Solving Constrained Horn Clauses as C Programs with CHC2C

Levente Bajczi

Vince Molnár

MŰEGYETEM 1782

BME FACULTY OF ELECTRICAL ENGINEERING AND INFORMATICS

ftsrg Critical Systems Research Group

Agenda

- Background & theory
- Goals & contributions
- Experiment design & results
- Significance & summary

Agenda

- Background & theory
- Goals & contributions
- Experiment design & results
- Significance & summary

Agenda

- Background & theory
- Goals & contributions
- Experiment design & results
- Significance & summary

Agenda

- Background & theory
- Goals & contributions
- Experiment design & results
- Significance & summary

Background & Theory

What are **CHCs**?

How to **transform** them **to C**?

What are CHCs?

What are CHCs?

Query / assertion

$A(6) \Rightarrow \text{false}$

What are CHCs?

Atom

Query / assertion

$n = 0 \Rightarrow A(n)$

$A(6) \Rightarrow \text{false}$

What are CHCs?

Atom

Query / assertion

$$n = 0 \Rightarrow A(n)$$

$$A(n - 2) \Rightarrow A(n)$$

$$A(6) \Rightarrow \text{false}$$

Linear deduction

What are CHCs?

Atom

Query / assertion

$$n = 0 \Rightarrow A(n)$$

$$A(n - 2) \Rightarrow A(n)$$

$$A(6) \Rightarrow \text{false}$$

Linear deduction

SAT

UNSAT

What are CHCs?

Atom

Query / assertion

$$n = 0 \Rightarrow A(n)$$

$$A(n - 2) \Rightarrow A(n)$$

$$A(6) \Rightarrow \text{false}$$

Linear deduction

Query failed: A(6) is not deducible **SAT** **UNSAT** Query succeeded: A(6) is deducible

