Principles of Stepwise Refinement

Heiko Mantel

Deduction and Multiagent Systems Lab

German Research Center for Artificial Intelligence (DFKI)

Saarbrücken, Germany

PRL Seminar

Important Research Areas (incomplete)

Existing Refinement Concepts (incomplete)

Hoare 72

GoguenThatcherWagner 78, SannellaTarlecki 88, Reif 91

Back 88

LynchTuttle 87

AbadiLamport 91

Overview (Part I)

Part I: Structure the jungle

Part II: What are the important problems?

Part III: The solutions

Introduction

Modeling systems by sets of traces

Modeling principles

Example: refinement in TLA

Future directions

Modeling System Executions

A state s

A system can be modeled by a set of traces.

A specification corresponds to a set of systems.

Usually, sets of traces are considered instead of sets of sets.

Safety and liveness prdperties [AlpernSchneider 85]

Theorem: Every prdperty is the intersection of a safety and a live40.8ss property. [AlpernSchneider 85]

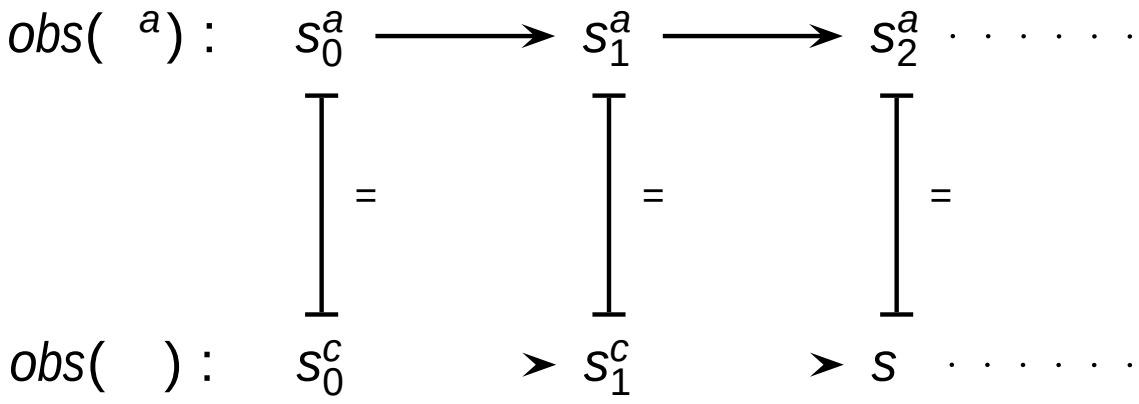
Principles of Refinement

Refinement of the set of traces S^c $_D$ S^a

S_c S_a

Design

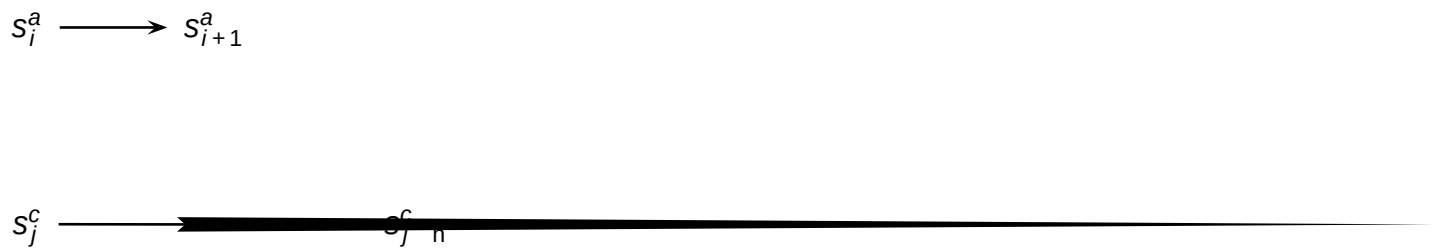
Refinement of single traces S^c $obsS^a$



Computation/R

Classes of Observation Functions

refinement of computation



What is my point?

For other specification formalisms use the intuition of these principles (Design/Computation/Representation).

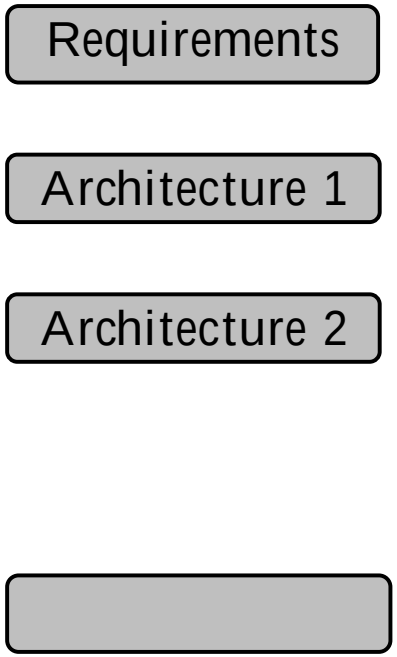
The principles can be c

Looking at the basic principles helps in understanding a possibly complicated refinement concept. $=)$ ex

The basic principles help in identifying which properties are preserved under refinement.

