Towards Automatic Update of Access Control Policy

Jinwei Hu, Yan Zhang, Ruixuan Li

Huazhong University of Science and Technology, Wuhan, China
University of Western Sydney, Sydney, Australia

jwhu@hust.edu.cn

Contents

- Motivations and Background
- Key Questions
- Ideas
- Conclusions

Contents

- Motivations and Background
- Key Questions
- Ideas
- Conclusions

Motivations - Why Update?

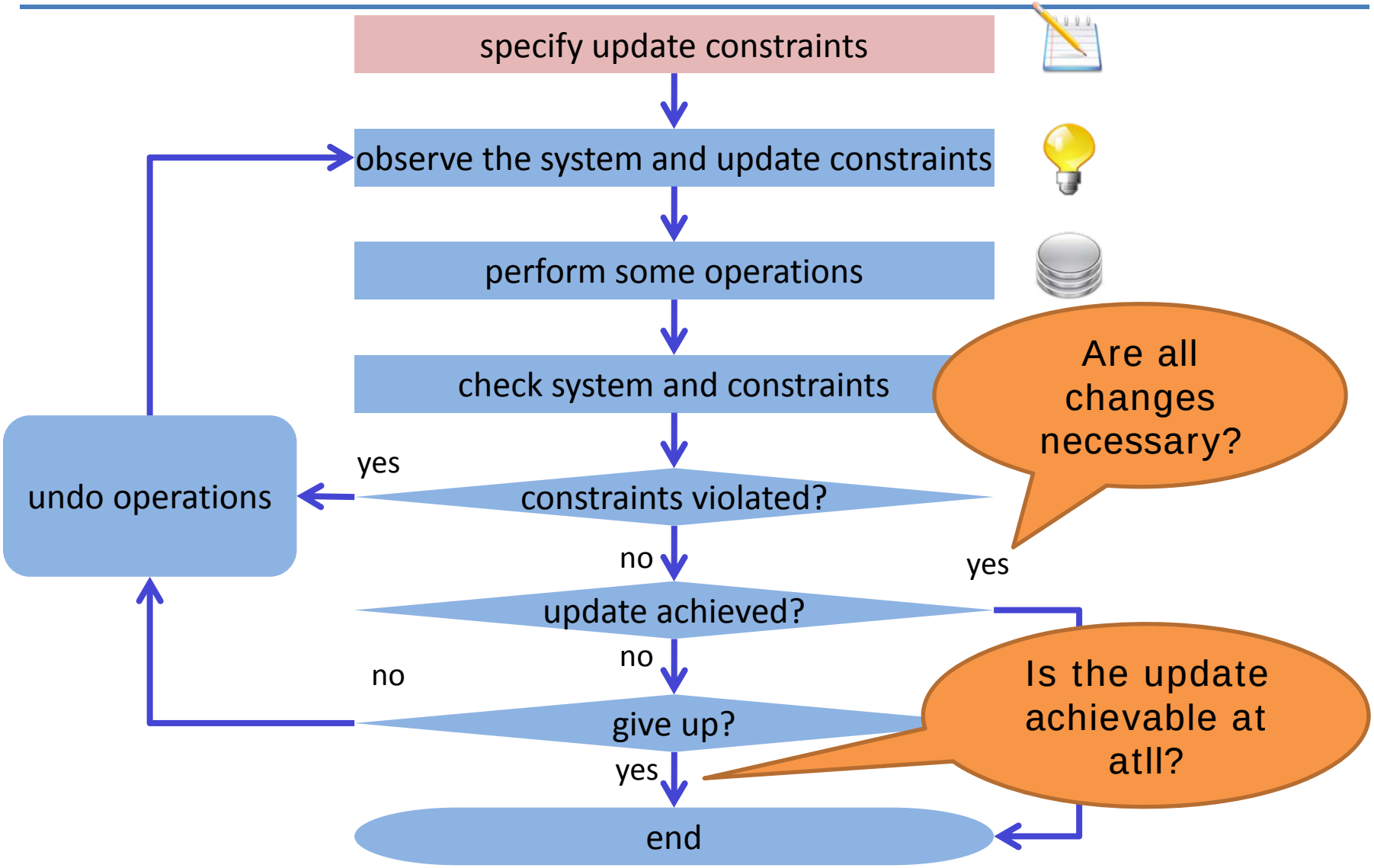
- Misconfigurations [SACMAT'08, USENIX SEC'10]

- Permission Assignment
  - A new user joins
  - Task assignment

- Property satisfactions [TISSEC]