CHC to Control Flow Automata

$$n = 0 \Rightarrow A(n)$$

$$A(n - 2) \Rightarrow A(n)$$

$$A(6) \Rightarrow \text{false}$$

CHC to Control Flow Automata

L0

$$n = 0 \Rightarrow A(n)$$

$$A(n - 2) \Rightarrow A(n)$$

$$A(6) \Rightarrow \text{false}$$

LE

CHC to Control Flow Automata

L0

A

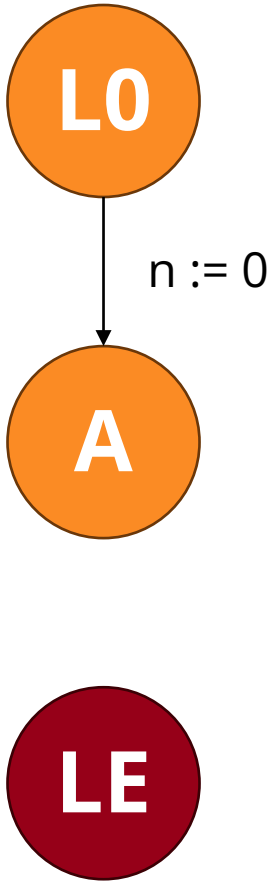
LE

$$n = 0 \Rightarrow A(n)$$

$$A(n - 2) \Rightarrow A(n)$$

$$A(6) \Rightarrow \text{false}$$

CHC to Control Flow Automata

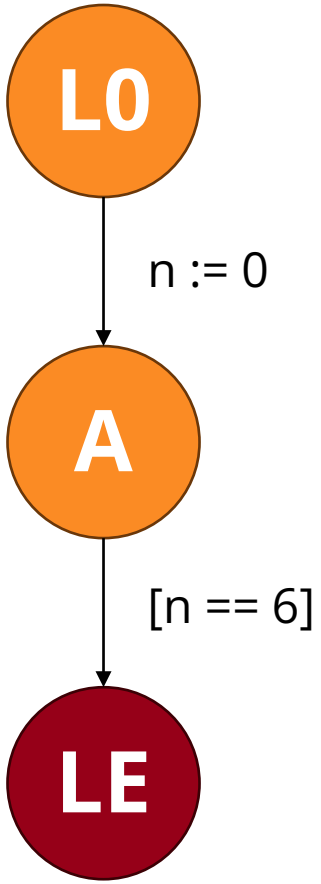


$$n = 0 \Rightarrow A(n)$$

$$A(n - 2) \Rightarrow A(n)$$

$$A(6) \Rightarrow \text{false}$$

CHC to Control Flow Automata

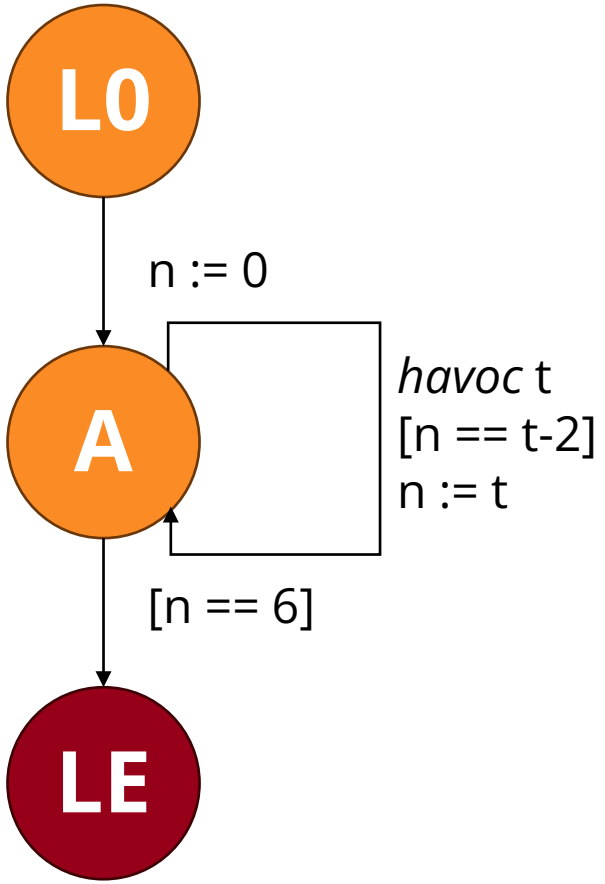


$$n = 0 \Rightarrow A(n)$$

$$A(n - 2) \Rightarrow A(n)$$

$$A(6) \Rightarrow \text{false}$$

CHC to Control Flow Automata

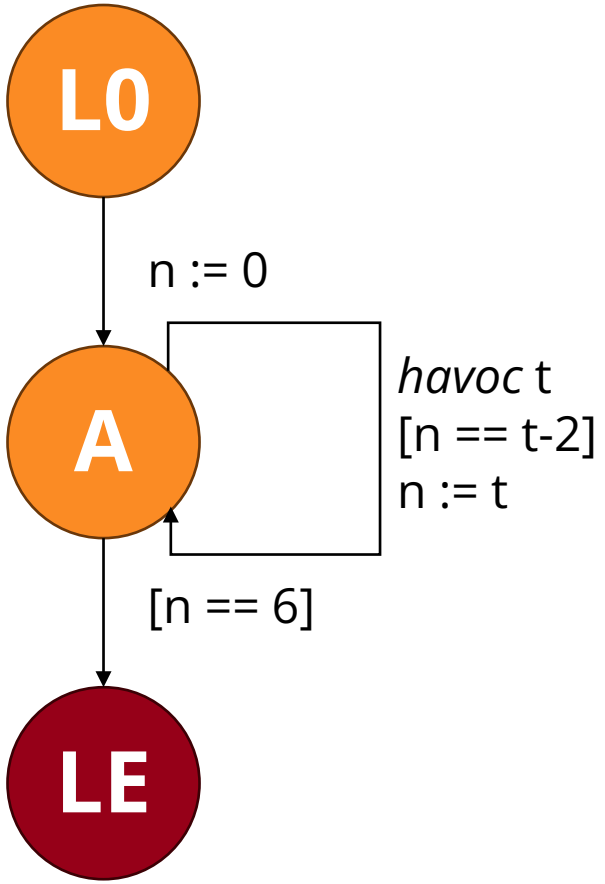


$$n = 0 \Rightarrow A(n)$$

$$A(n-2) \Rightarrow A(n)$$

$$A(6) \Rightarrow \text{false}$$

CHC to Control Flow Automata



$$n = 0 \Rightarrow A(n)$$

$$A(n-2) \Rightarrow A(n)$$

$$A(6) \Rightarrow \text{false}$$

```
int main() {
  int n, t = 0;
  n = t;
  while(true) {
    t = nondet();
    if(n == 6) return -1;
    else if(n == t-2) n = t;
  }
}
```

Forward

Bottom-up

CHC to Control Flow Automata

Bottoms Up for CHCs: Novel Transformation of Linear Constrained Horn Clauses to Software Verification

Márk Somorjai Mihály Dobos-Kovács Zsófia Ádám
Levente Bajczi András Vörös
vori@mit.bme.hu
Department of Measurement and Information Systems
Budapest University of Technology and Economics

Constrained Horn Clauses (CHCs) have conventionally been used as a low-level representation in formal verification. Most existing solvers use a diverse set of specialized techniques, including direct state space traversal or under-approximating abstraction, necessitating purpose-built complex algorithms. Other solvers successfully simplified the verification workflow by translating the problem to inputs for other verification tasks, leveraging the strengths of existing algorithms. One such approach transforms the CHC problem into a recursive program roughly emulating a *top-down* solver for the deduction task; and verifying the reachability of a safety violation specified as a control location. We propose an alternative *bottom-up* approach for linear CHCs, and evaluate the two options in the open-source model checking framework THETA on both synthetic and industrial examples. We find that there is a more than twofold increase in the number of solved tasks when the novel *bottom-up* approach is used in the verification workflow, in contrast with the *top-down* technique.

```
int main() {
  int n, t = 0;
  n = t;
  while(true) {
    t = nondet();
    if(n == 6) return -1;
    else if(n == t-2) n = t;
  }
}
```

Forward

Bottom-up

https://ftsrg.mit.bme.hu/paper-hcvs23-chc/paper.pdf

CHC to Programs

```
int main() {
  int n, t = 0;
  n = t;
  while(true) {
    t = nondet();
    if(n == 6) return -1;
    else if(n == t-2) n = t;
  }
}
```

CHC to Programs

- What if t > MAX_INT?
  - Or array out of bounds, …

```
int main() {
  int n, t = 0;
  n = t;
  while(true) {
    t = nondet();
    if(n == 6) return -1;
    else if(n == t-2) n = t;
  }
}
```

CHC to Programs

- What if t > MAX_INT?
  - Or array out of bounds, …

Tell the verification tool to use SMT semantics

- Not available with every tool
- Not *really* a C program any more

```
int main() {
  int n, t = 0;
  n = t;
  while(true) {
    t = nondet();
    if(n == 6) return -1;
    else if(n == t-2) n = t;
  }
}
```

CHC to Programs

- What if t > MAX_INT?
  - Or array out of bounds, …

Tell the verification tool to use SMT semantics

- Not available with every tool
- Not *really* a C program any more

Use *safeguarding* to prevent erroneous verdicts

- Limits verification power
  - Safe verdicts are dependent on all variables being bounded
  - Unsafe verdicts are still valid

```
int main() {
  int n, t = 0;
  n = t;
  while(true) {
    t = nondet();
    if(n == 6) return -1;
    else if(n == t-2) n = t;
  }
}
```

Can only return t ∈ [min; max]

Goals & Contributions

What did we want to achieve?

Goals of this Work

Broaden the field of **CHC solvers** with **SW verification tools**

Provide **SW verification** tools with valuable benchmarks to **test** and **debug**

Experiment design & results

What did **we** do?

How did the **tools** do?

