HiFrog: Interpolation-based Software Verification using Theory Refinement

Sepideh Asadi

joint work with Karine Even Mendoza, Grigory Fedyukovich, Antti Hyvärinen, Hana Chockler, Natasha Sharygina

Formal Verification and Security Lab

University of Lugano (USI), Switzerland

FMCAD 2017

What is HiFrog?

- An SMT-based bounded model checker for C

- Computes and reuses Function Summaries
  - Based on Craig interpolation

What is HiFrog?

- **An SMT-based bounded model checker for C**

- **Computes and reuses Function Summaries**
  - **Based on Craig interpolation**

- **Controllable interpolation system for SMT**
  - **Flexible in Size & Strength**
  - **Compact and readable summaries**

What is HiFrog?

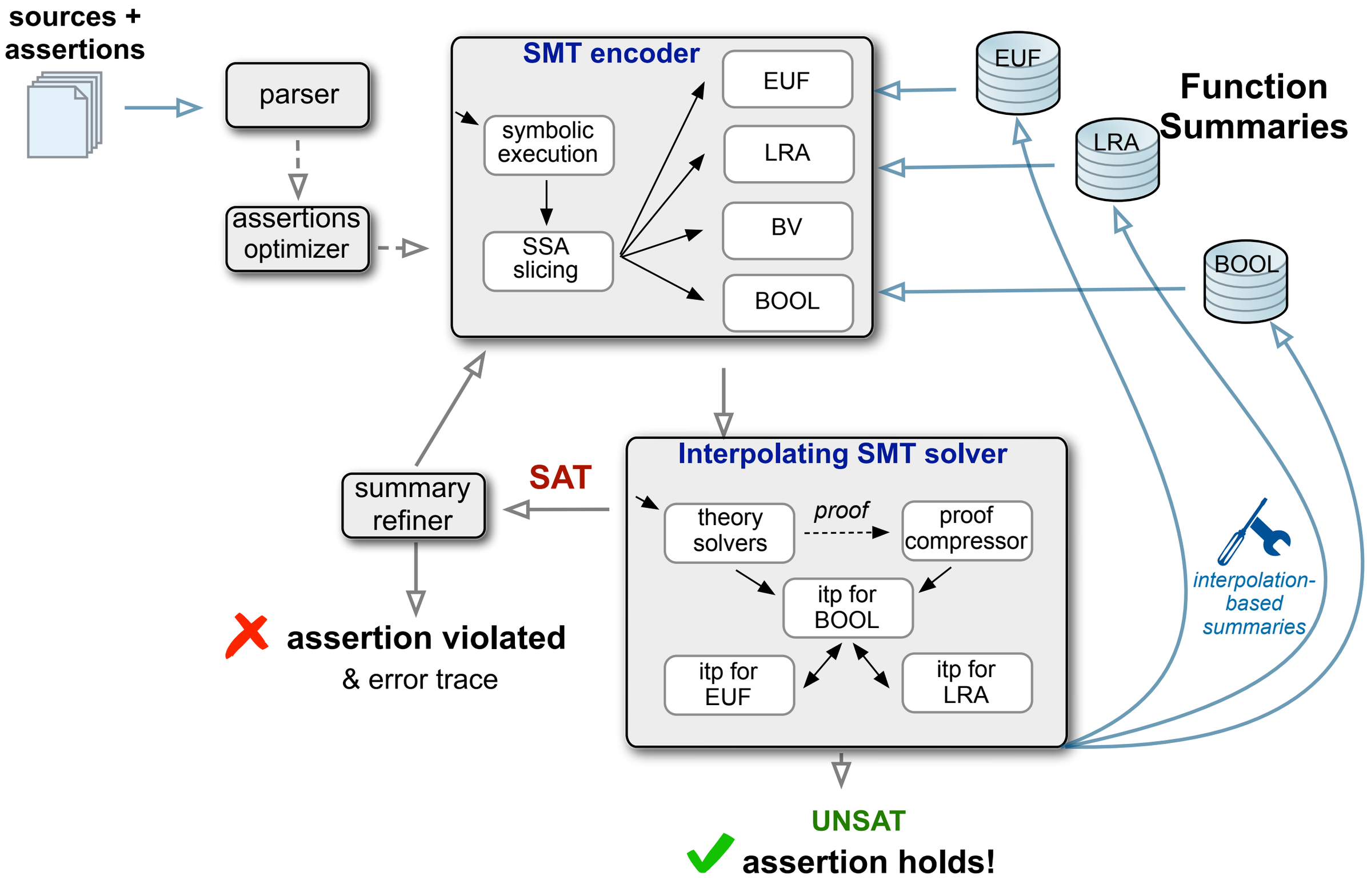
- **An SMT-based bounded model checker for C**

- **Computes and reuses Function Summaries**
  - **Based on Craig interpolation**