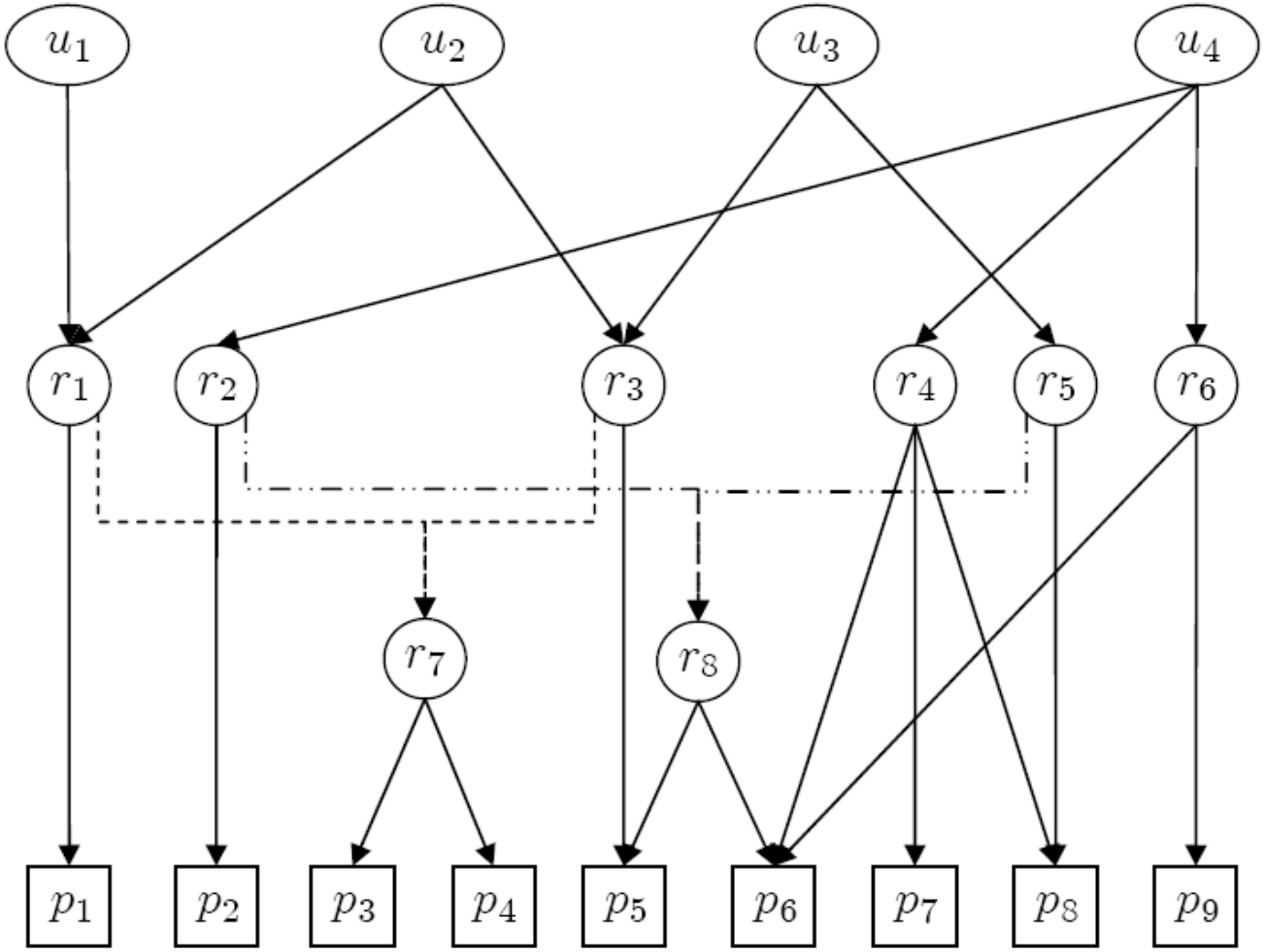
- Requirement dynamics [CACM]

Workflow of manual update



Background - RBAC Systems

- Role-based access control



Contents

- Motivations and Background
- Key Questions
- Ideas
- Conclusions

Key Questions

- Q1: What is the update objective?
  - Assign $\{p_5, p_8, p_9\}$ via $\{r_1, r_2, r_3, r_4, r_5, r_6\}$

Key Questions

- Q1: What is the update objective?
- Q2: Who is to implement the update?
  - Different administrators come with different power.
  - Interactions/dependencies among administrators.

Key Questions

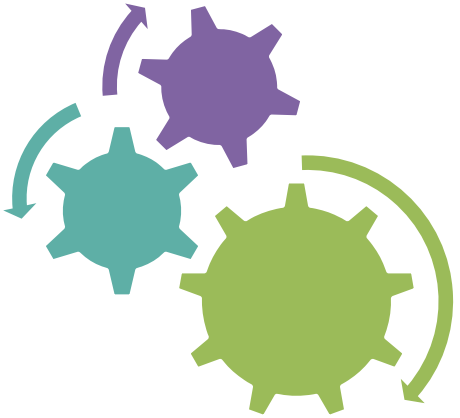
- Q1: What is the update objective?
- Q2: Who is to implement the update?
- Q3: What is the system behavior after update?
  - Can users still perform their works?

Consideration of Q3

- Users' permissions vary within range

  [lower bound, upper bound]

  - transparency to users
  - maintain access control system functions smoothly



Key Questions

- Q1: What is the update objective?
- Q2: Who is to implement the update?
- Q3: What is the system behavior after update?
- Q4: What are the tolerable changes to roles and role hierarchies?