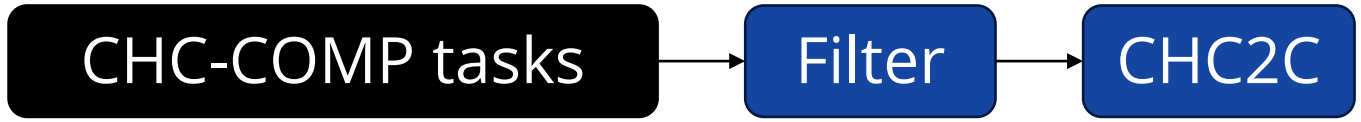
Experiment Overview

Experiment Overview

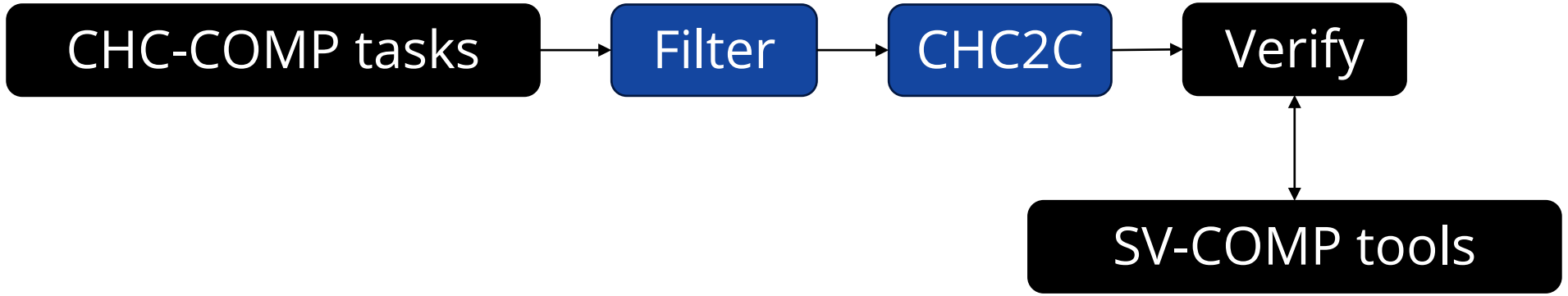
CHC-COMP tasks

Experiment Overview

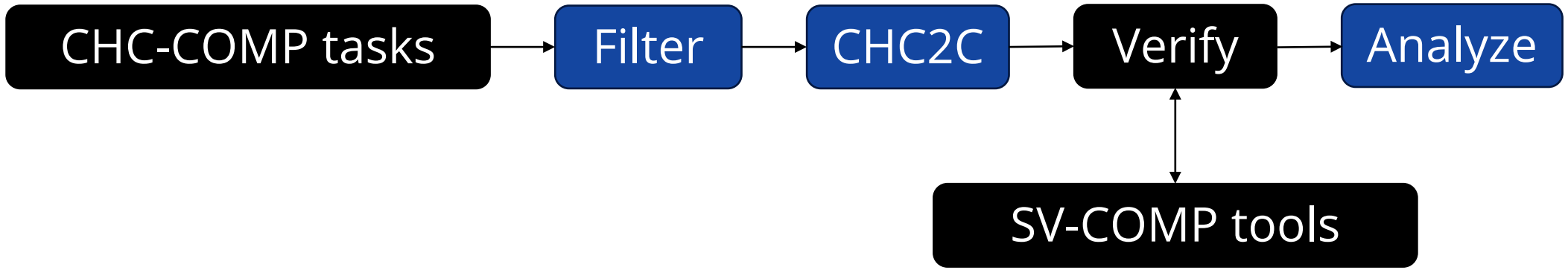
Experiment Overview



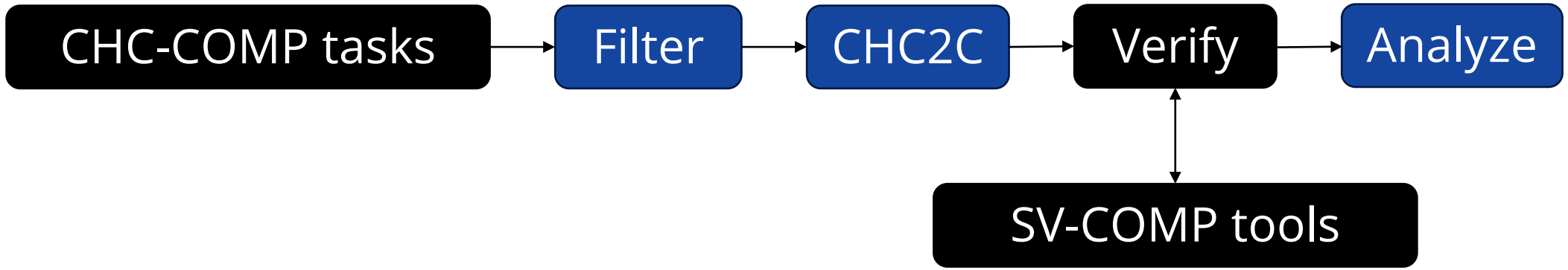
Experiment Overview



Experiment Overview

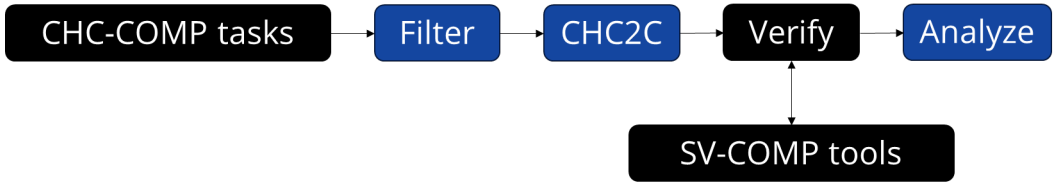


Experiment Overview

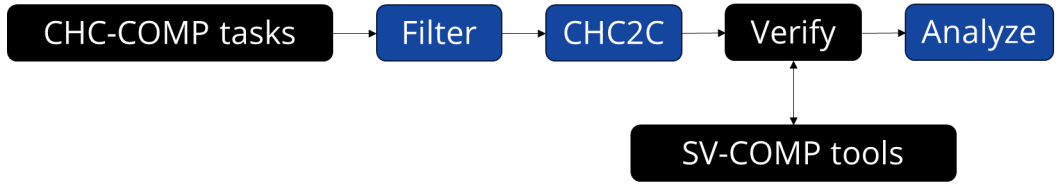


Only linear tasks, no arrays, no ADTs.