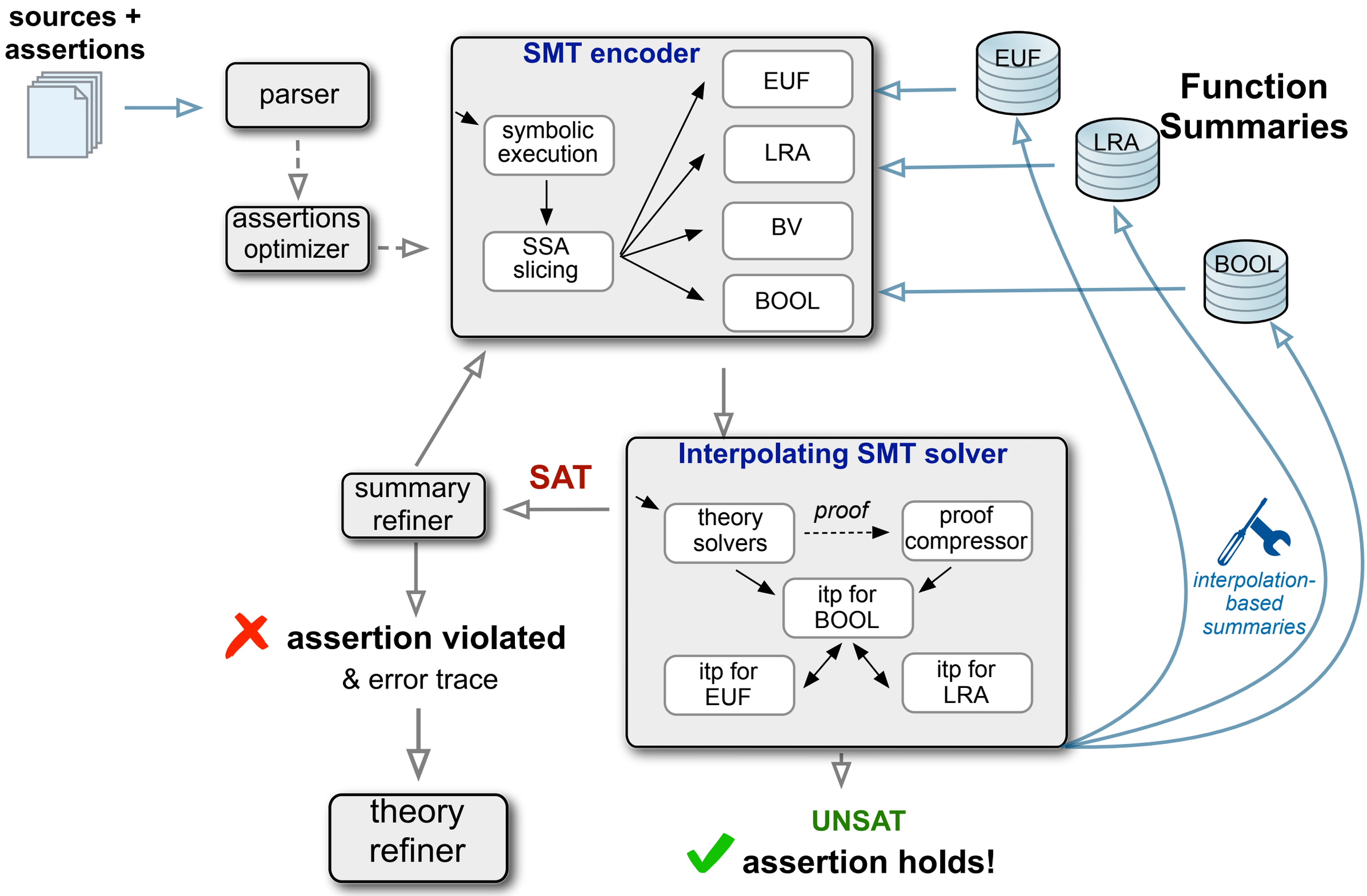
- **Controllable interpolation system for SMT**
  - **Flexible in Size & Strength**
  - **Compact and readable summaries**

- **Automatic adjustment of abstraction using different theories**
  - **Theory Refinement**