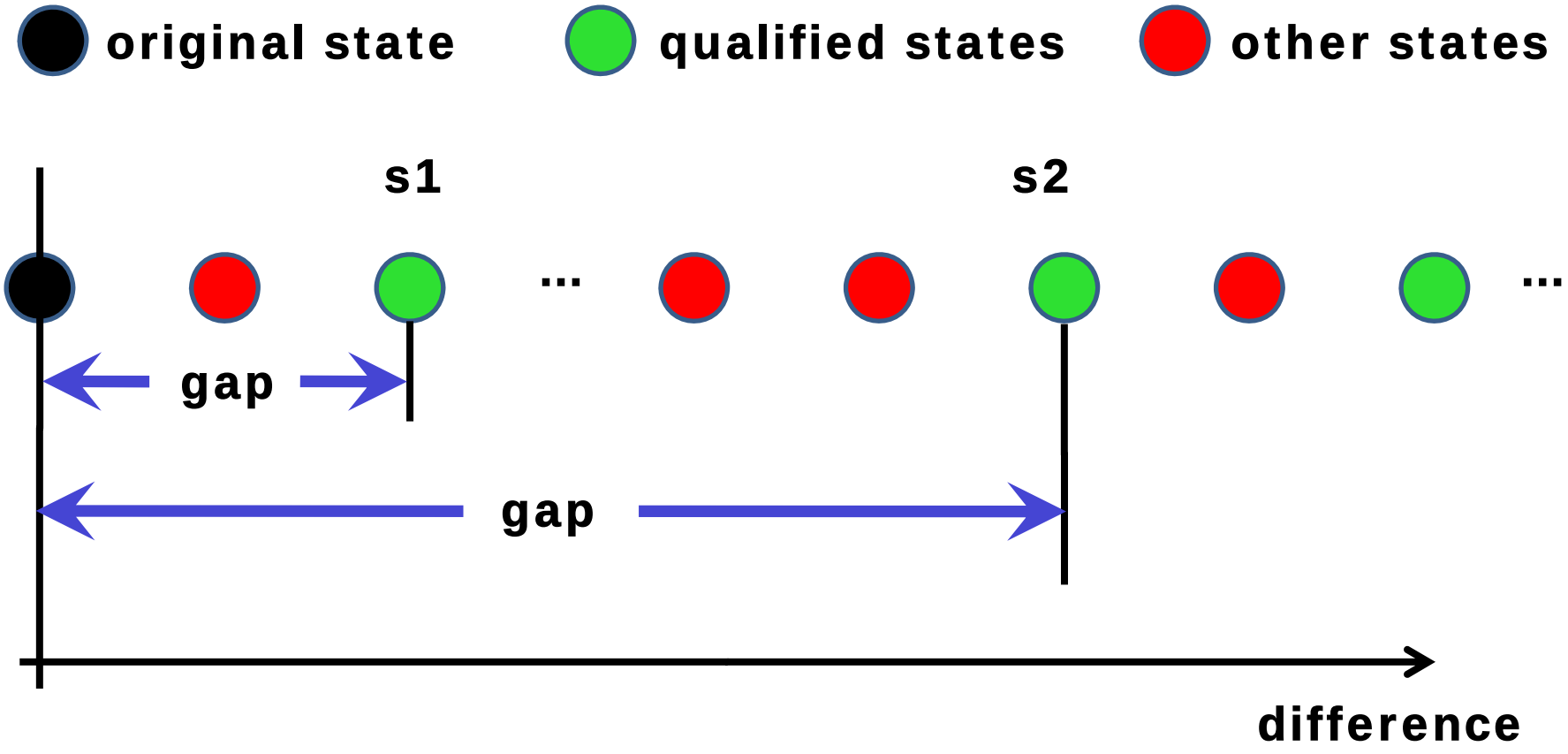
Consideration of Q4

- Role definitions
  - in terms of permissions, e.g., student = {use_printer, use_lab, ...}
- Top-down
  - Business meanings, semantics
- Bottom-up
  - role engineering/mining
- Role definitions change as needed? No change at all?

Key Questions

- Q1: What is the update objective?
- Q2: Who is to implement the update?
- Q3: What is the system behavior after update?
- Q4: What are the tolerable changes to roles and role hierarchies?
- Q5: Is an update optimal (minimal)?

Consideration of Q5



Which update is better, s1 or s2?