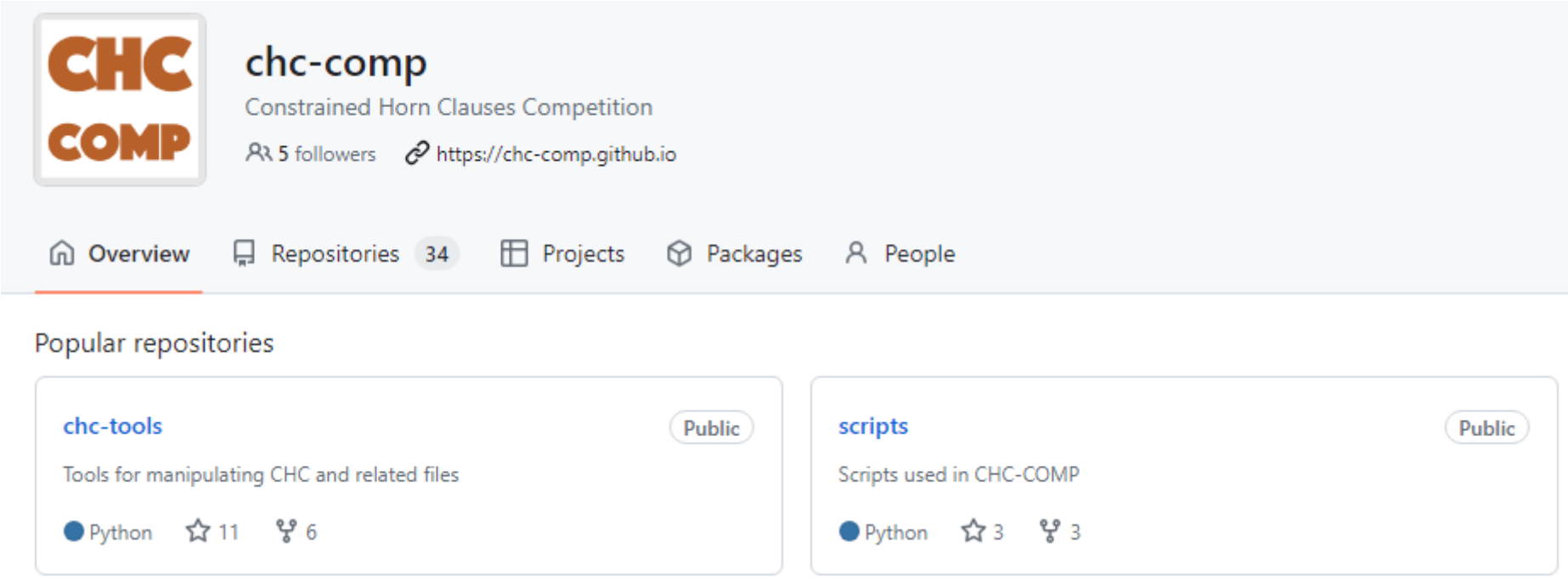
Benchmark Selection



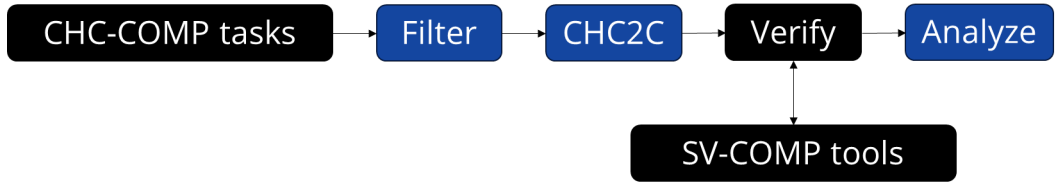
Benchmark Selection



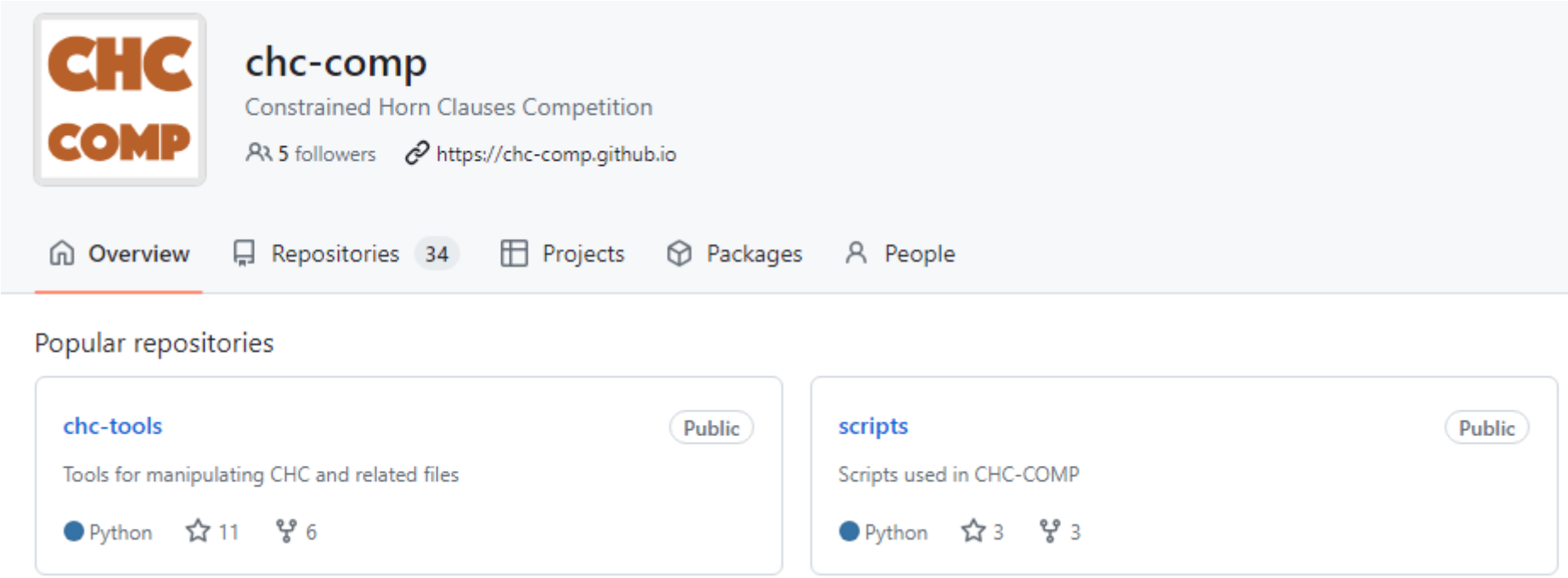
- From the CHC-COMP GitHub organization



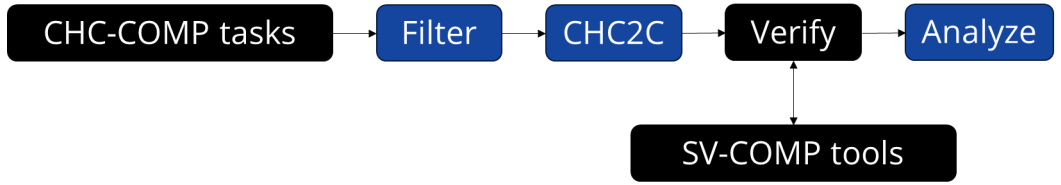
Benchmark Selection



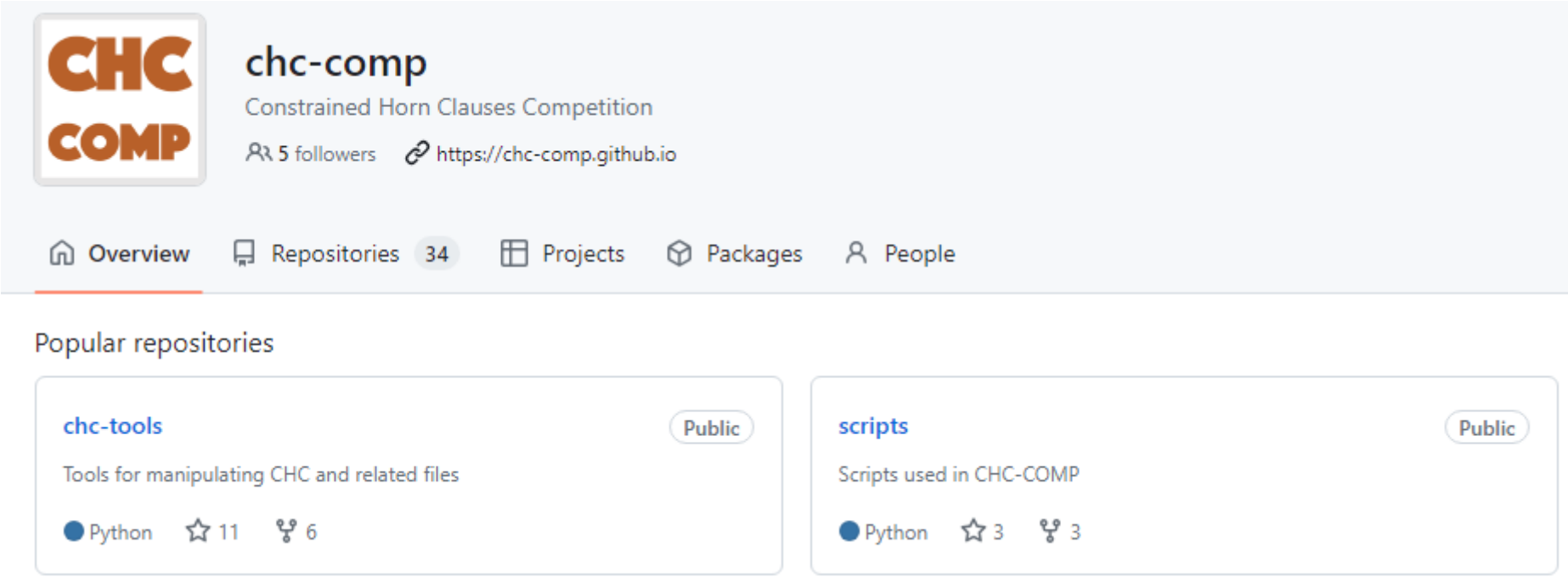
