Logical Support for Bike-Sharing System Design

Ionuţ Ţuţu   Claudia Elena Chiriţă
Antónia Lopes   José Luiz Fiadeiro

IMAR, Romania   RHUL, UK   ULisboa, Portugal

SG65 @ Formal Methods

Porto 2019

Challenges in modelling and analysing quantitative aspects of a bike-sharing product line

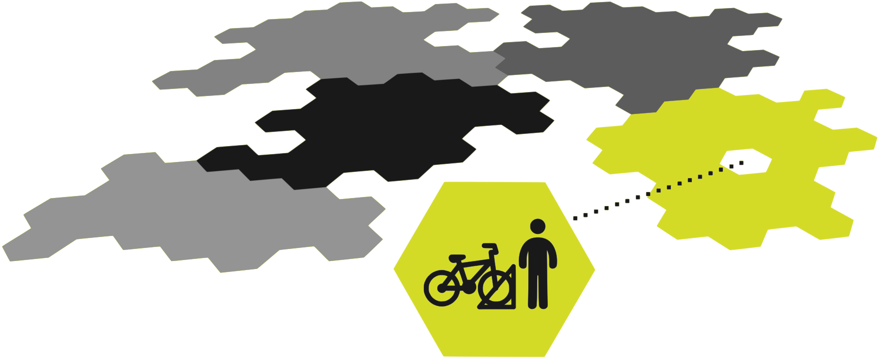
Challenges in modelling and analysing
qualitative ~~quantitative~~ aspects of
a bike-sharing ~~product line~~ system

Challenges in modelling and analysing
qualitative ~~quantitative~~ aspects of
a bike-sharing ~~product line~~ system

