

# HiFrog: Interpolation-based Software Verification using Theory Refinement

**Sepideh Asadi**

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

**Formal Verification and Security Lab**  
**University of Lugano (USI), Switzerland**

FMCAD 2017



Università  
della  
Svizzera  
italiana

# 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

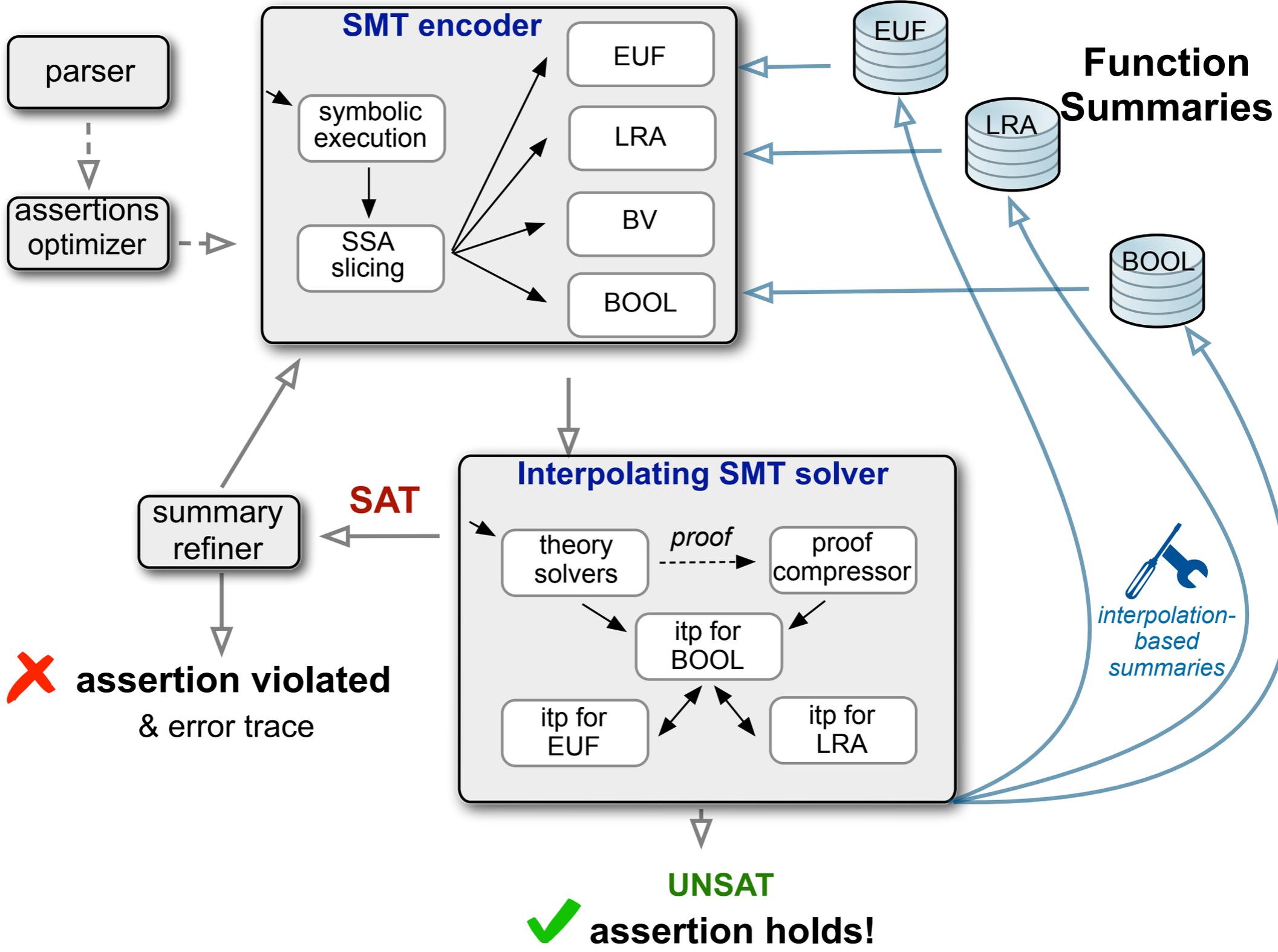
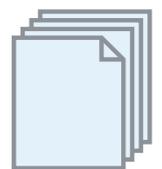
# What is HiFrog?