- From the CHC-COMP GitHub organization
- **23958** tasks (8644 with ADTs, 8892 with arrays)



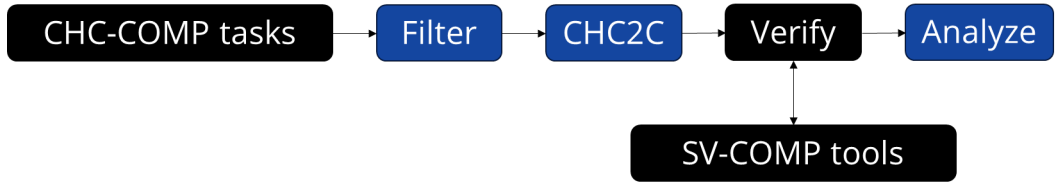
Benchmark Selection



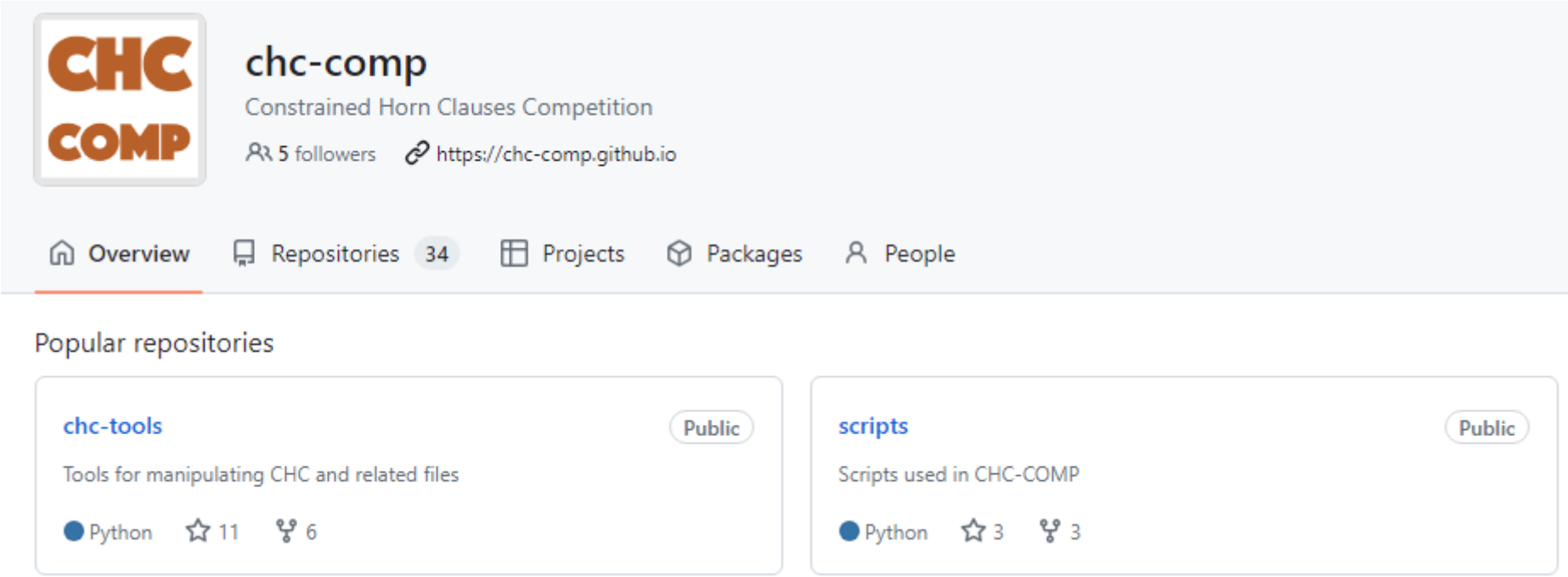
- From the CHC-COMP GitHub organization
- **23958** tasks (8644 with ADTs, 8892 with arrays)
- **3076** tasks are parsed by the CHC2C tool (see later)