information-flow properties

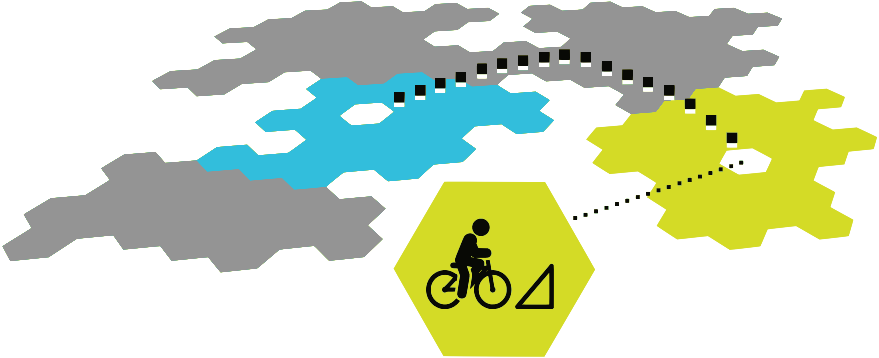
The bike-sharing system

The bike-sharing system

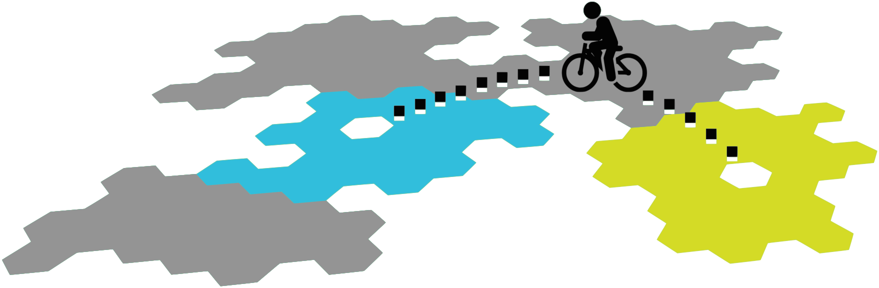


The bike-sharing system

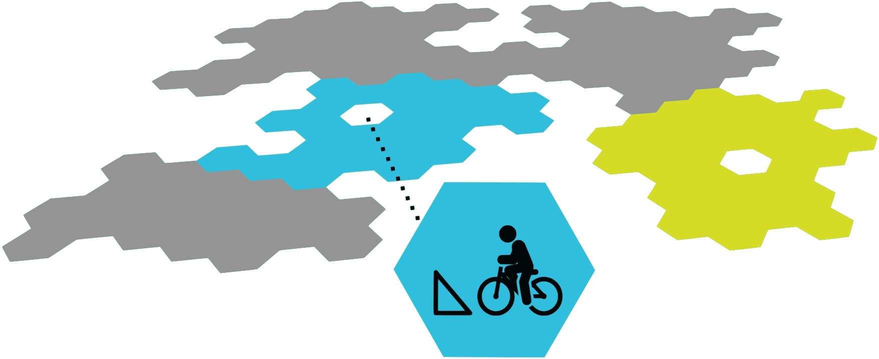
The bike-sharing system



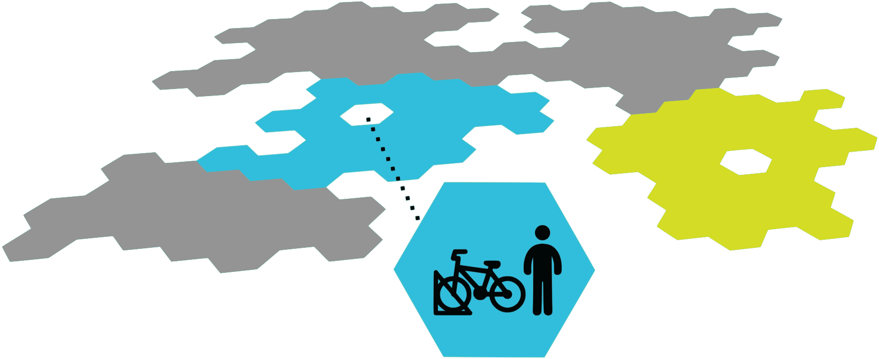
The bike-sharing system



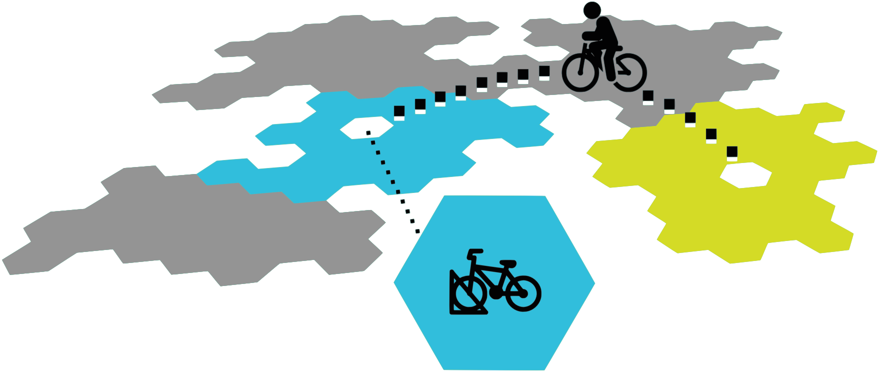
The bike-sharing system



The bike-sharing system

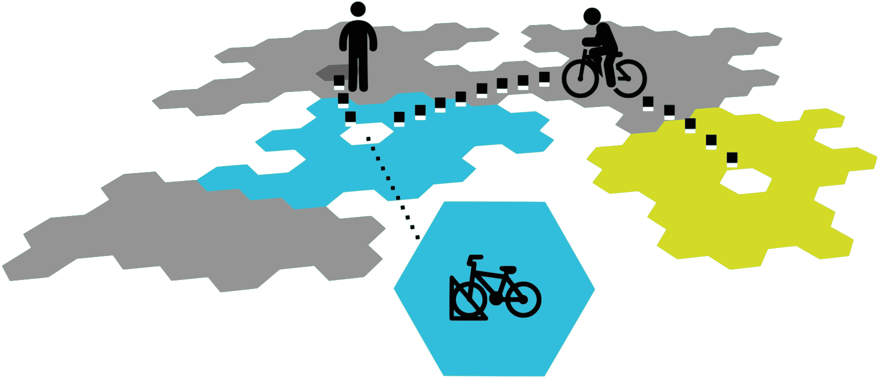


The bike-sharing system

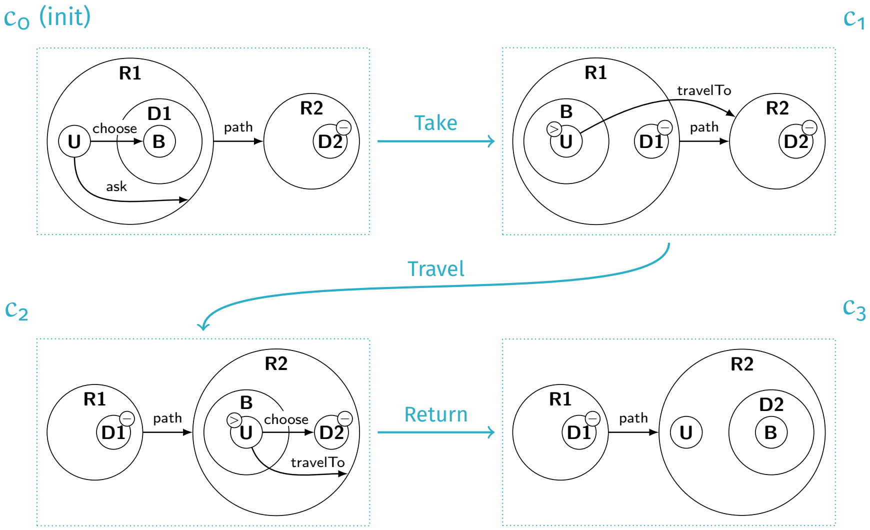


The bike-sharing system

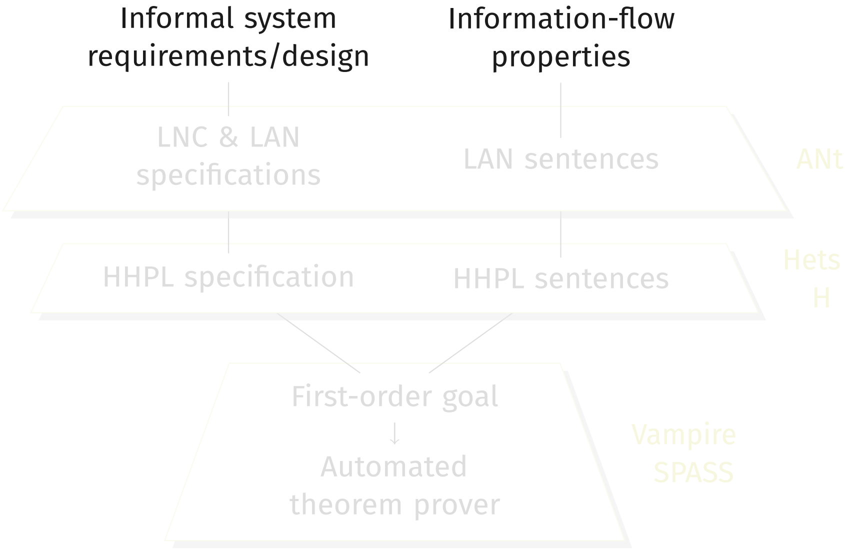