- 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

sources + assertions



**✗ assertion violated & error trace**

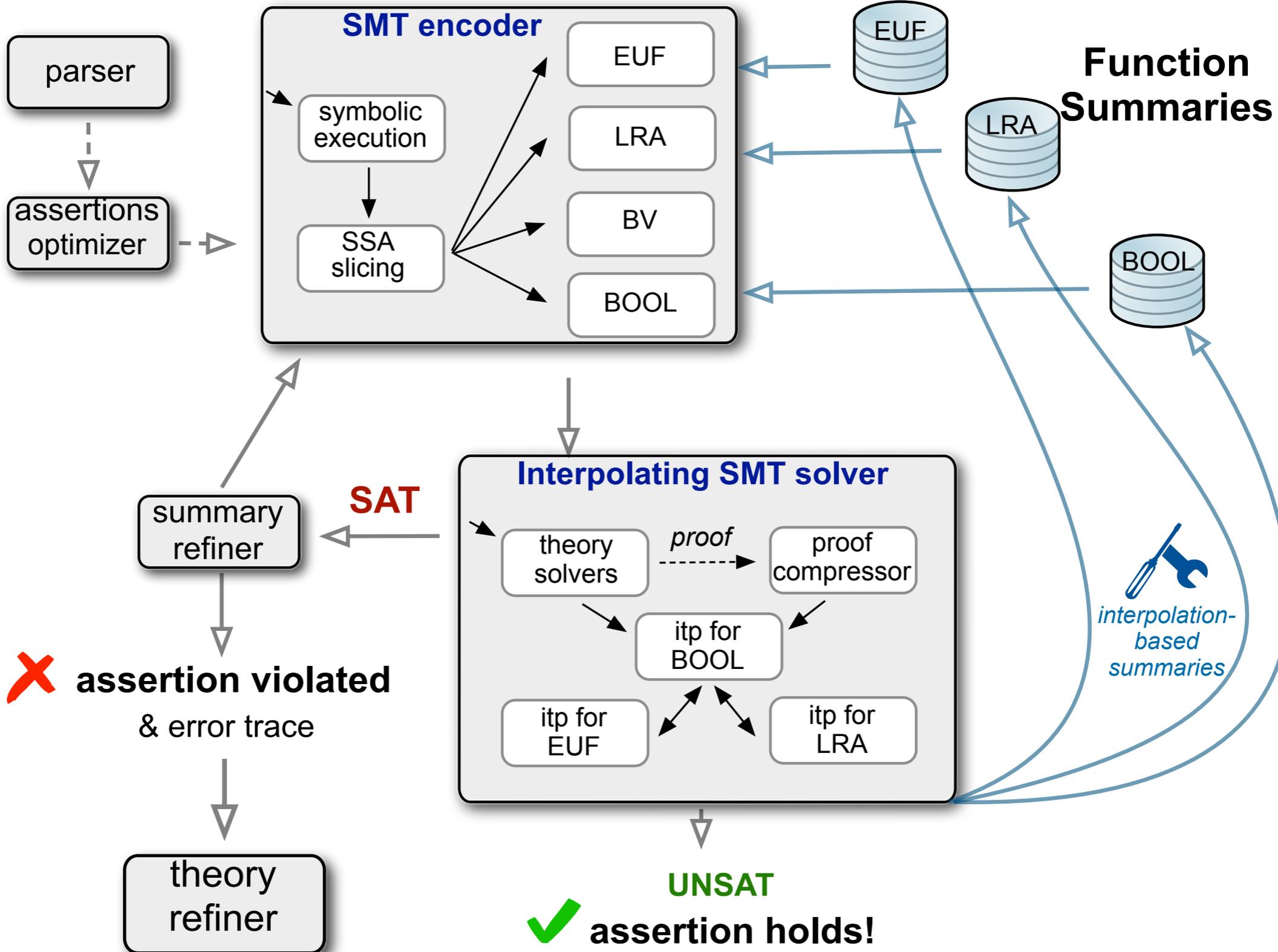
**✓ UNSAT assertion holds!**

**Function Summaries**

*interpolation-based summaries*

# HiFrog and Function Summarization

sources + assertions



**✗ assertion violated & error trace**

theory refiner