HiFrog and Function Summarization



HiFrog and Function Summarization

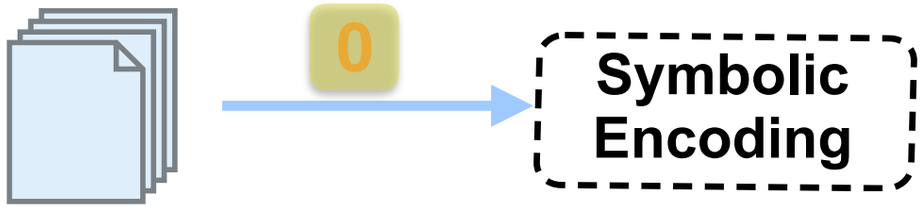


HiFrog and Theory Refinement

Università della Svizzera italiana

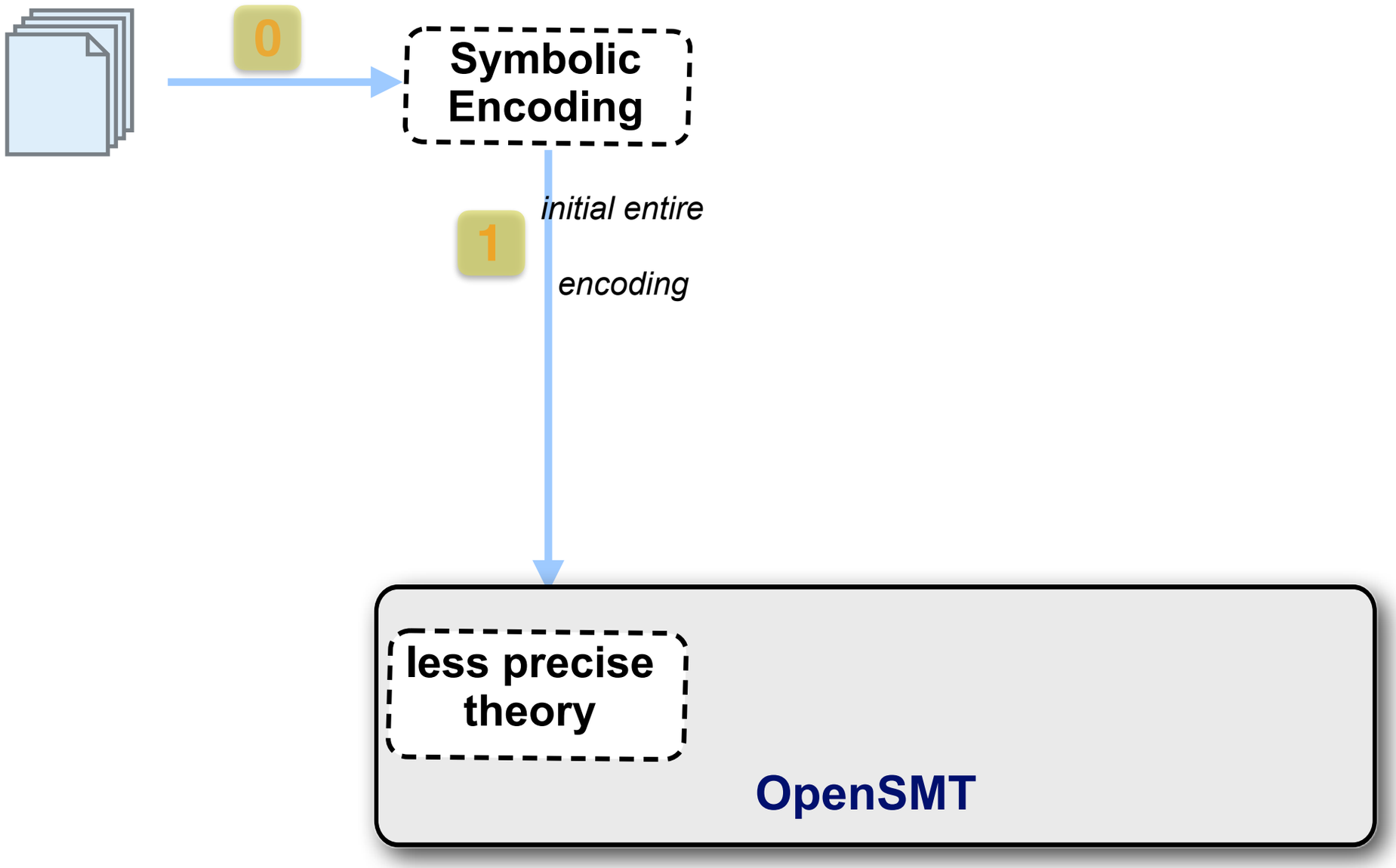
HiFrog and Theory Refinement

Program +
Assertions



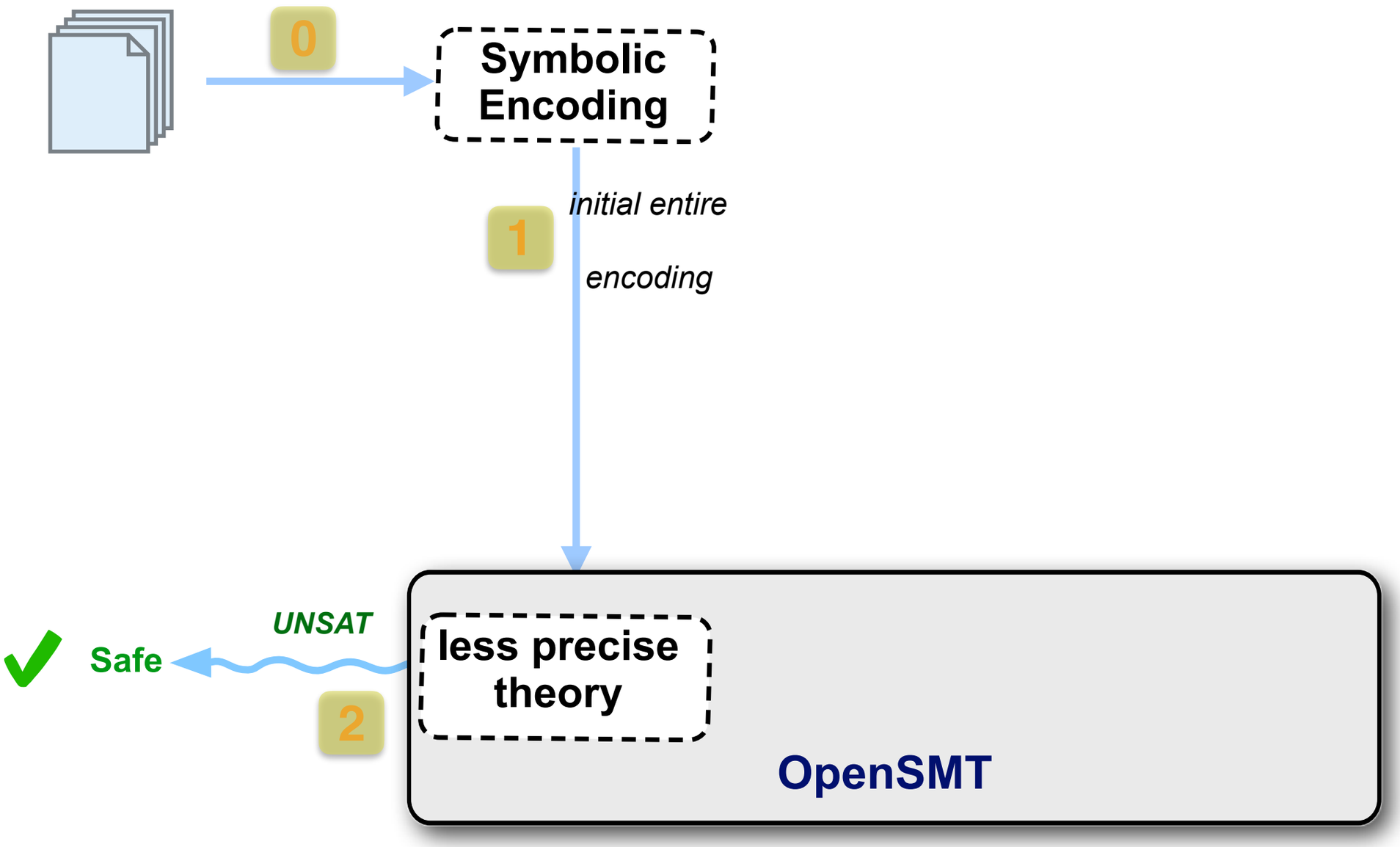
HiFrog and Theory Refinement