The bike-sharing system



A typical model



Specification and verification methodology



Informal system requirements/design

Information-flow properties

LNC & LAN specifications

LAN sentences

ANt

HHPL specification

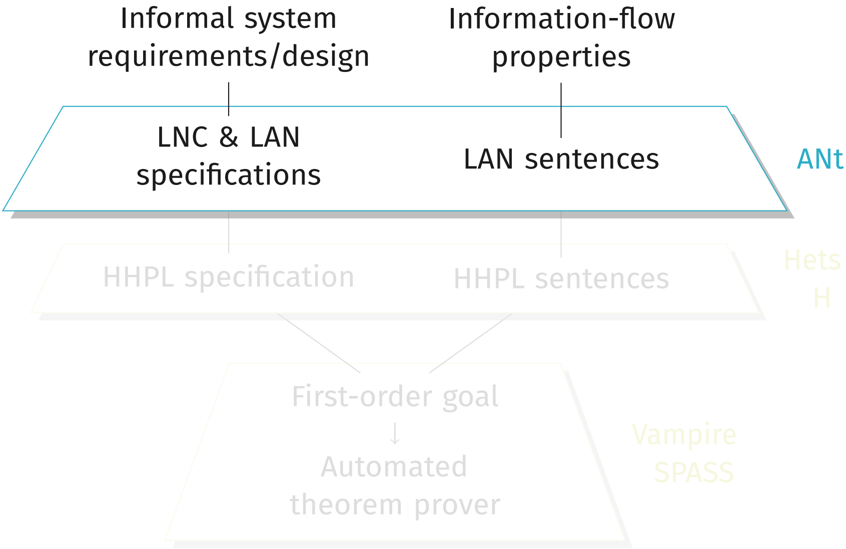
HHPL sentences

Hets
H

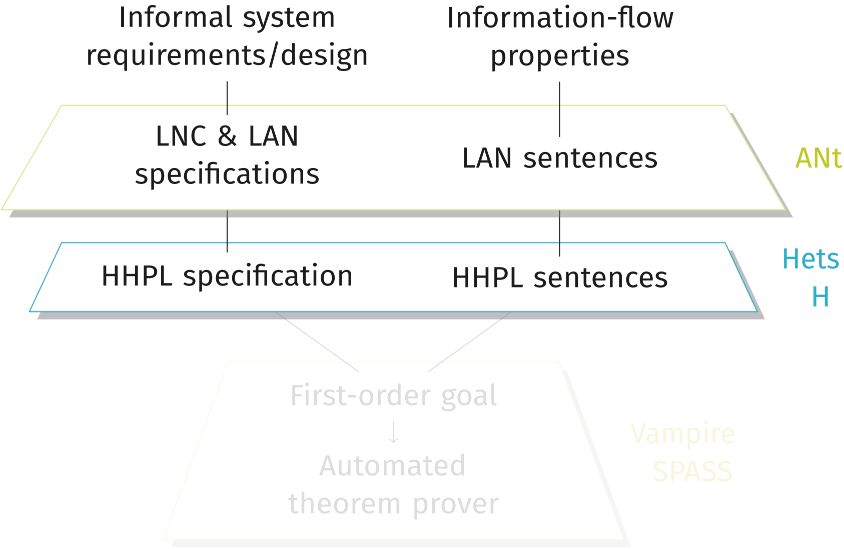
First-order goal
↓
Automated theorem prover

Vampire
SPASS

Specification and verification methodology



Specification and verification methodology



Informal system requirements/design

Information-flow properties

LNC & LAN specifications