**UNSAT**  
**✓ assertion holds!**

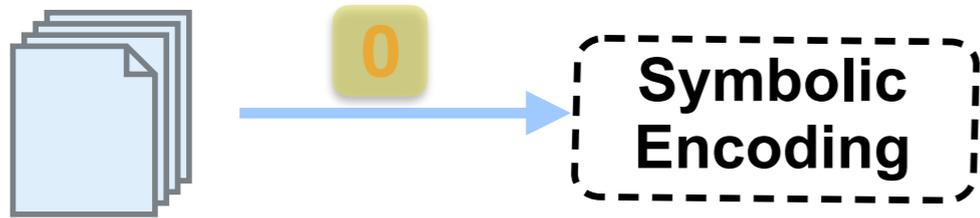
**Function Summaries**

*interpolation-based summaries*

# HiFrog and Theory Refinement

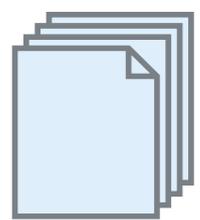
# HiFrog and Theory Refinement

Program +  
Assertions



# HiFrog and Theory Refinement

Program +  
Assertions



0

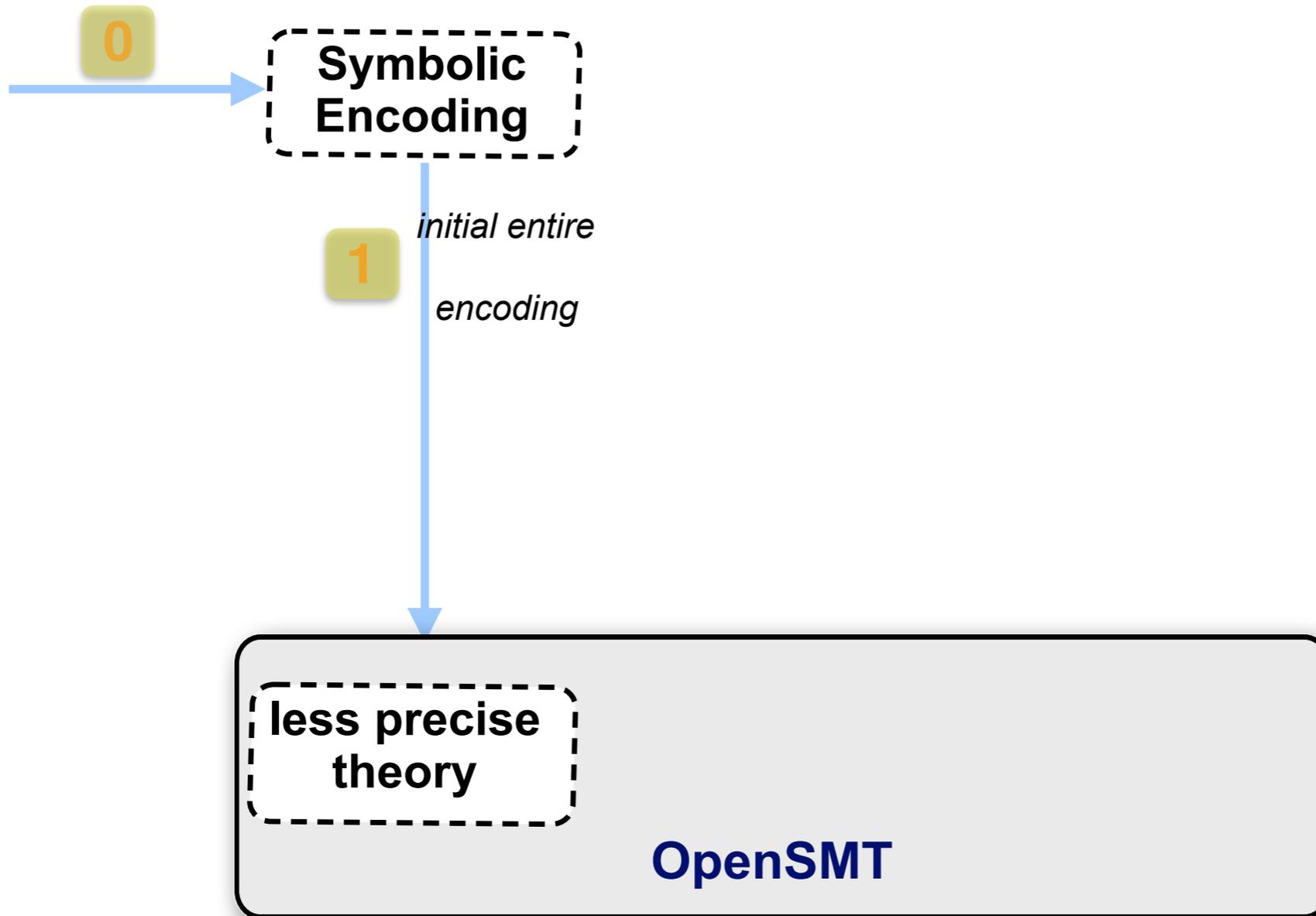
Symbolic  