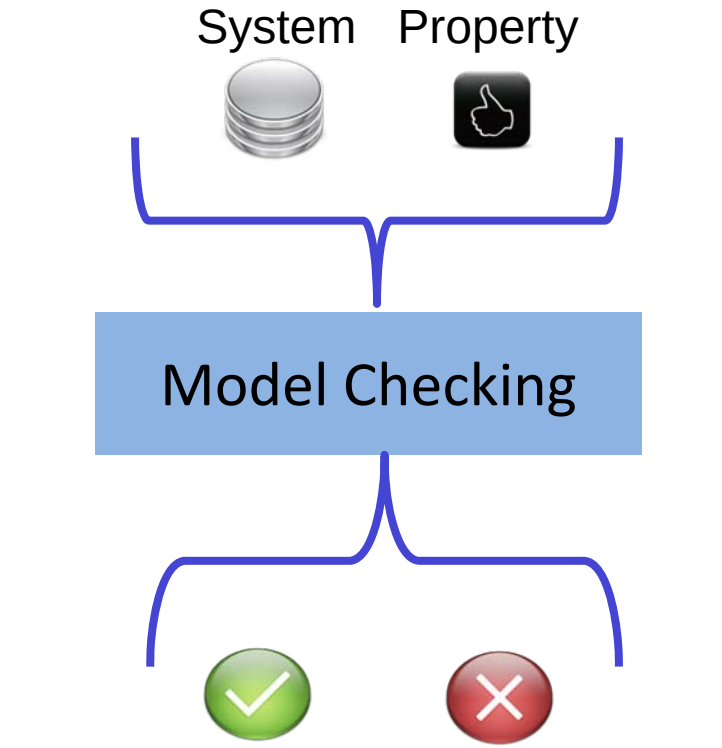
Contents

- Motivations and Background
- Key Questions
- Ideas
- Conclusions

Update specification

update
make $\mathcal{P} = \{p_5, p_8, p_9\}$ **available via** $\mathcal{T} = \{r_1, r_2, r_3, r_4, r_5, r_6\}$
with
administrators $admin_1$, $admin_2$;
user-permission constraints
(u_1, **no-less-than** $\{p_1\}$, **no-more-than** $\{p_1, p_3, p_4\}$),
(u_2, **no-less-than** $\{p_1, p_3, p_4, p_5\}$, **no-more-than** $\{p_1, p_3, p_4, p_5\}$),
(u_3, **no-less-than** $\{p_3, p_4, p_5\}$, **no-more-than** $\{p_3, p_4, p_5, p_6, p_8\}$),
(u_4, **no-less-than** $\{p_7, p_8, p_9\}$, **no-more-than** $\{p_3, p_5, p_6, p_7, p_8, p_9\}$);
restricted-role constraints
(r_4, **no-less-than** $\{p_6, p_7\}$, **no-more-than** $\{p_6, p_7, p_8, p_9\}$),
(r_8, **no-less-than** $\{p_5, p_6\}$, **no-more-than** $\{p_5, p_6\}$);
role-hierarchy = $\{(r_2, r_8), (r_3, r_7)\}$;
minimal;

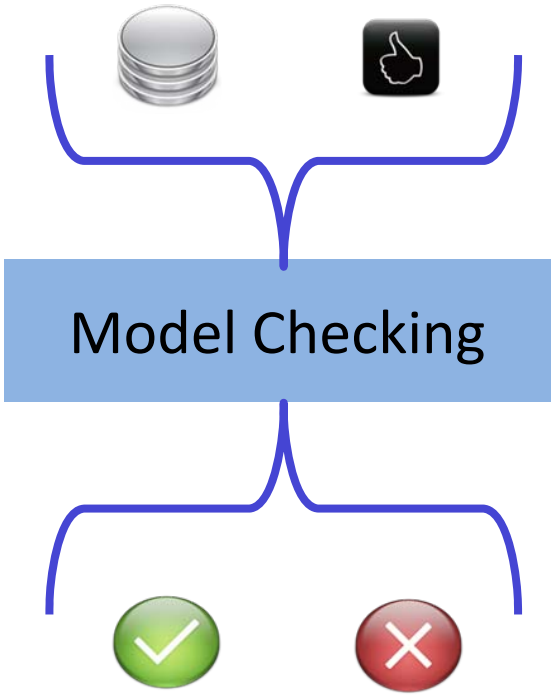
Model Checking



Updating via Model Checking

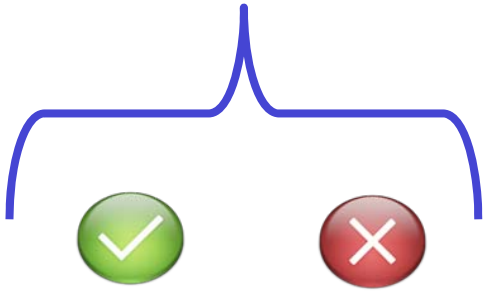
RBAC System

Property: Requested state is *never* reachable.



Property holds.

Property fails; A counter-example is generated.