Given properties which should be preserved one can construct the appropriate refinement concept. $=)$ development process

The Development Process



TLA

syntax: $t^{\theta}, F_f, \quad F, WF(F), SF(F), \ldots$

semantic:

Data Race Conditions

```
{
```

Refinement in TLA

A concrete specification S^c refines an abstract specification S^a

iff

$S^c \quad S^a$

$=)$ looks like refinement of design principle

{

Principles of Refinement in TLA

refinement of design p

refinement of computation p

equivalence under stuttering

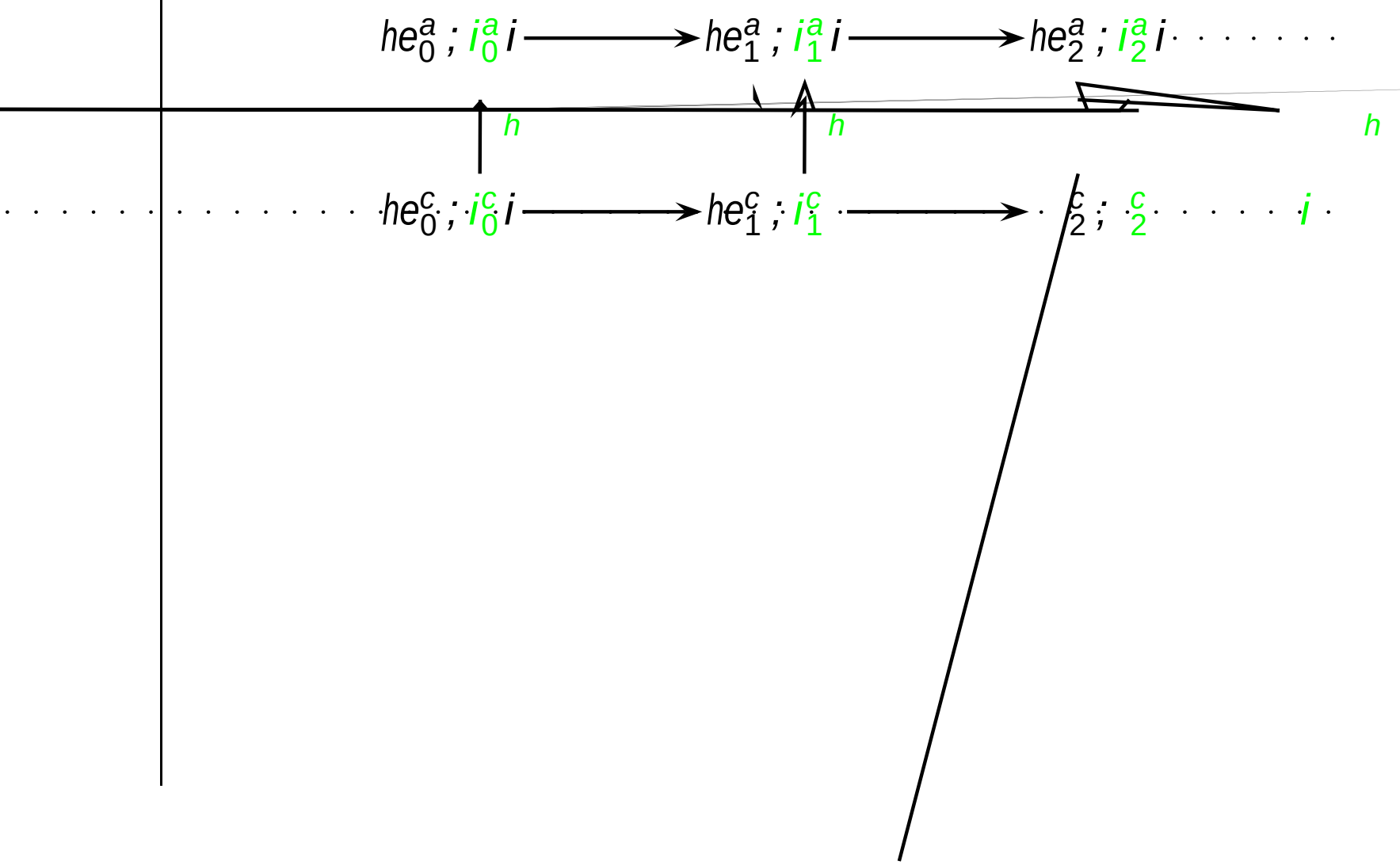
{ in combination with hiding

refinement of state space p

{ hiding

refinement of representation

Refinement Mappings



How to apply a Refinement Step?

Invent and Verify

- A specification is invented and then verified against a more abstract specification.
- [illegible]
- [illegible]

[illegible]

- Intelligence is required in choosing a rule (and in verifying side conditions).
- Apply known transfomation hoping to achieve the goal.

Future Directions

identify the basic principles in other refinement concepts

compare refinement concepts in the framework

prepare 2nd talk in this series

What are the important problems?

prepare 3rd talk in this series

The solutions

use the techniques in a real world project