Encoding

1

*initial entire  
encoding*

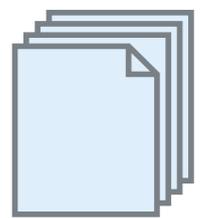
less precise  
theory

OpenSMT



# HiFrog and Theory Refinement

Program +  
Assertions



0

Symbolic  
Encoding

1

*initial entire  
encoding*

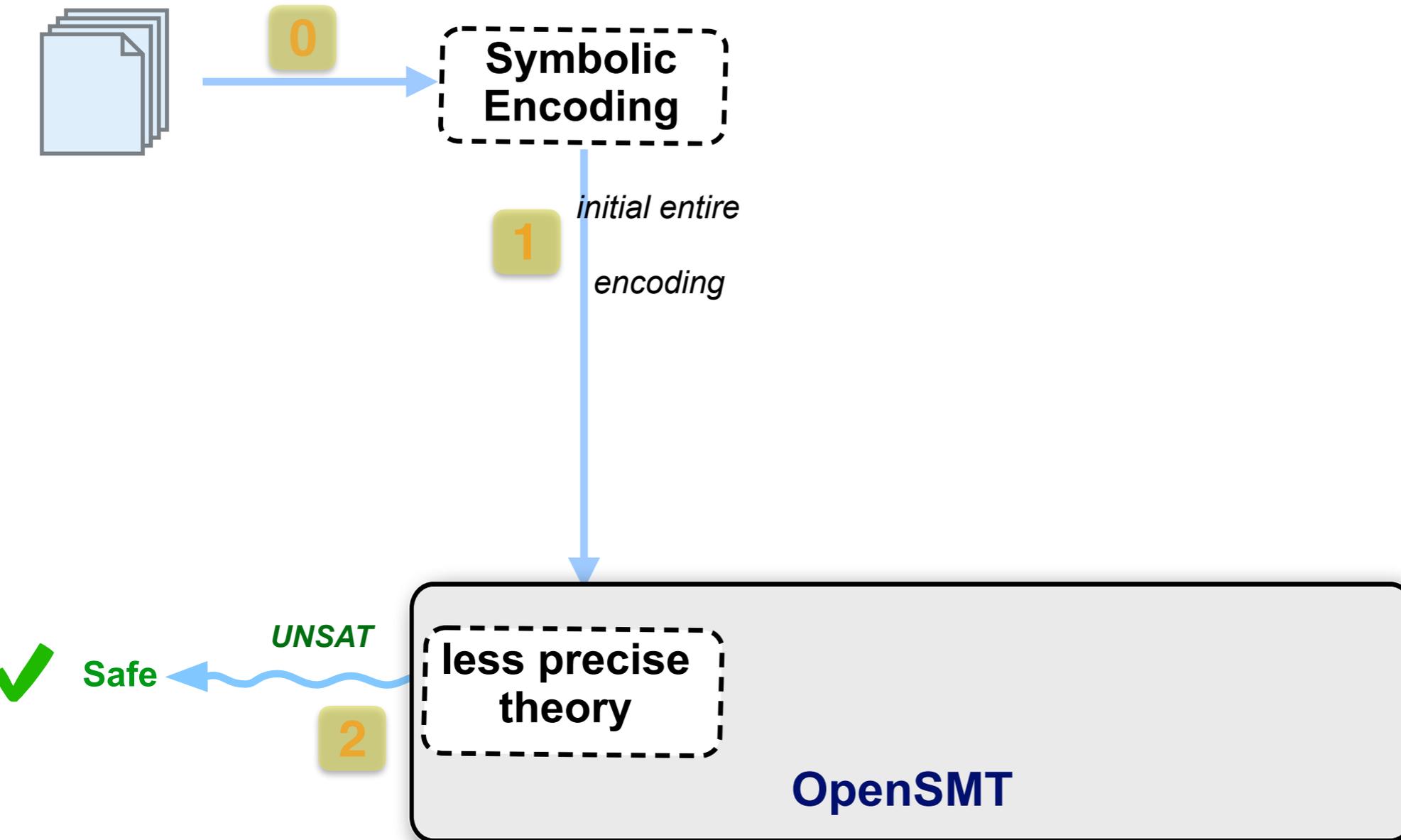
*UNSAT*

Safe

2

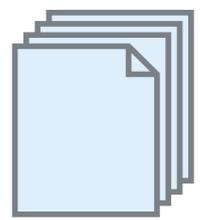
less precise  
theory

OpenSMT



