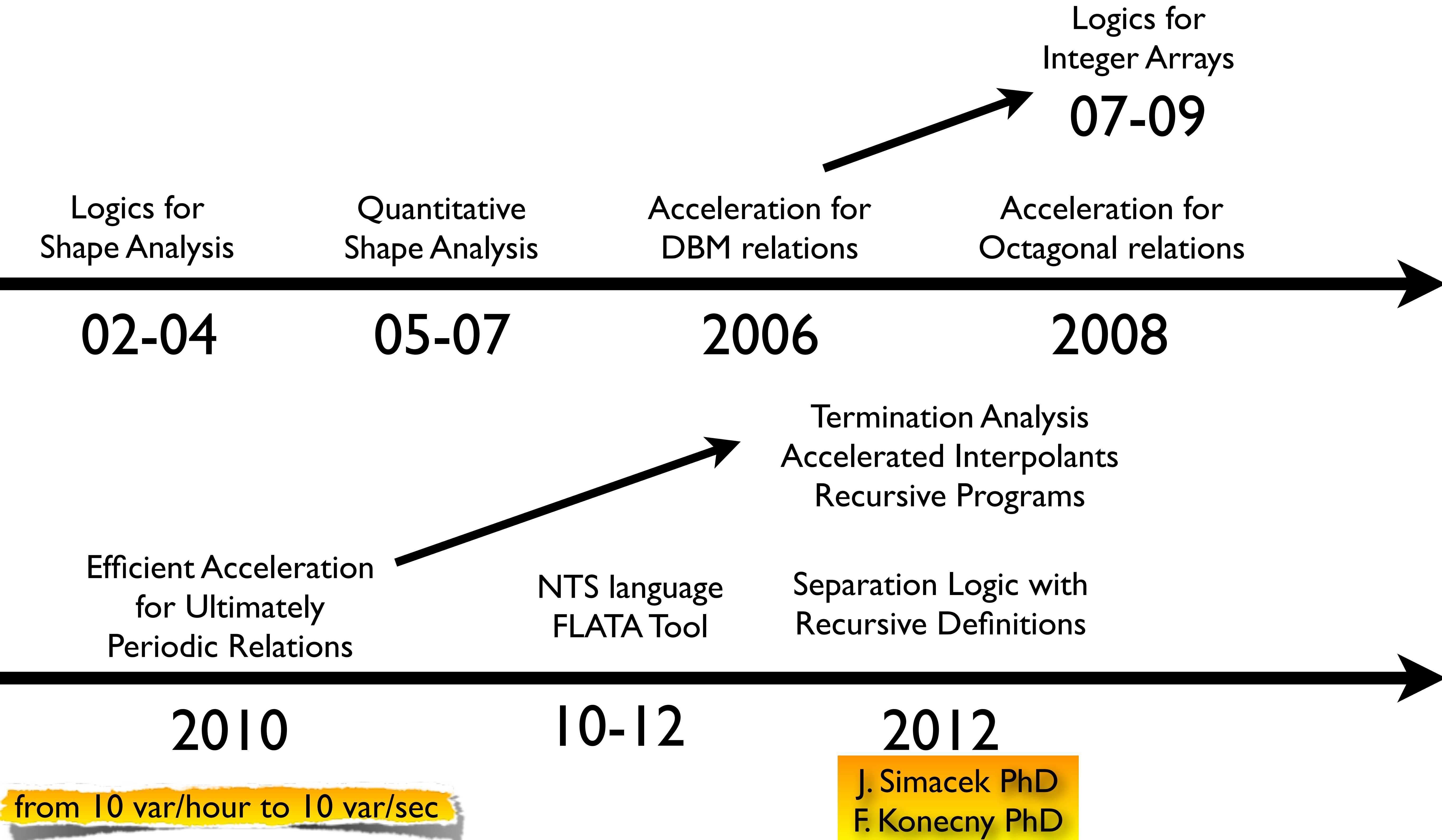
2010

NTS language
FLATA Tool

10-12

from 10 var/hour to 10 var/sec

A Personal Timeline



Logics for Integer Arrays

07-09

Logics for Shape Analysis

02-04

Quantitative Shape Analysis

05-07

Acceleration for DBM relations

2006

Acceleration for Octagonal relations

2008

Termination Analysis
Accelerated Interpolants
Recursive Programs

Efficient Acceleration for Ultimately Periodic Relations

2010

from 10 var/hour to 10 var/sec

NTS language
FLATA Tool

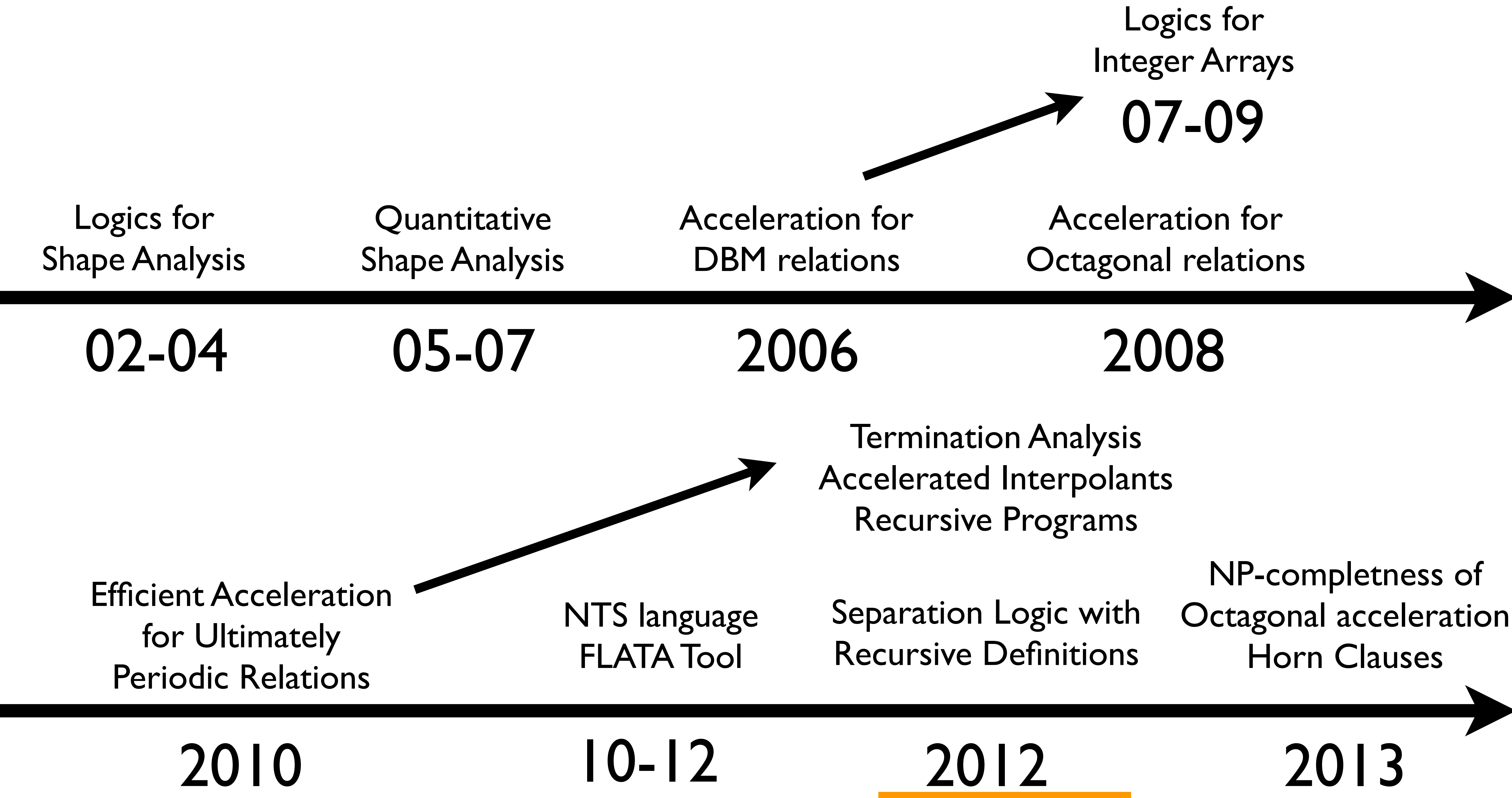
10-12

Separation Logic with Recursive Definitions

2012

J. Simacek PhD
F. Konecny PhD

A Personal Timeline



Logics for Integer Arrays
07-09

Logics for Shape Analysis
02-04

Quantitative Shape Analysis
05-07

Acceleration for DBM relations
2006

Acceleration for Octagonal relations
2008

Termination Analysis
Accelerated Interpolants
Recursive Programs

Efficient Acceleration for Ultimately Periodic Relations
2010

NTS language
FLATA Tool
10-12

Separation Logic with Recursive Definitions
2012

NP-completness of Octagonal acceleration
Horn Clauses
2013

from 10 var/hour to 10 var/sec

J. Simacek PhD
F. Konecny PhD

Future Projects

- Study the complexity of discrete systems from a different perspective (algorithmic entropy)
- Computational complexity of temporal logic for discrete infinite state systems
- Compositional shape analysis based on Separation Logic
- Multi-level program analysis (axiomatic vs. imperative)

Projects and Collaborations

- AVERILES (RNTL 2006-2009)
- VERIDYC (ANR SEGI 2009-2013)
- ADEPT (ANR INS - decision pending)

- LIAFA Paris (Equipe Modelisation et Verification)
- Brno University of Technology (VeriFIT group)
- IMDEA Madrid (Pierre Ganty)
- EPFL Lausanne (LARA group), TUM (Rybalchenko group), MSR (Bjorner, Qadeer)