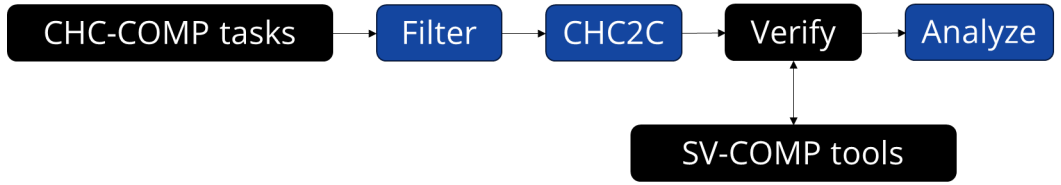
Benchmark Selection



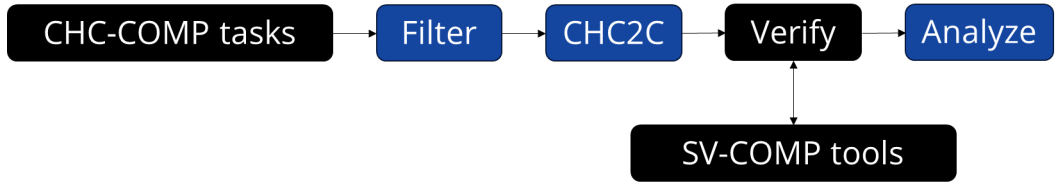
- From the CHC-COMP GitHub organization
- **23958** tasks (8644 with ADTs, 8892 with arrays)
- **3076** tasks are parsed by the CHC2C tool (see later)
- **1914** linear



CHC2C Prototype

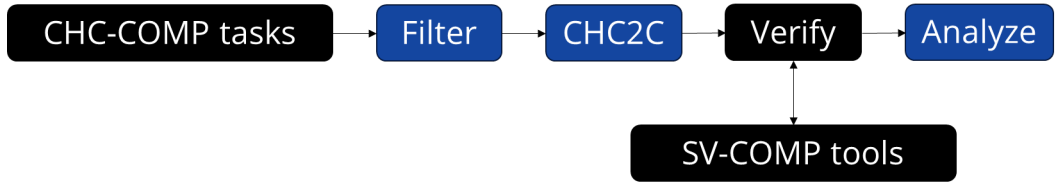


CHC2C Prototype



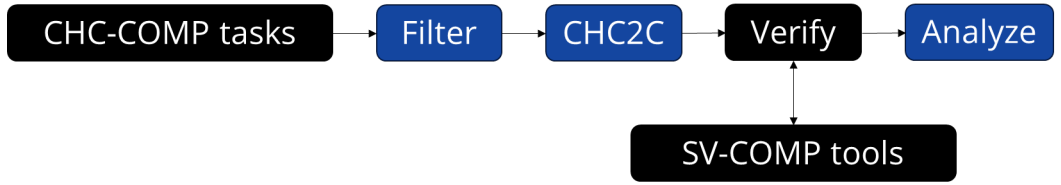
- In **Theta**
  - CHC → CFA forward transformation already supported
  - CFA → C serialization easy to achieve

CHC2C Prototype



- In **Theta**
  - CHC → CFA forward transformation already supported
  - CFA → C serialization easy to achieve
- Support for:
  - Linear CHCs
  - Single query
  - Int + Bool SMT theory

CHC2C Prototype



- In **Theta**
  - CHC → CFA forward transformation already supported
  - CFA → C serialization easy to achieve
- Support for:
  - Linear CHCs
  - Single query
  - Int + Bool SMT theory
- No support for:
  - Arrays
  - ADTs
  - Nonlinear CHCs (with the forward transformation)

Results – Verdicts

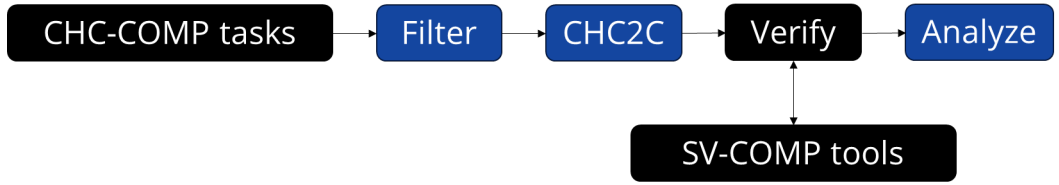


Table 2. Safeguarded transformation (all tasks)

	False						True			Unconf.	Points
	Common			Tool							
	All	+	-	All	+	-	All	+	-		
uautomizer	25	0	25	38	38	0	1054	686	368	4	1054
ukojak	24	0	24	38	38	0	1036	680	356	3	1036
utaipan	25	0	25	35	35	0	952	621	331	4	952
cpachecker	23	0	23	39	39	0	765	444	321	6	765
esbmc-kind	23	0	23	4	1	3	805	427	378	8	709
mopsa	20	0	20	1	0	1	210	210	0	0	178
2ls	0	0	0	0	0	0	101	84	17	0	101
infer	0	0	0	0	0	0	0	0	0	0	0
cpv	0	0	0	0	0	0	0	0	0	0	0
emergentheta	82	0	82	98	0	98	911	832	79	59	-2225
theta	81	0	81	191	0	191	1354	1157	197	55	-4758
bubaak	84	0	84	379	0	379	1183	1171	12	59	-10945
symbiotic	84	0	84	379	0	379	1183	1171	12	59	-10945
bubaak-split	84	0	84	379	0	379	1182	1170	12	59	-10946
veriabs	70	0	70	391	0	391	1117	1117	0	59	-11395
veriabsl	70	0	70	391	0	391	1113	1113	0	59	-11399
goblint	71	0	71	391	0	391	1101	1101	0	59	-11411