# HiFrog and Theory Refinement

Program +  
Assertions



0

Symbolic  
Encoding

1

*initial entire  
encoding*

*SAT  
+ model*

2

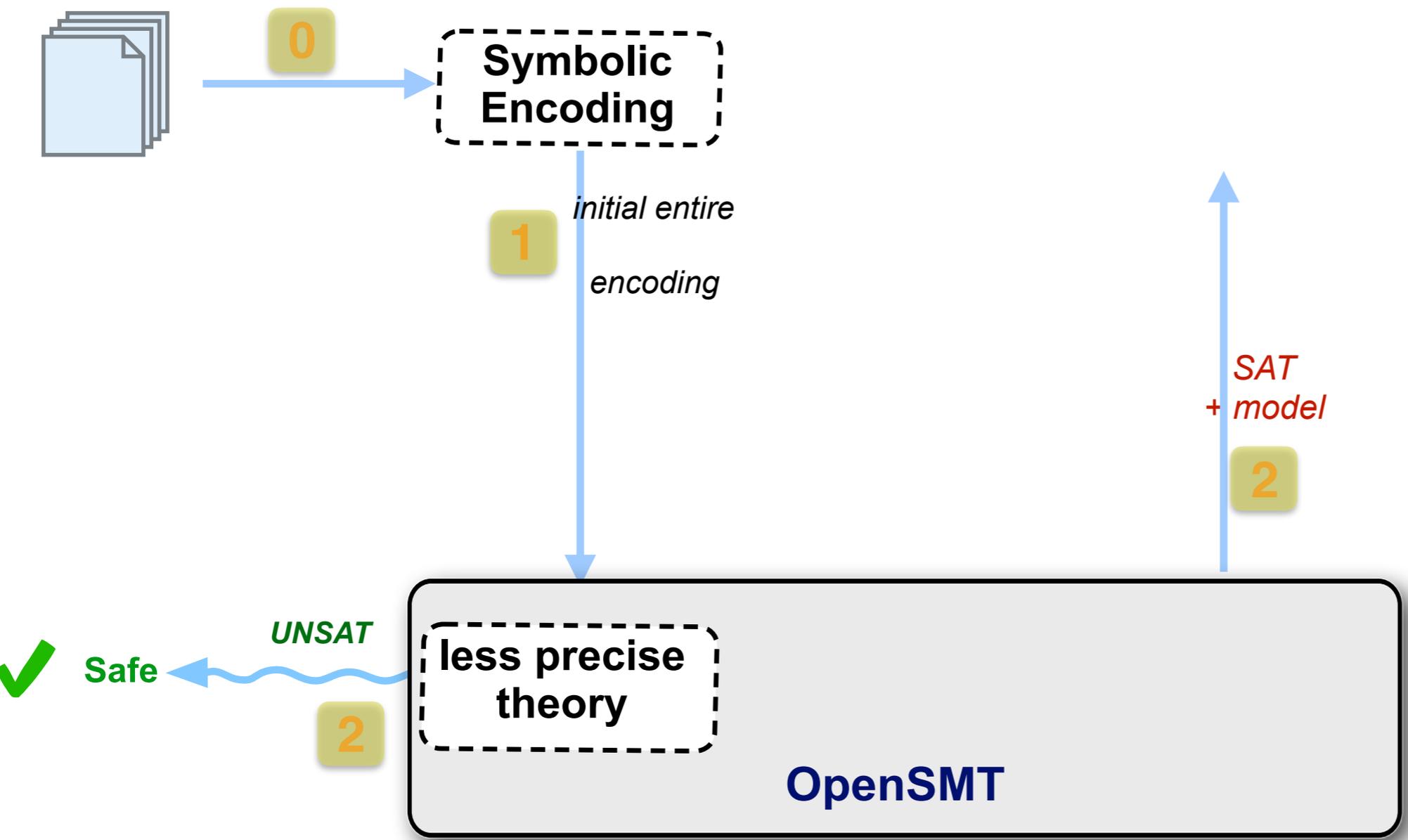
*UNSAT*

2

Safe

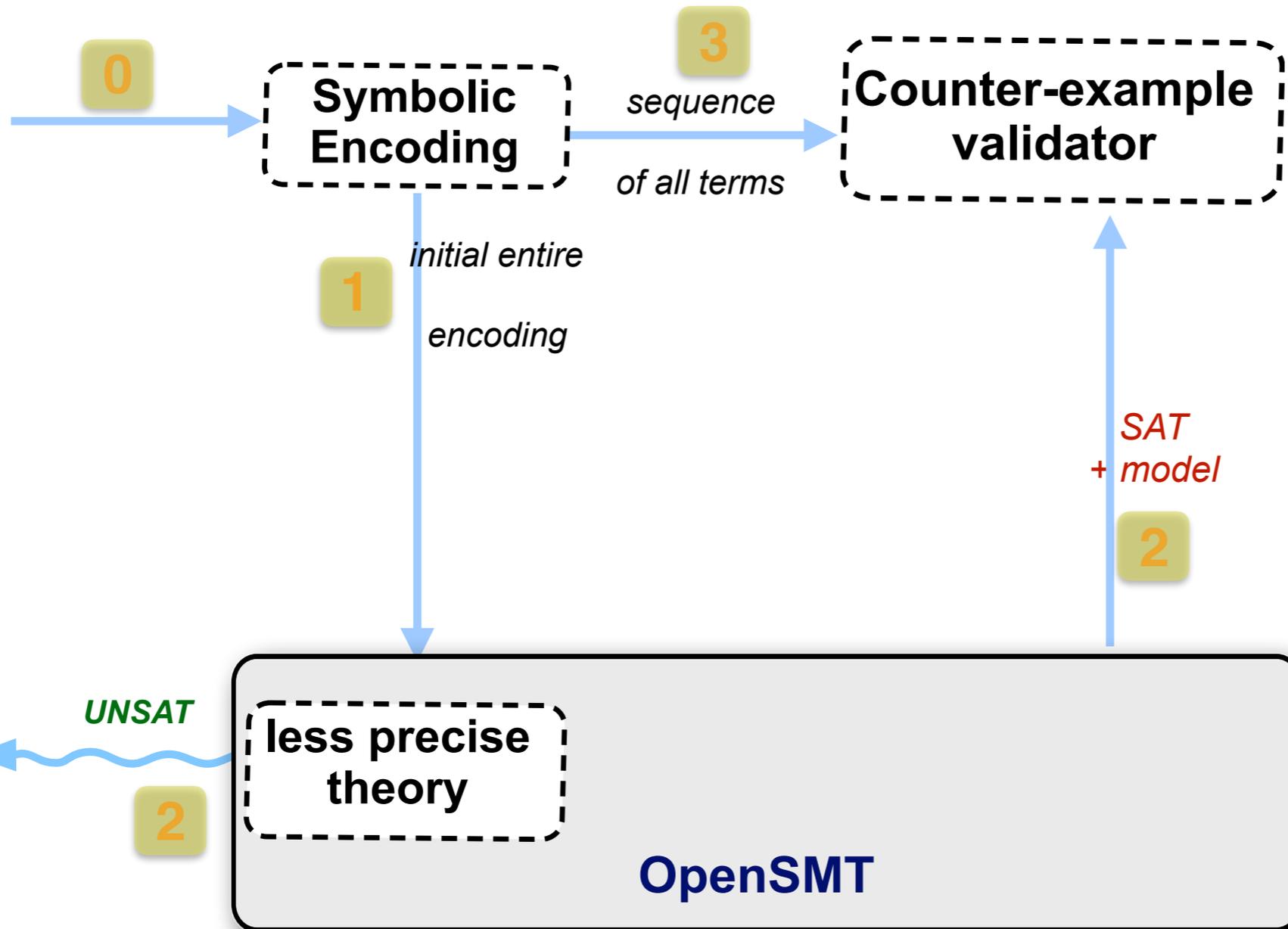
less precise  
theory

OpenSMT



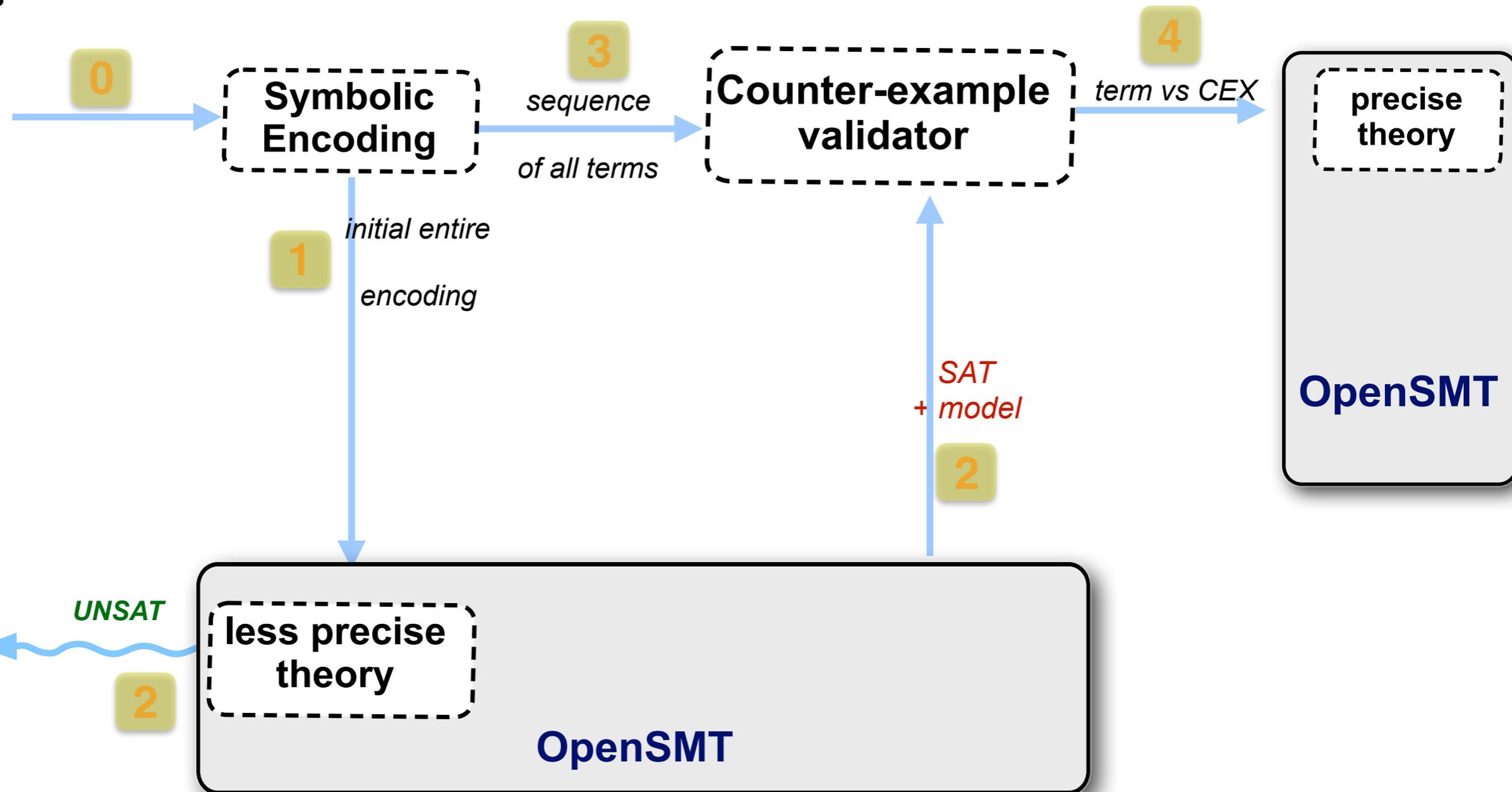
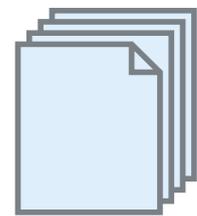
# HiFrog and Theory Refinement