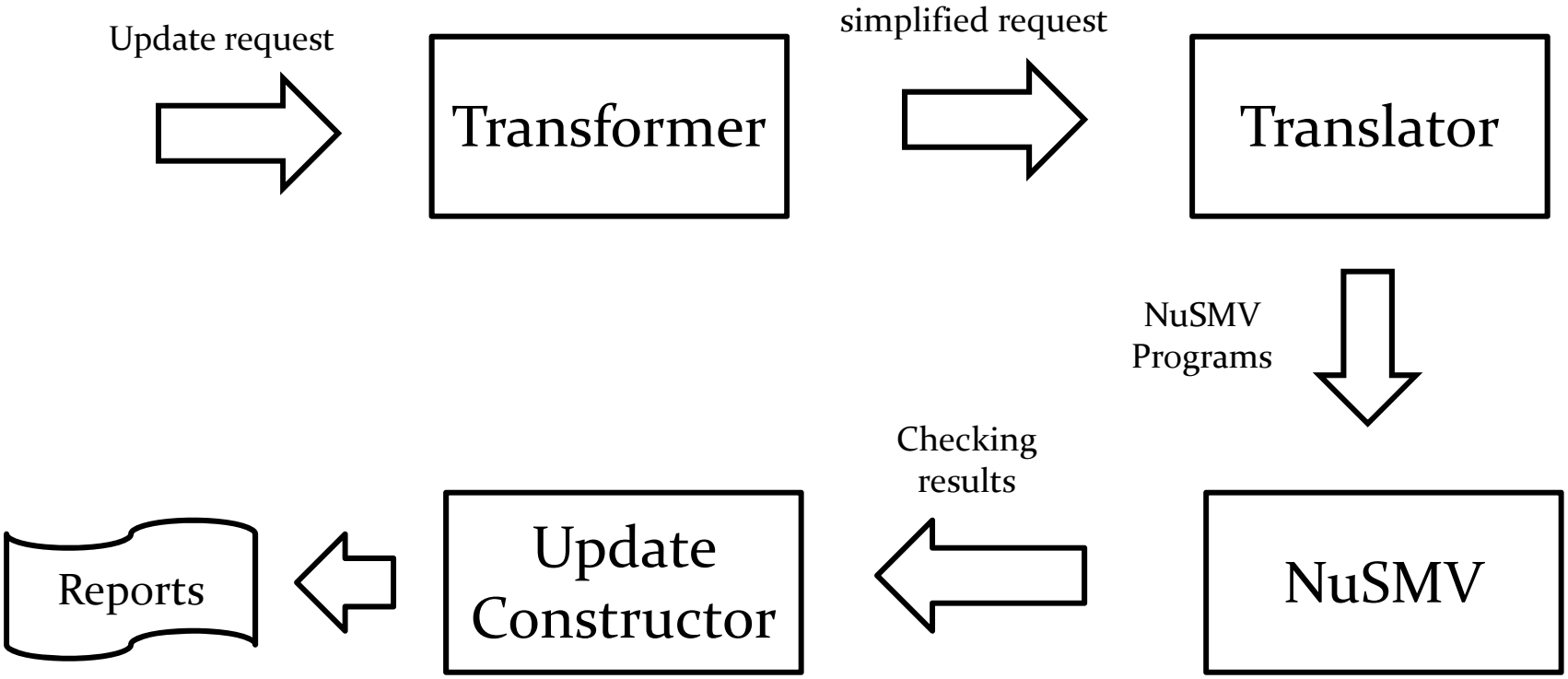


update achievable?

No. Requested state is never reachable.

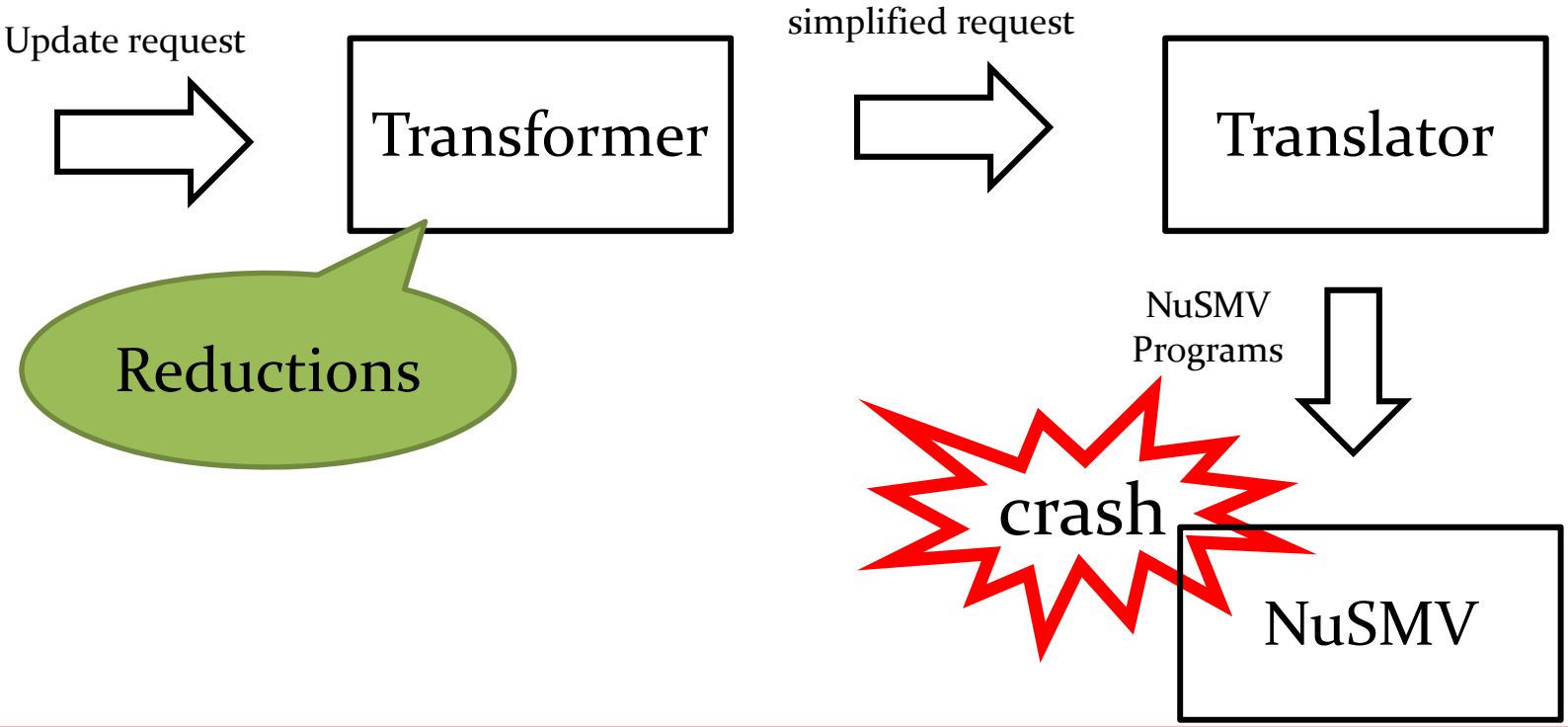
Yes. Requested state is *not* never reachable, and can be constructed from the counter-example.