Program +
Assertions



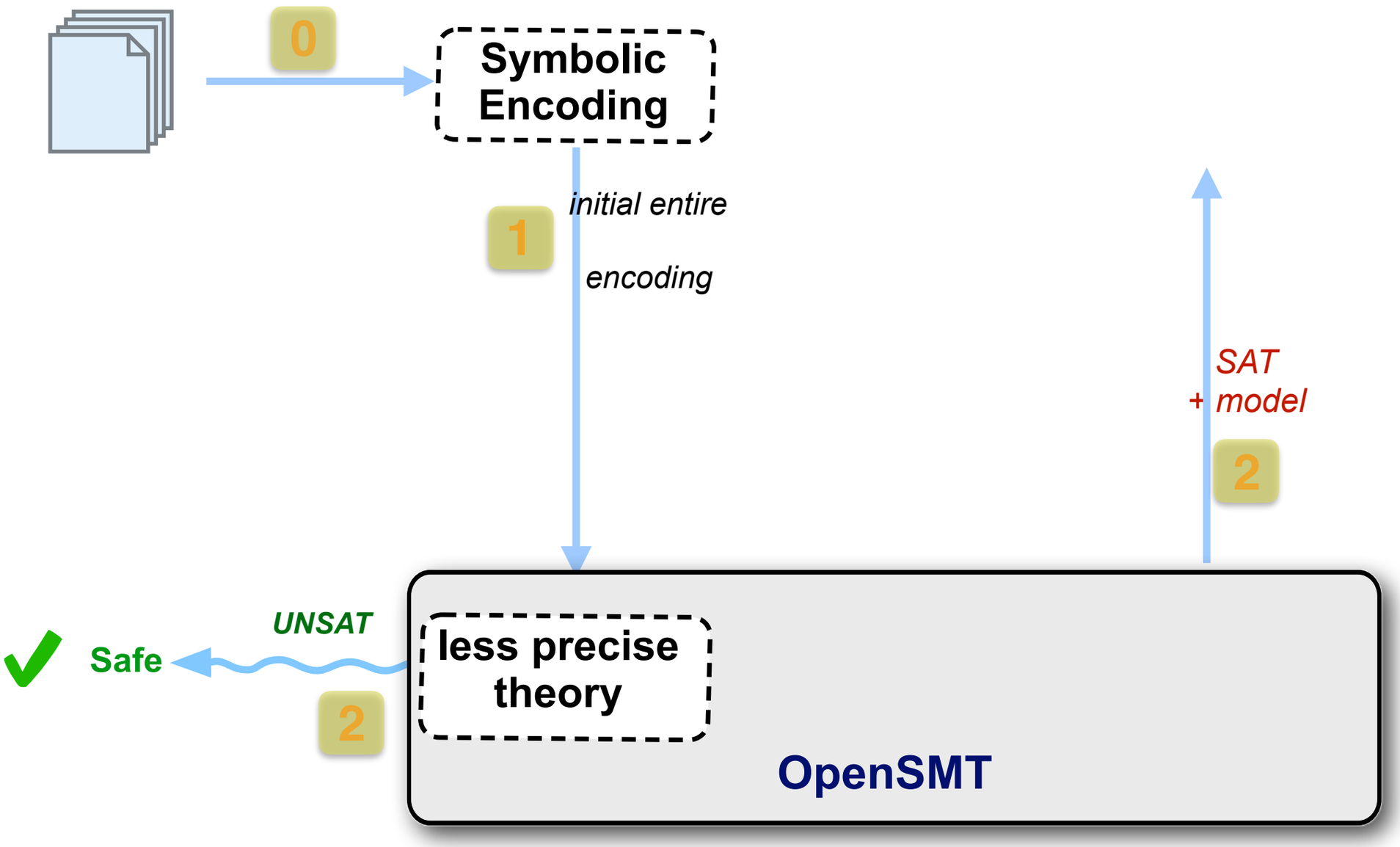
HiFrog and Theory Refinement

Program +
Assertions

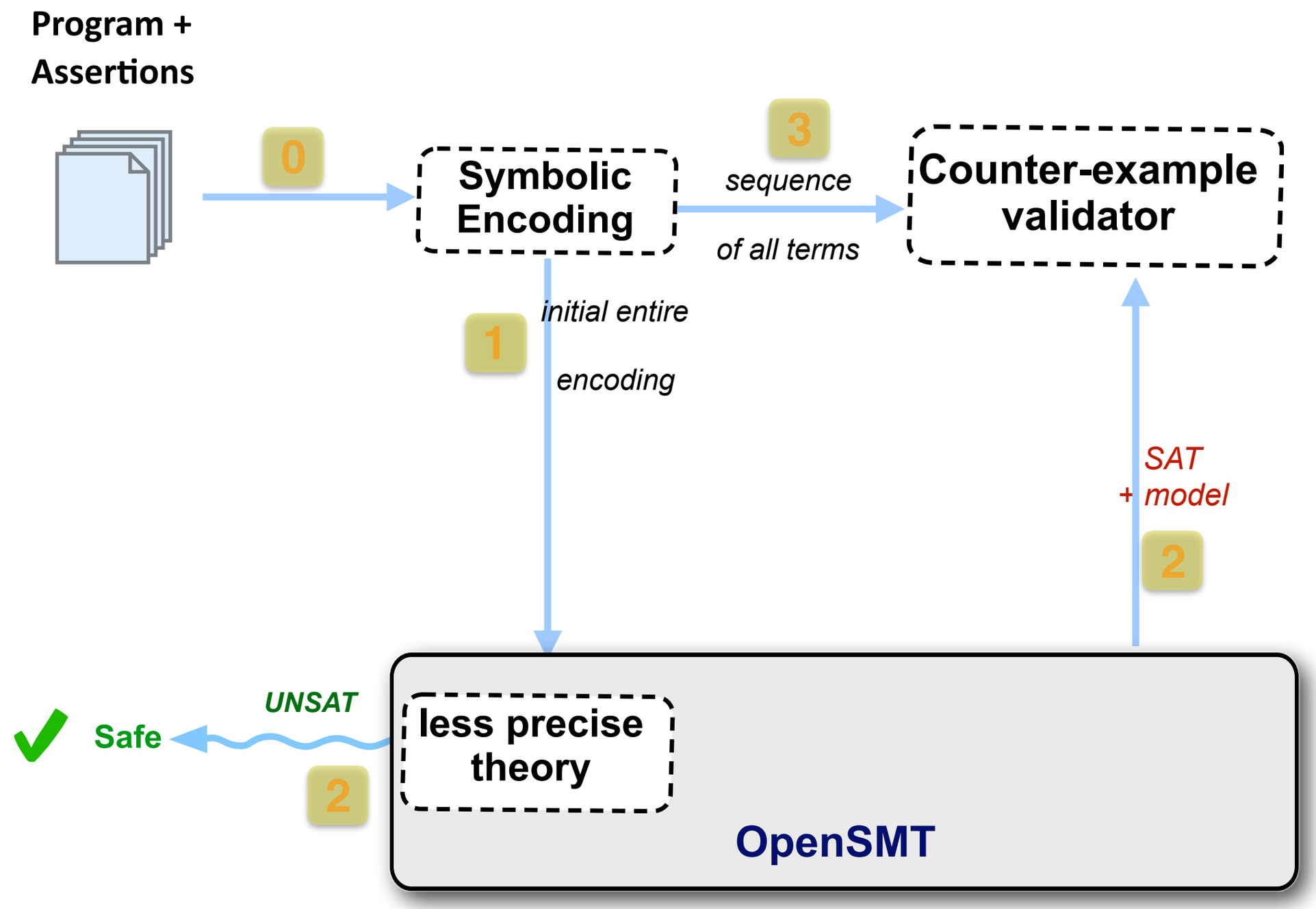