Program +  
Assertions



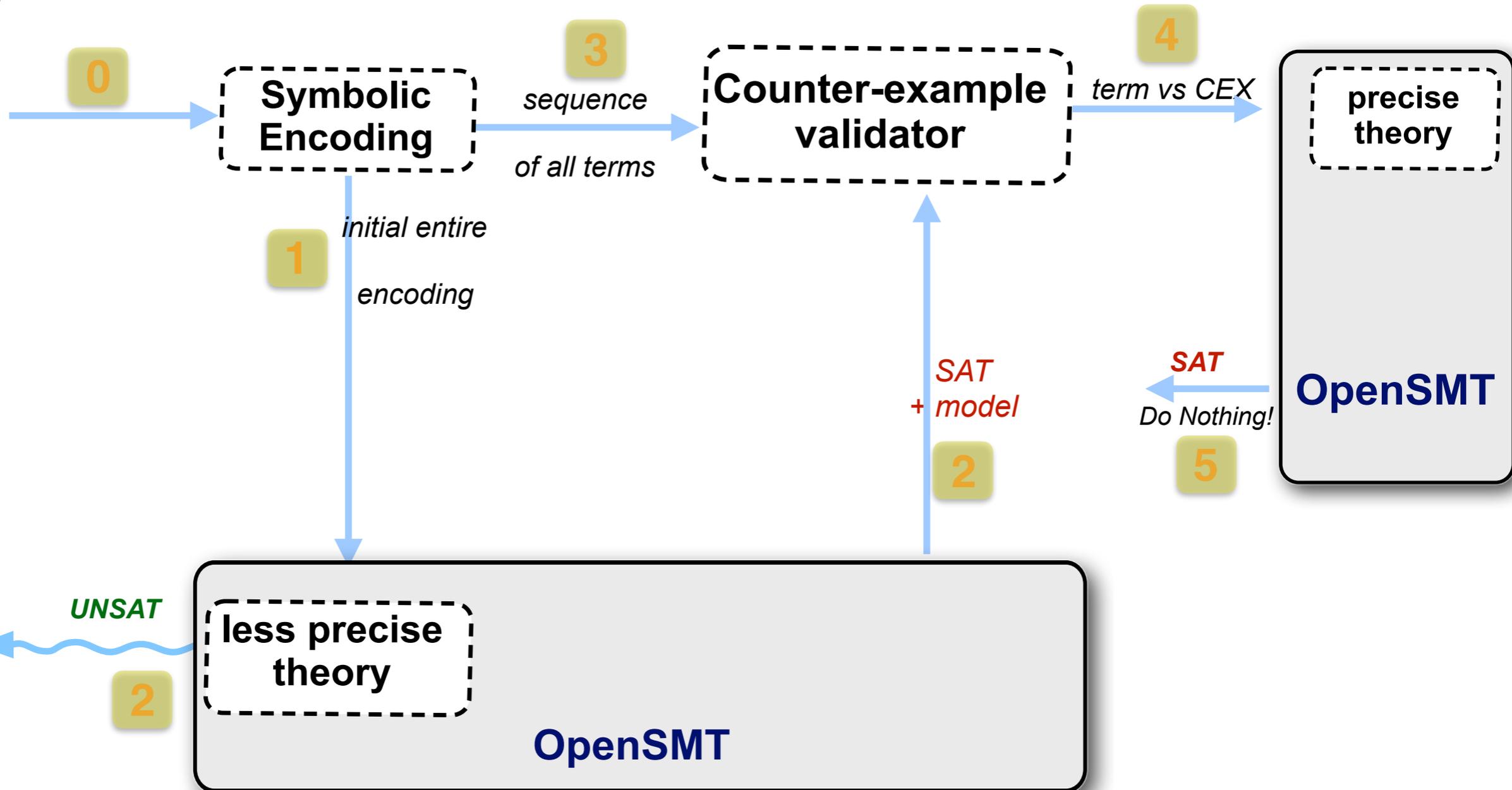
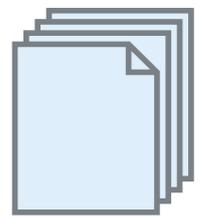
# HiFrog and Theory Refinement