Overview

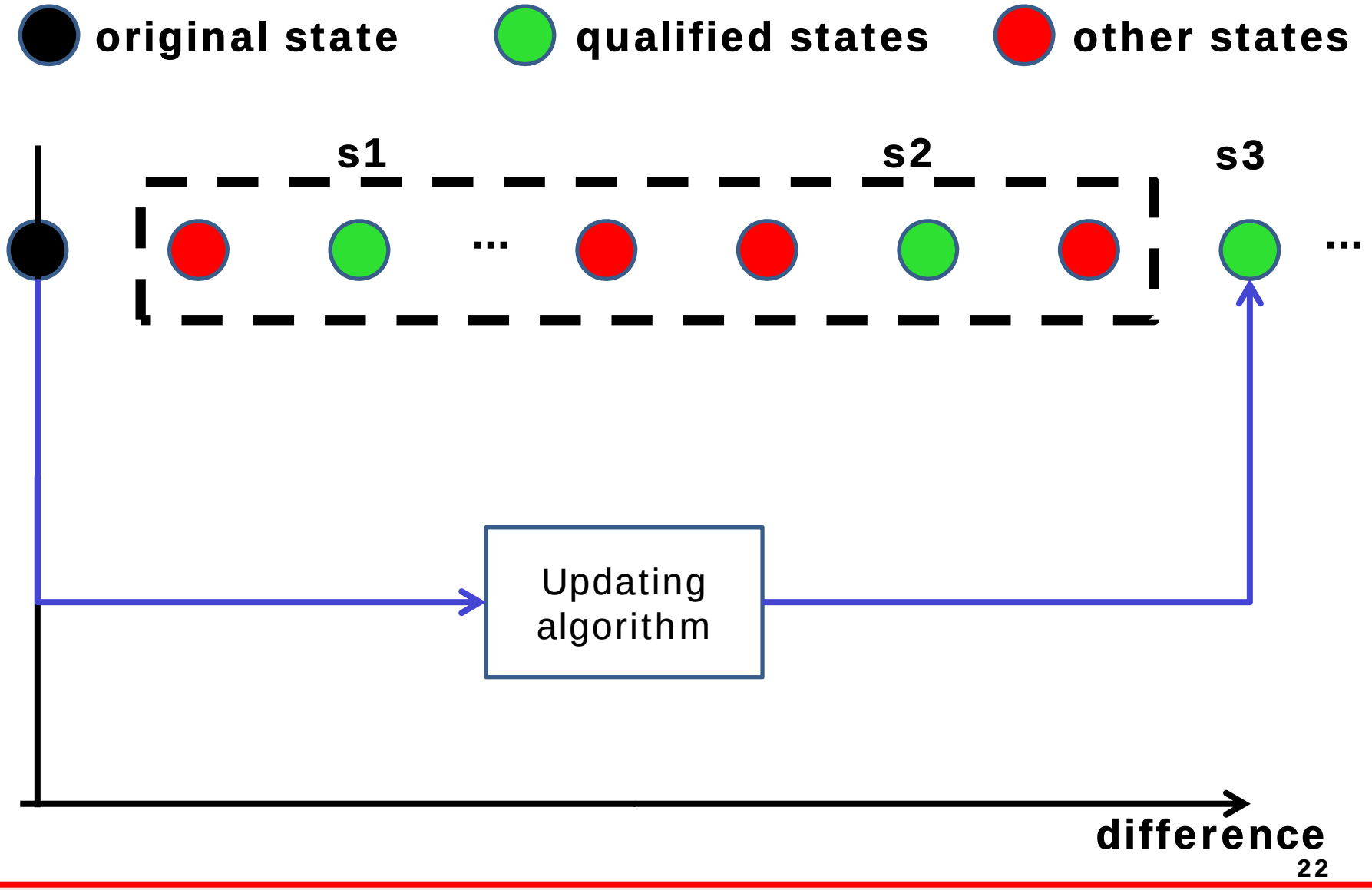

Update request
Transformer
simplified request
Translator
NuSMV
Programs
NuSMV
Checking
results
Update
Constructor
Reports