HiFrog and Theory Refinement

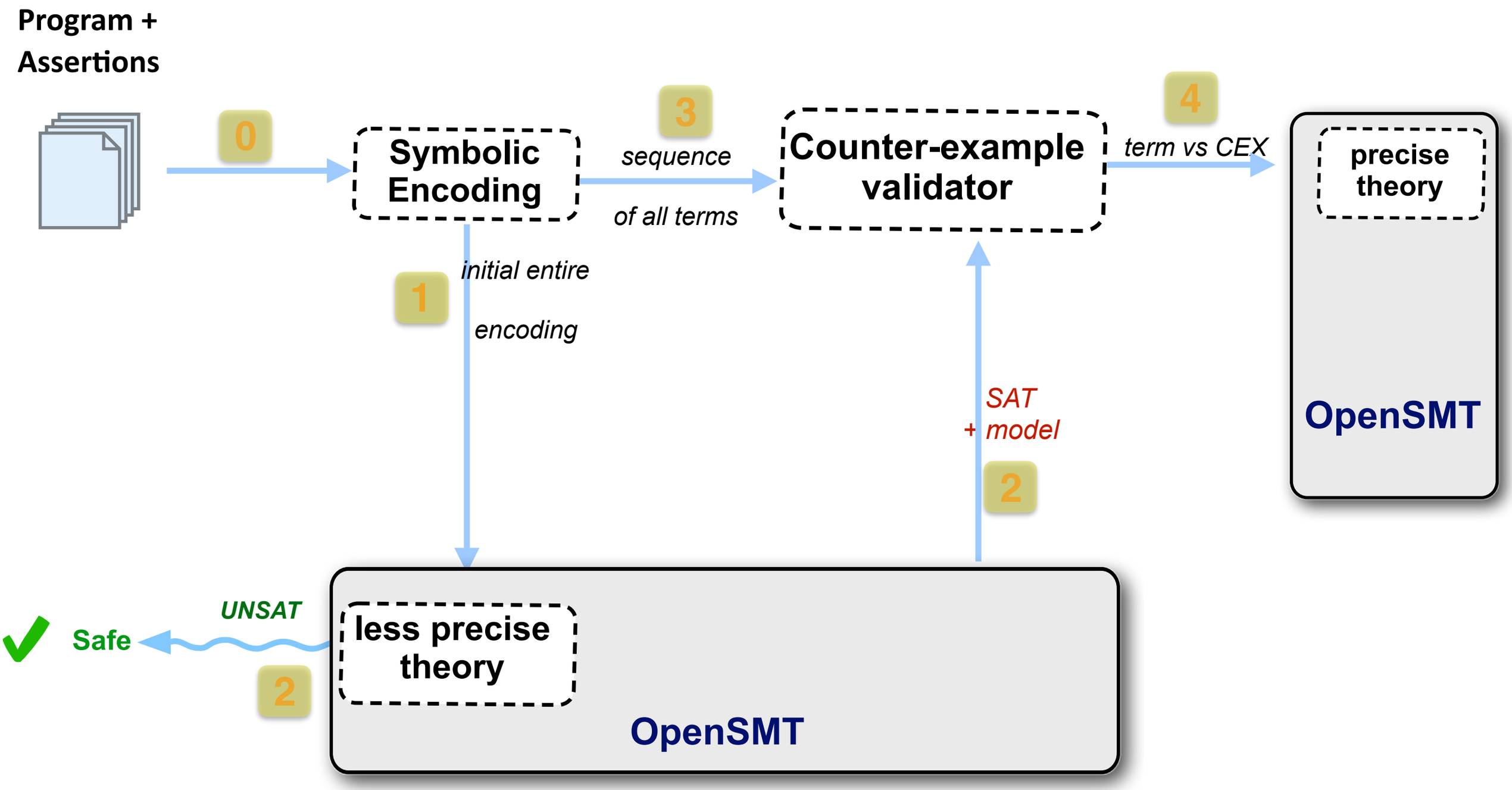
Program +
Assertions



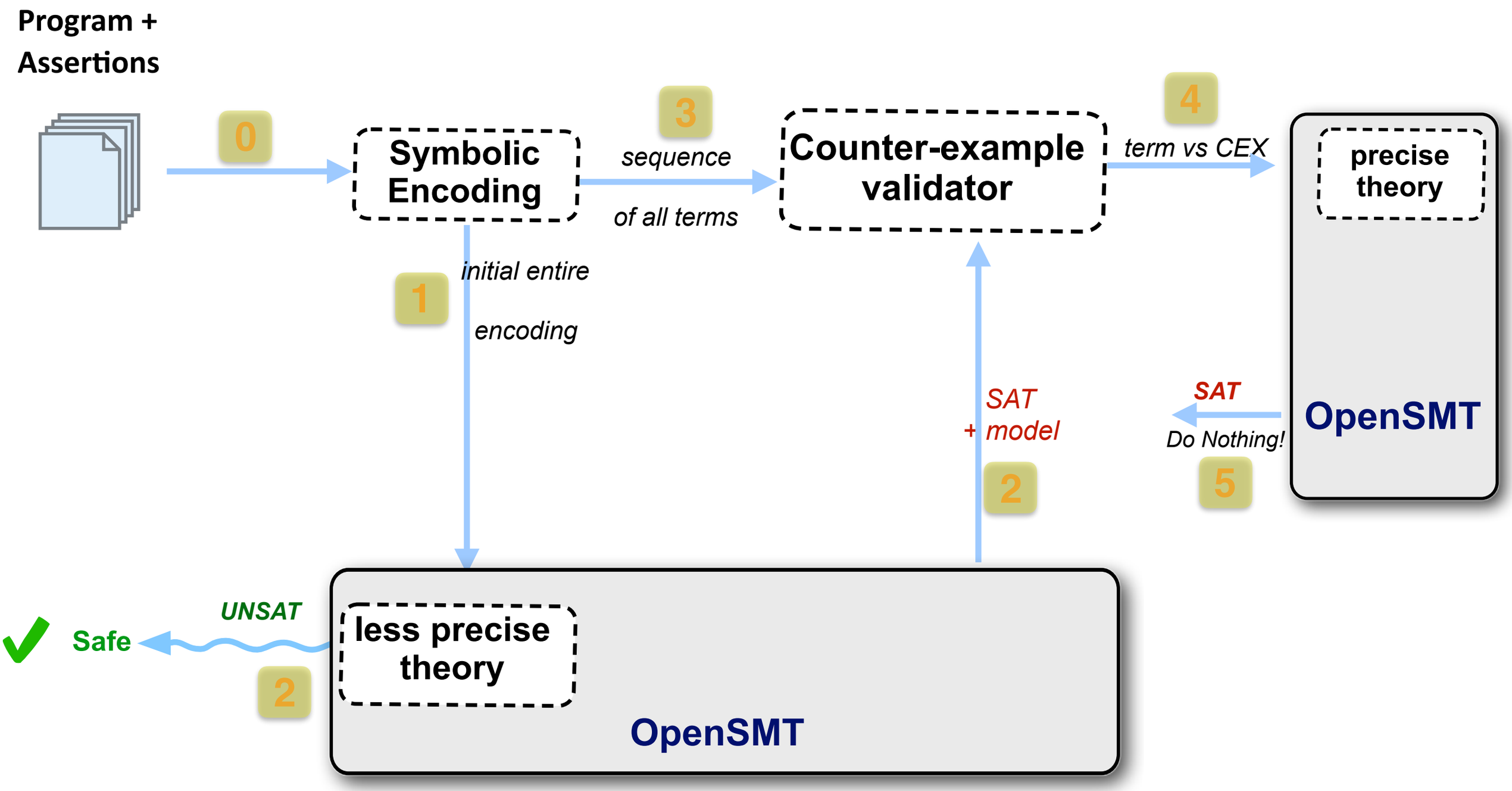
HiFrog and Theory Refinement