Program +  
Assertions



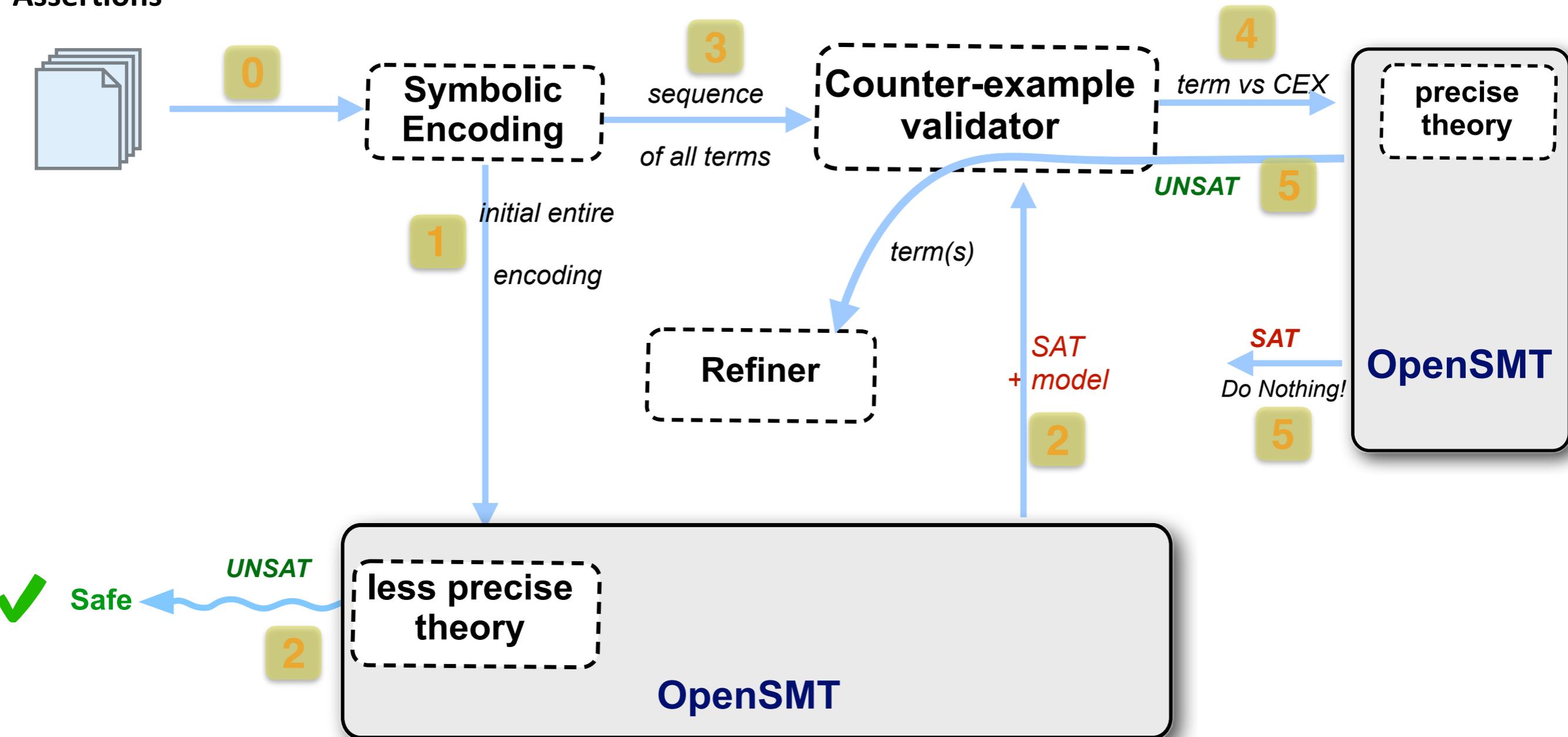
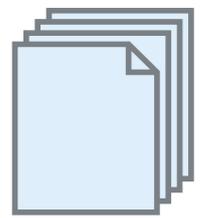
# HiFrog and Theory Refinement

Program +  
Assertions



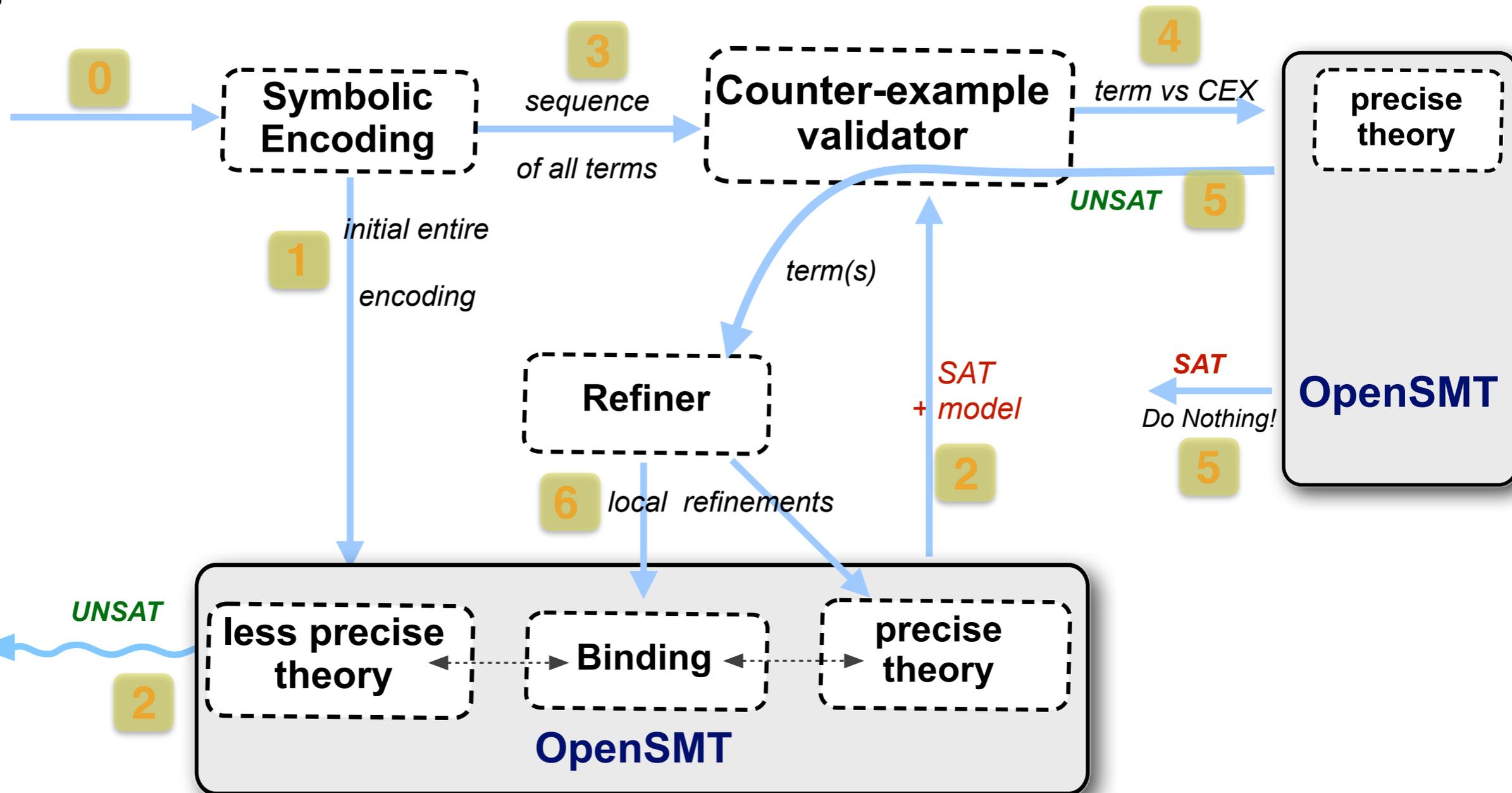
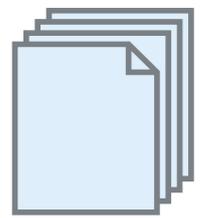
# HiFrog and Theory Refinement