Table 3. Non-safeguarded transformation (all tasks)

	False						True			Unconf.	Points
	Common			Tool							
	All	+	-	All	+	-	All	+	-		
uautomizer	24	0	24	39	38	1	1142	769	373	5	1110
ukojak	23	0	23	39	38	1	1097	739	358	3	1065
utaipan	24	0	24	36	36	0	1028	690	338	5	1028
cpachecker	22	0	22	78	78	0	792	451	341	5	792
esbmc-kind	22	0	22	60	57	3	827	444	383	8	731
mopsa	22	0	22	1	0	1	212	212	0	0	180
2ls	0	0	0	3	3	0	98	81	17	0	98
infer	0	0	0	0	0	0	0	0	0	0	0
cpv	0	0	0	0	0	0	0	0	0	0	0
theta	67	0	67	208	0	208	1355	1158	197	66	-5301
emergentheta	68	0	68	210	0	210	1344	1147	197	59	-5376
symbiotic	65	0	65	352	1	351	1190	1139	51	173	-10042
bubaak	67	0	67	355	1	354	1229	1176	53	236	-10099
bubaak-split	68	0	68	375	0	375	1201	1170	31	59	-10799
goblint	66	0	66	396	0	396	1120	1120	0	59	-11552
veriabs	65	0	65	407	0	407	1169	1169	0	59	-11855
veriabsl	65	0	65	407	0	407	1169	1169	0	59	-11855

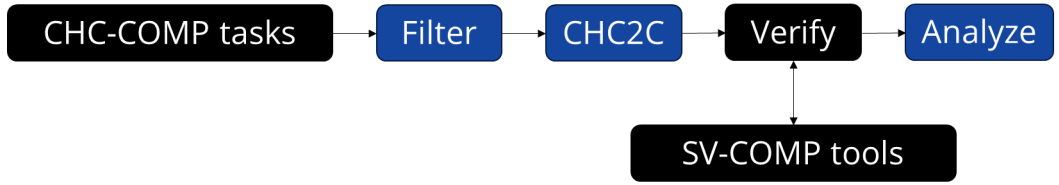
Table 4. Safeguarded transformation (CHC-COMP'23)

	False						True			Unconf.	Points
	Common			Tool							
	All	+	-	All	+	-	All	+	-		
utaipan	8	0	8	4	4	0	103	82	21	9	103
uautomizer	8	0	8	6	6	0	94	73	21	7	94
cpachecker	8	0	8	6	6	0	91	71	20	11	91
ukojak	7	0	7	6	6	0	87	68	19	9	87
mopsa	10	0	10	0	0	0	56	56	0	9	56
esbmc-kind	9	0	9	1	0	1	86	67	19	14	54
2ls	0	0	0	0	0	0	17	15	2	0	17
infer	0	0	0	0	0	0	0	0	0	0	0
cpv	0	0	0	0	0	0	0	0	0	0	0
emergentheta	32	0	32	13	0	13	168	163	5	48	-248
theta	37	0	37	14	0	14	198	190	8	48	-250
bubaak	39	0	39	23	0	23	234	234	0	52	-502
symbiotic	37	0	37	23	0	23	208	208	0	51	-528
bubaak-split	34	0	34	23	0	23	198	198	0	50	-538
veriabsl	30	0	30	23	0	23	190	190	0	50	-546
veriabs	31	0	31	23	0	23	189	189	0	50	-547
goblint	28	0	28	23	0	23	182	182	0	50	-554

Table 5. Non-safeguarded transformation (CHC-COMP'23)

	False						True			Unconf.	Points
	Common			Tool							
	All	+	-	All	+	-	All	+	-		
utaipan	8	0	8	4	4	0	133	108	25	10	133
cpachecker	12	0	12	15	15	0	117	90	27	10	117
uautomizer	8	0	8	7	6	1	116	93	23	10	84
ukojak	7	0	7	7	6	1	114	91	23	9	82
mopsa	12	0	12	0	0	0	76	76	0	9	76
esbmc-kind	9	0	9	15	14	1	93	72	21	14	61
2ls	0	0	0	0	0	0	17	15	2	0	17
infer	0	0	0	0	0	0	0	0	0	0	0
cpv	0	0	0	0	0	0	0	0	0	0	0
bubaak	34	0	34	20	0	20	258	247	11	70	-382
symbiotic	29	0	29	20	0	20	219	209	10	63	-421
emergentheta	31	0	31	23	0	23	226	218	8	51	-510
theta	29	0	29	23	0	23	212	204	8	50	-524
goblint	28	0	28	25	0	25	190	190	0	50	-610
bubaak-split	28	0	28	28	0	28	207	204	3	50	-689
veriabs	29	0	29	31	0	31	203	203	0	51	-789
veriabsl	29	0	29	31	0	31	202	202	0	51	-790

Results – Verdicts



- True +/-: **+1** points
- False +/-: **-16/-32** points
  - *Common* false results
  - *Tool-specific* false results
- *Unconfirmed*: **no** points

Table 2. Safeguarded transformation (all tasks)

	False						True			Unconf.	Points
	Common			Tool							
	All	+	-	All	+	-	All	+	-		
uautomizer	25	0	25	38	38	0	1054	686	368	4	1054
ukojak	24	0	24	38	38	0	1036	680	356	3	1036
utaipan	25	0	25	35	35	0	952	621	331	4	952
cpachecker	23	0	23	39	39	0	765	444	321	6	765
esbmc-kind	23	0	23	4	1	3	805	427	378	8	709
mopsa	20	0	20	1	0	1	210	210	0	0	178
2ls	0	0	0	0	0	0	101	84	17	0	101
infer	0	0	0	0	0	0	0	0	0	0	0
cpv	0	0	0	0	0	0	0	0	0	0	0
emergentheta	82	0	82	98	0	98	911	832	79	59	-2225
theta	81	0	81	191	0	191	1354	1157	197	55	-4758
bubaak	84	0	84	379	0	379	1183	1171	12	59	-10945
symbiotic	84	0	84	379	0	379	1183	1171	12	59	-10945
bubaak-split	84	0	84	379	0	379	1182	1170	12	59	-10946
veriabs	70	0	70	391	0	391	1117	1117	0	59	-11395
veriabsl	70	0	70	391	0	391	1113	1113	0	59	-11399
goblint	71	0	71	391	0	391	1101	1101	0	59	-11411