Problems

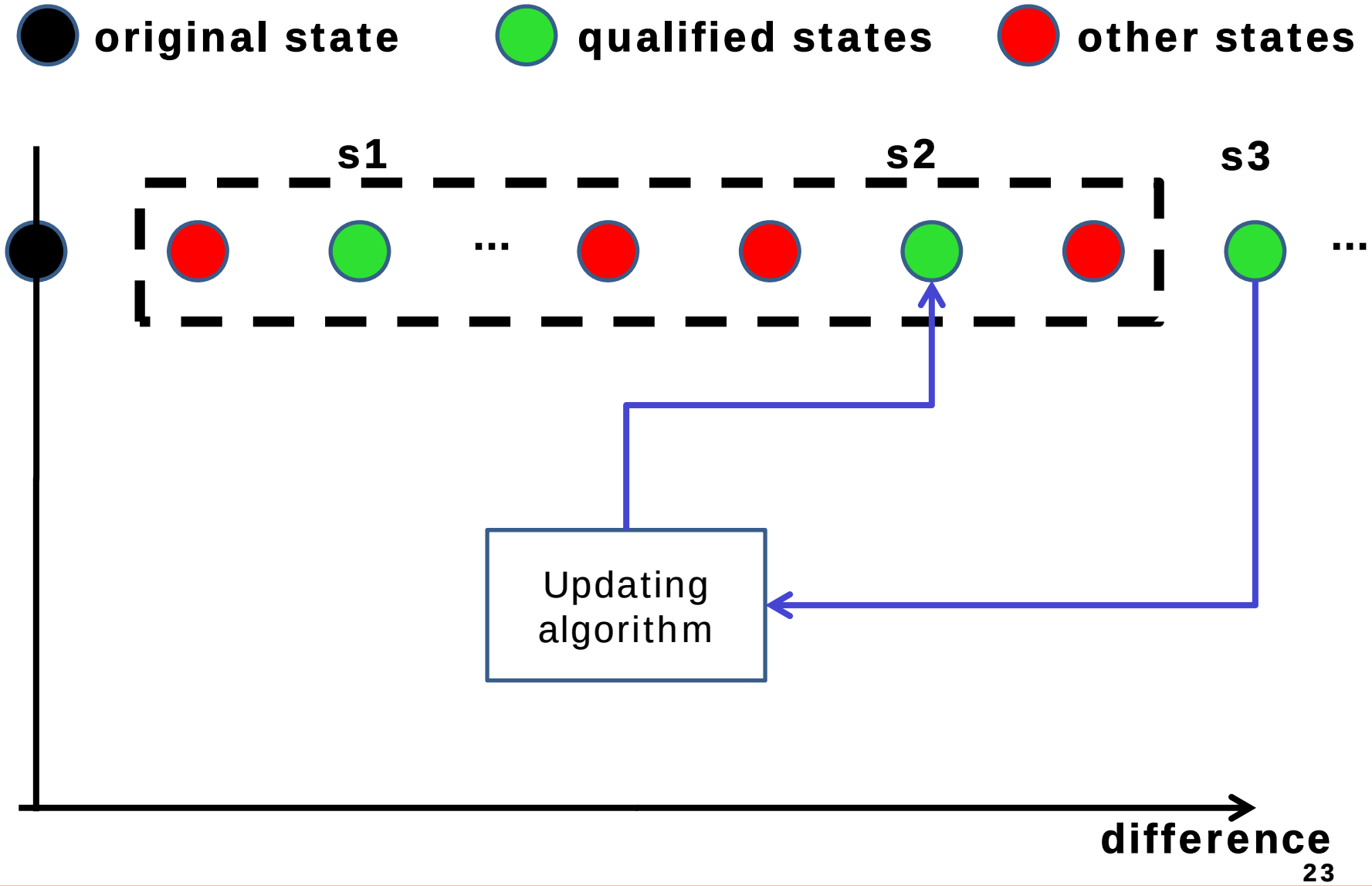
- State explosion problem
- Memory crash