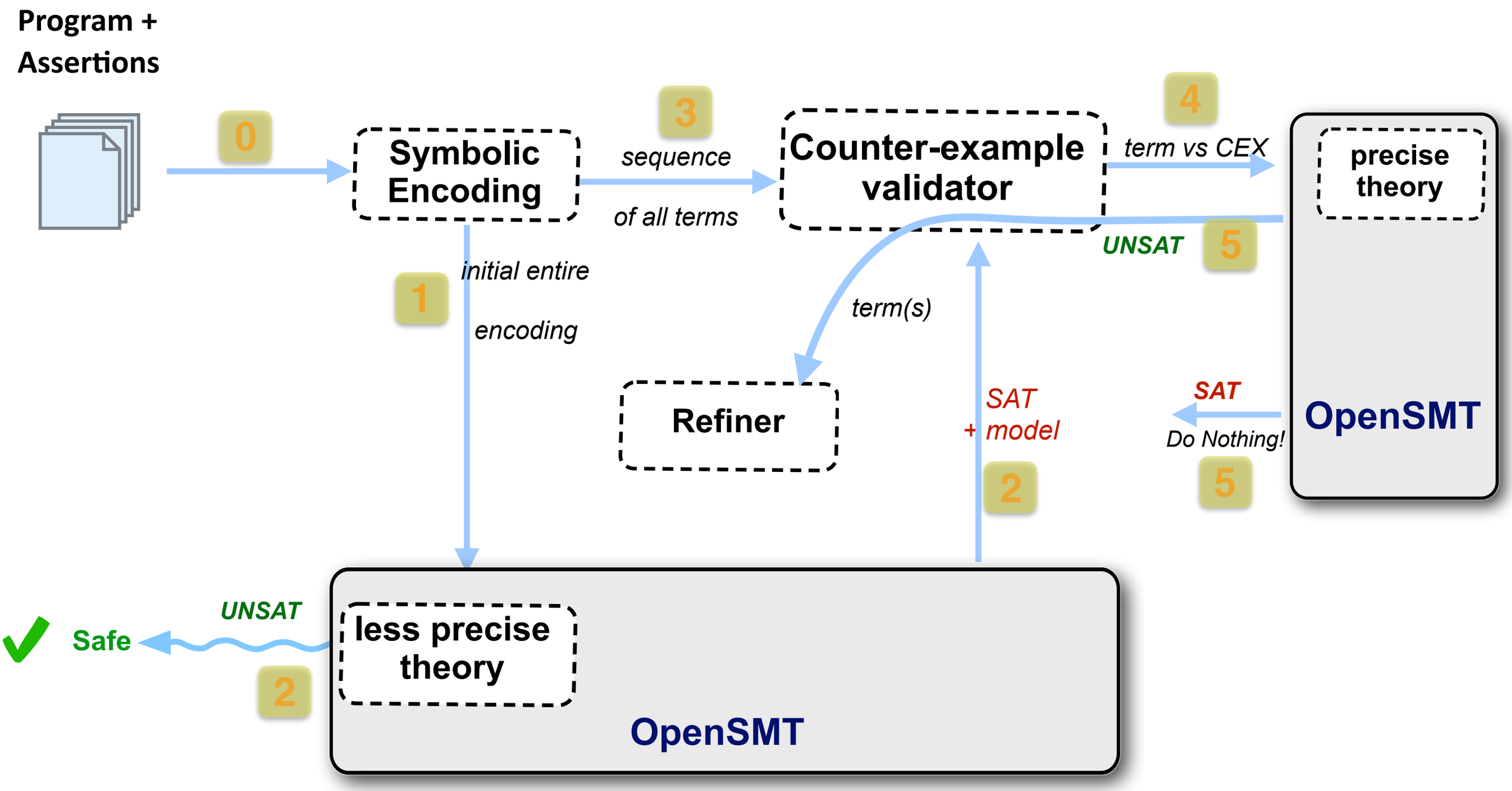
HiFrog and Theory Refinement



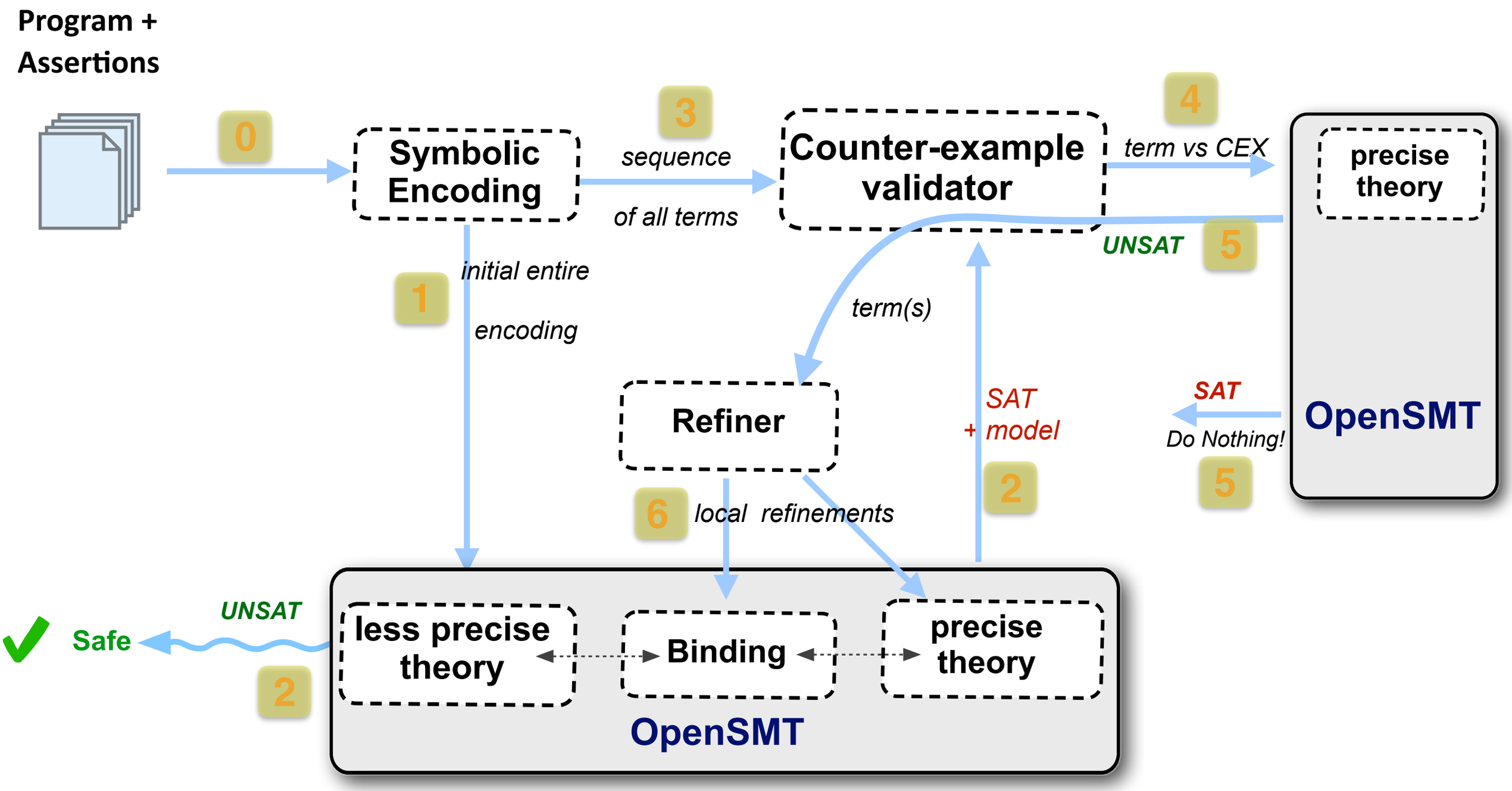
HiFrog and Theory Refinement



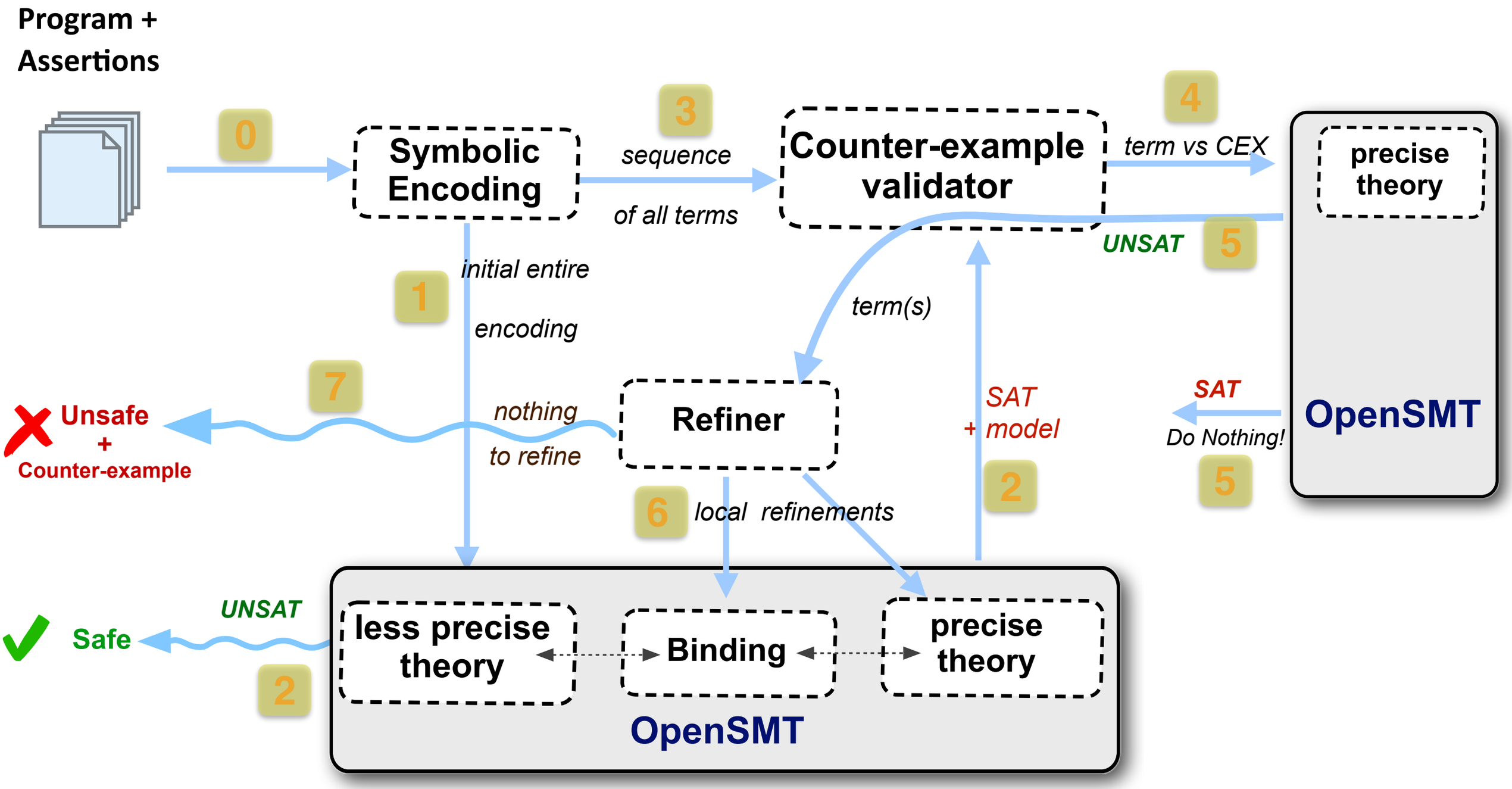
HiFrog and Theory Refinement



HiFrog and Theory Refinement



HiFrog and Theory Refinement



http://verify.inf.usi.ch/hifrog/

Looking forward to seeing you at poster sessions!