LAN sentences

ANt

HHPL specification

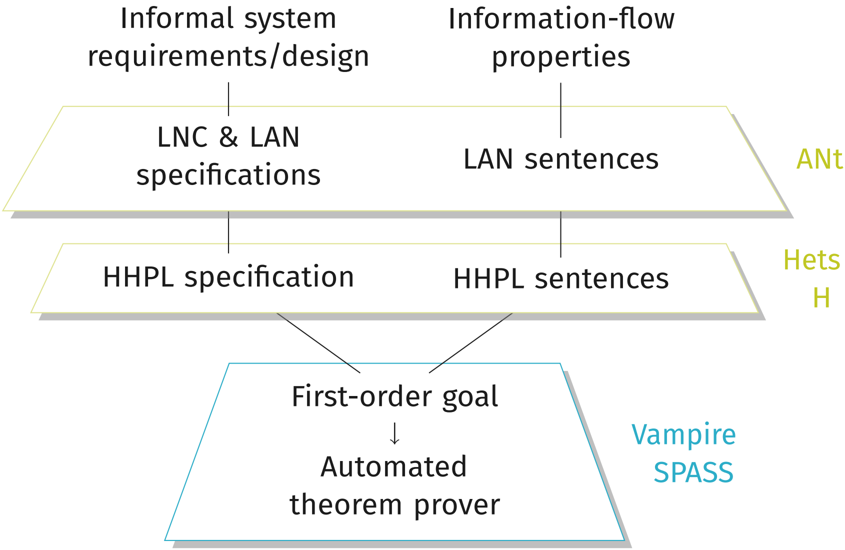
HHPL sentences

Hets H

First-order goal
↓
Automated theorem prover

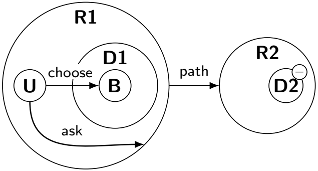
Vampire SPASS

Specification and verification methodology



The actor-network specification

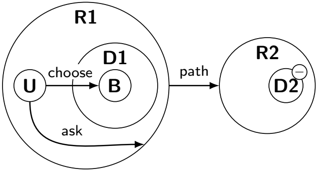
· actor types ·



actor types User, Bike, Dock, Region

The actor-network specification

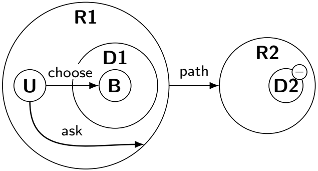
· attributes ·



attributes	freeDock: Dock	⊖
	travelling: User	⧁
	fullRegion: Region	⊕
	rewardOffered: Region	⊛