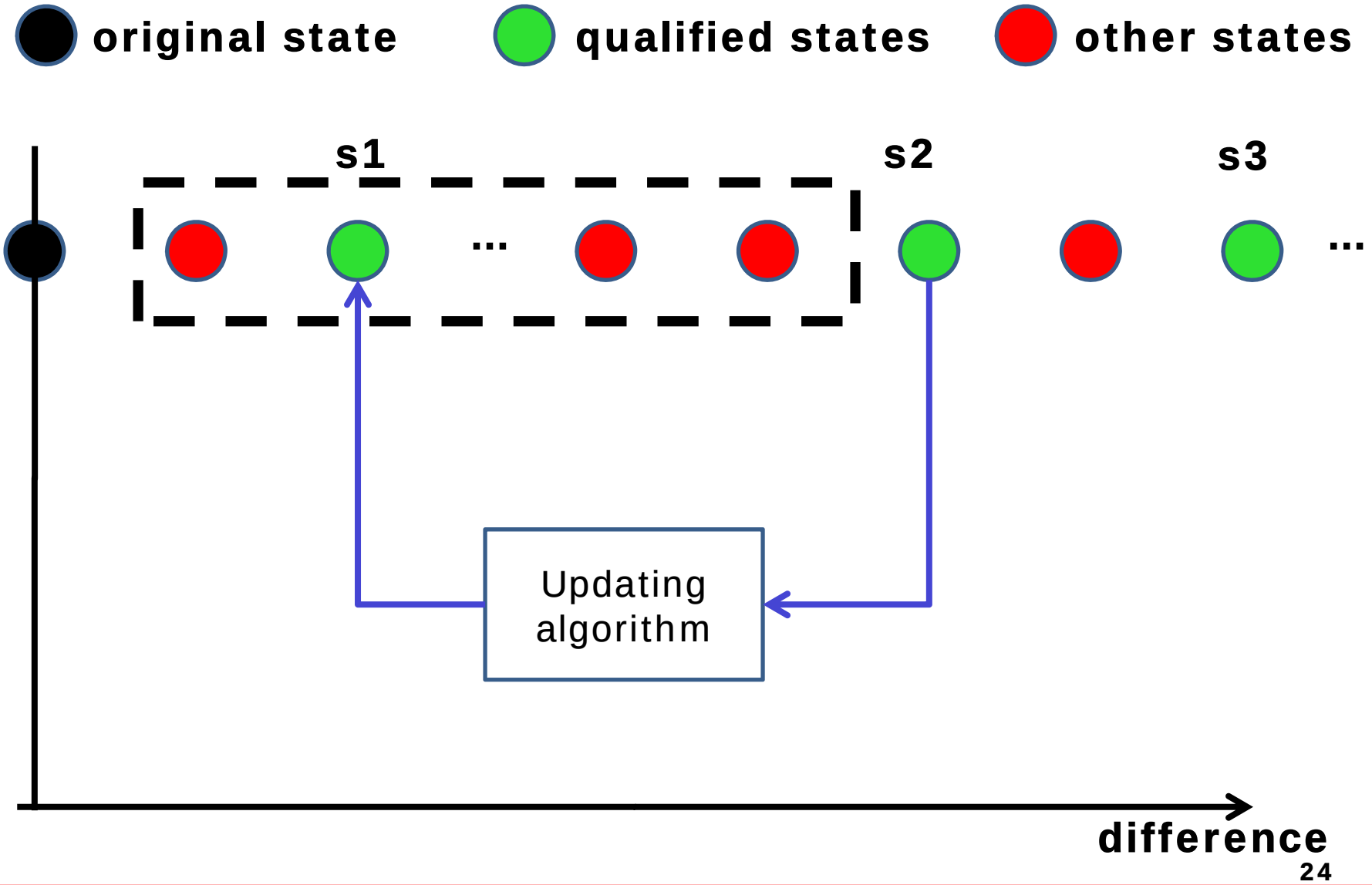
The Idea of Minimal Update



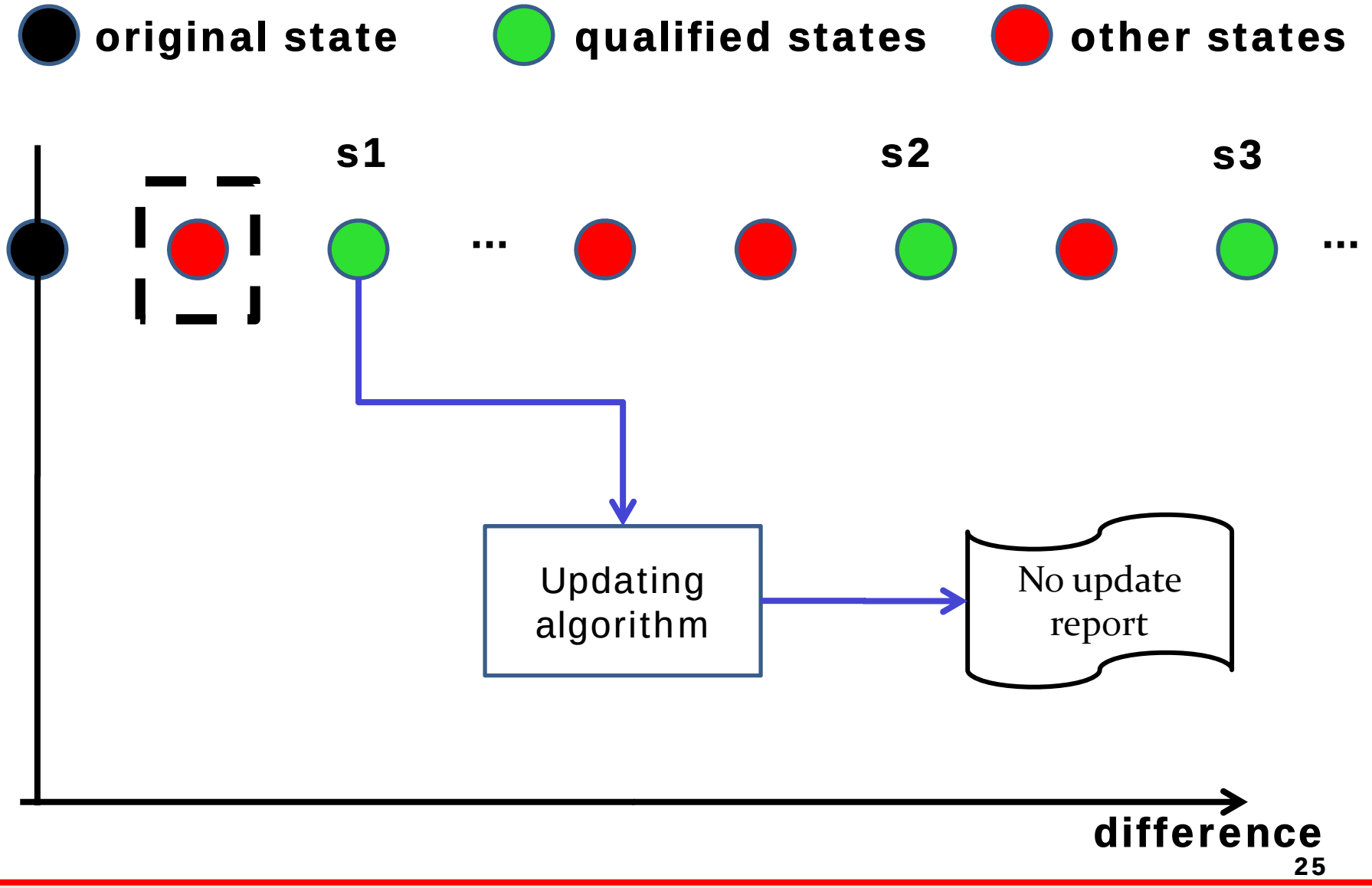
The Idea of Minimal Update



The Idea of Minimal Update



The Idea of Minimal Update



Contents

- Motivations and Background
- Key Questions
- Ideas
- Conclusions

Conclusions

- A tool that accepts and answers high-level update requests.
- Experiments (synthesized data)
- Future work
  - Full administrative model
  - Composition (sequence of update requests)

Thank you !