Program + Assertions



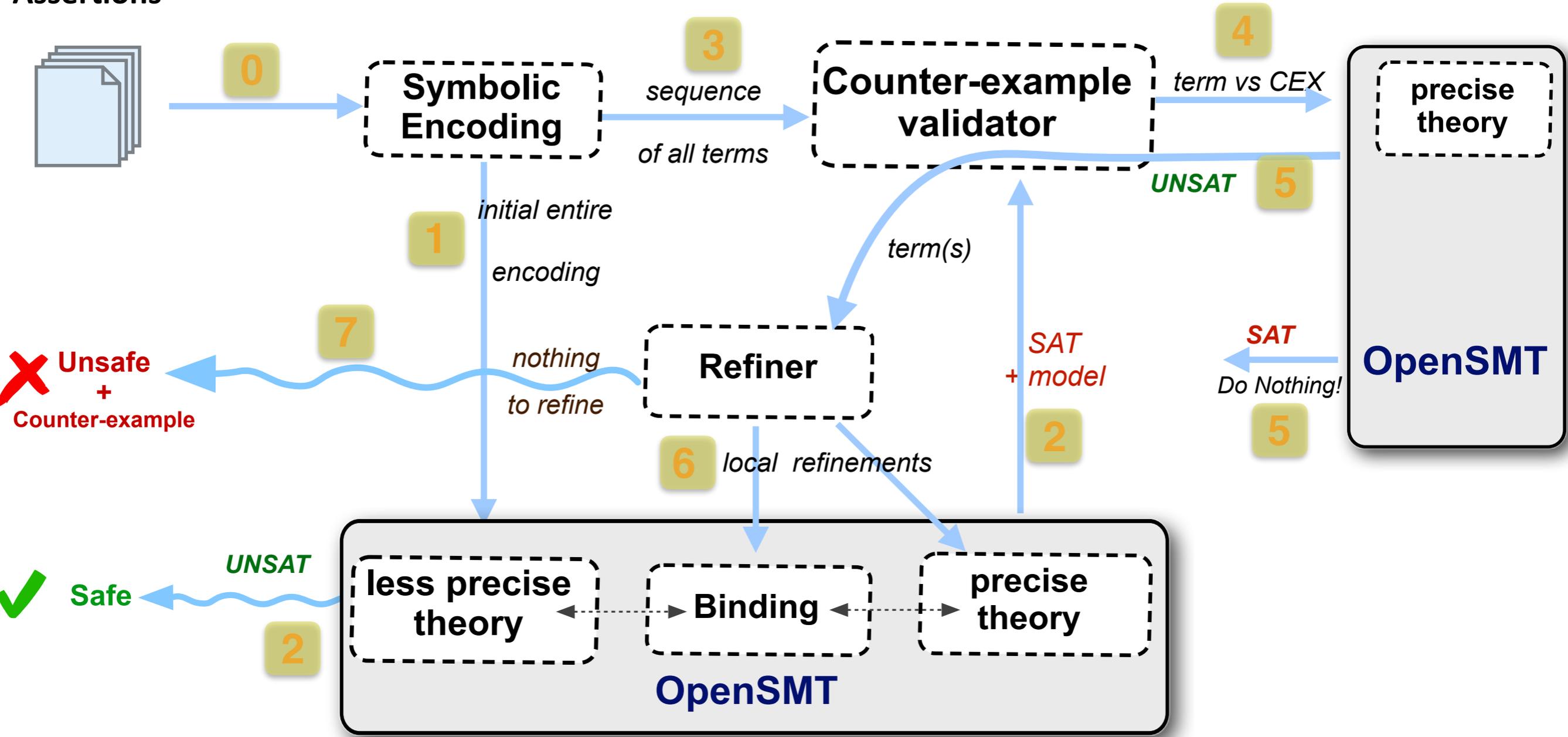
# HiFrog and Theory Refinement

Program + Assertions



# HiFrog and Theory Refinement

Program + Assertions





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

**Looking forward to seeing you at poster sessions!**