The actor-network specification

· channel types ·



channel types ask: User → Region

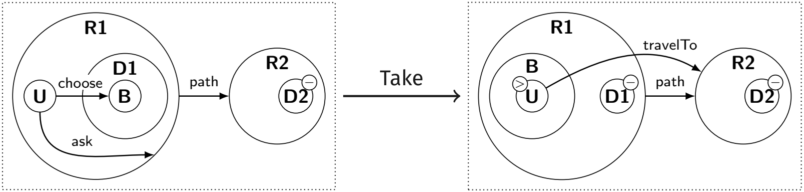
choose: User → Bike

path: Region → Region

travelTo: User → Region

The actor-network specification

· interactions ·



interactions Take: $\exists u\colon \text{User}; b\colon \text{Bike}; d\colon \text{Dock}; r\colon \text{Region}$

$$\cdot\ @_u\,(\langle\pi\rangle\, r \wedge \langle\text{ask}\rangle\, r \wedge \langle\text{choose}\rangle\, b) \wedge$$
$$@_b\,\langle\pi\rangle\,(d \wedge \langle\pi\rangle\, r)$$

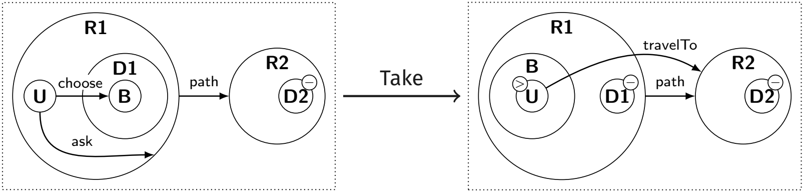
Travel: $\ldots$

Return: $\ldots$

Reward: $\ldots$

The actor-network specification

· effects and non-effects of interactions ·



rules $\forall\, u\colon \text{User};\ b\colon \text{Bike};\ d\colon \text{Dock};\ r\colon \text{Region}$

$$\cdot\ @_u\,(\langle\pi\rangle\, r \wedge \langle\text{ask}\rangle\, r \wedge \langle\text{choose}\rangle\, b) \wedge @_b\,\langle\pi\rangle\,(d \wedge \langle\pi\rangle\, r)$$

$$\Rightarrow$$

$$[\![\text{Take}]\!]\ @_u\,(\langle\pi\rangle\,(b \wedge \langle\pi\rangle\, r) \wedge \exists\, r'\colon \text{Region} \cdot \langle\text{travelTo}\rangle\, r')$$

...

Information-flow properties

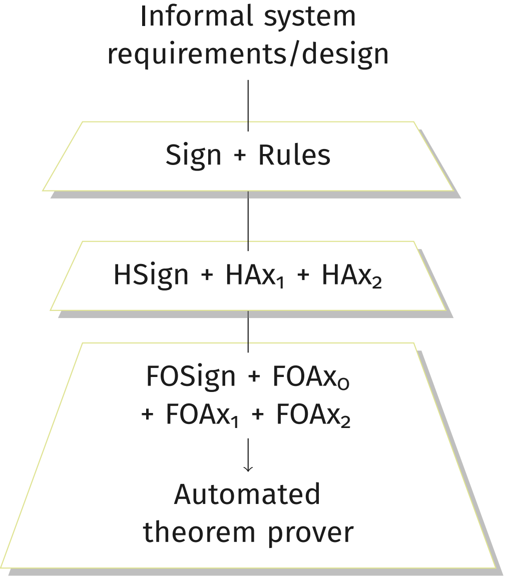
- If a region has a free dock, then no reward is offered there.

  $\forall\, d\colon \mathsf{Dock} \cdot @_d\, (\mathsf{freeDock} \to [\pi]\, \neg\, \mathsf{rewardOffered})$

- If a reward is offered at a region, then a traveller is expected to arrive at that region.

  $\forall\, r\colon \mathsf{Region} \cdot @_r\, \mathsf{rewardOffered} \to \exists\, u\colon \mathsf{User} \cdot @_u\, \langle \mathsf{travelTo} \rangle\, r$

Challenges in automated verification


Informal system requirements/design
Sign + Rules
HSign + HAx$_1$ + HAx$_2$
FOSign + FOAx$_0$ + FOAx$_1$ + FOAx$_2$
Automated theorem prover

- size
- complexity
- reliance on FO theorem provers
- limited theorem-proving support for hybrid logic
- finding suitable lemmas

Thank you!