Table 3. Non-safeguarded transformation (all tasks)

	False						True			Unconf.	Points
	Common			Tool							
	All	+	-	All	+	-	All	+	-		
uautomizer	24	0	24	39	38	1	1142	769	373	5	1110
ukojak	23	0	23	39	38	1	1097	739	358	3	1065
utaipan	24	0	24	36	36	0	1028	690	338	5	1028
cpachecker	22	0	22	78	78	0	792	451	341	5	792
esbmc-kind	22	0	22	60	57	3	827	444	383	8	731
mopsa	22	0	22	1	0	1	212	212	0	0	180
2ls	0	0	0	3	3	0	98	81	17	0	98
infer	0	0	0	0	0	0	0	0	0	0	0
cpv	0	0	0	0	0	0	0	0	0	0	0
theta	67	0	67	208	0	208	1355	1158	197	66	-5301
emergentheta	68	0	68	210	0	210	1344	1147	197	59	-5376
symbiotic	65	0	65	352	1	351	1190	1139	51	173	-10042
bubaak	67	0	67	355	1	354	1229	1176	53	236	-10099
bubaak-split	68	0	68	375	0	375	1201	1170	31	59	-10799
goblint	66	0	66	396	0	396	1120	1120	0	59	-11552
veriabs	65	0	65	407	0	407	1169	1169	0	59	-11855
veriabsl	65	0	65	407	0	407	1169	1169	0	59	-11855

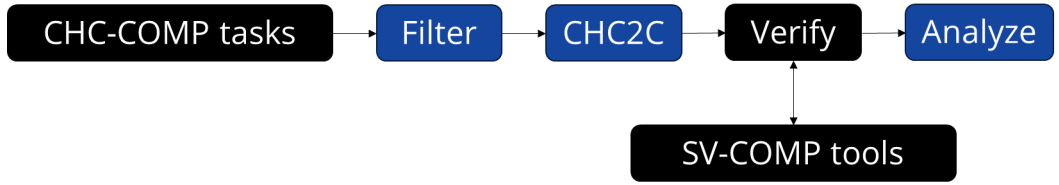
Table 4. Safeguarded transformation (CHC-COMP'23)

	False						True			Unconf.	Points
	Common			Tool							
	All	+	-	All	+	-	All	+	-		
utaipan	8	0	8	4	4	0	103	82	21	9	103
uautomizer	8	0	8	6	6	0	94	73	21	7	94
cpachecker	8	0	8	6	6	0	91	71	20	11	91
ukojak	7	0	7	6	6	0	87	68	19	9	87
mopsa	10	0	10	0	0	0	56	56	0	9	56
esbmc-kind	9	0	9	1	0	1	86	67	19	14	54
2ls	0	0	0	0	0	0	17	15	2	0	17
infer	0	0	0	0	0	0	0	0	0	0	0
cpv	0	0	0	0	0	0	0	0	0	0	0
emergentheta	32	0	32	13	0	13	168	163	5	48	-248
theta	37	0	37	14	0	14	198	190	8	48	-250
bubaak	39	0	39	23	0	23	234	234	0	52	-502
symbiotic	37	0	37	23	0	23	208	208	0	51	-528
bubaak-split	34	0	34	23	0	23	198	198	0	50	-538
veriabsl	30	0	30	23	0	23	190	190	0	50	-546
veriabs	31	0	31	23	0	23	189	189	0	50	-547
goblint	28	0	28	23	0	23	182	182	0	50	-554

Table 5. Non-safeguarded transformation (CHC-COMP'23)

	False						True			Unconf.	Points
	Common			Tool							
	All	+	-	All	+	-	All	+	-		
utaipan	8	0	8	4	4	0	133	108	25	10	133
cpachecker	12	0	12	15	15	0	117	90	27	10	117
uautomizer	8	0	8	7	6	1	116	93	23	10	84
ukojak	7	0	7	7	6	1	114	91	23	9	82
mopsa	12	0	12	0	0	0	76	76	0	9	76
esbmc-kind	9	0	9	15	14	1	93	72	21	14	61
2ls	0	0	0	0	0	0	17	15	2	0	17
infer	0	0	0	0	0	0	0	0	0	0	0
cpv	0	0	0	0	0	0	0	0	0	0	0
bubaak	34	0	34	20	0	20	258	247	11	70	-382
symbiotic	29	0	29	20	0	20	219	209	10	63	-421
emergentheta	31	0	31	23	0	23	226	218	8	51	-510
theta	29	0	29	23	0	23	212	204	8	50	-524
goblint	28	0	28	25	0	25	190	190	0	50	-610
bubaak-split	28	0	28	28	0	28	207	204	3	50	-689
veriabs	29	0	29	31	0	31	203	203	0	51	-789
veriabsl	29	0	29	31	0	31	202	202	0	51	-790

Results – Verdicts



- True +/-: **+1** points
- False +/-: **-16/-32** points
  - *Common* false results
  - *Tool-specific* false results
- *Unconfirmed*: **no** points

No common false positives
(low number of common false negatives)

Table 2. Safeguarded transformation (all tasks)

	False						True			Unconf.	Points
	Common			Tool							
	All	+	-	All	+	-	All	+	-		
uautomizer	25	0	25	38	38	0	1054	686	368	4	1054
ukojak	24	0	24	38	38	0	1036	680	356	3	1036
utaipan	25	0	25	35	35	0	952	621	331	4	952
cpachecker	23	0	23	39	39	0	765	444	321	6	765
esbmc-kind	23	0	23	4	1	3	805	427	378	8	709
mopsa	20	0	20	1	0	1	210	210	0	0	178
2ls	0	0	0	0	0	0	101	84	17	0	101
infer	0	0	0	0	0	0	0	0	0	0	0
cpv	0	0	0	0	0	0	0	0	0	0	0
emergentheta	82	0	82	98	0	98	911	832	79	59	-2225
theta	81	0	81	191	0	191	1354	1157	197	55	-4758
bubaak	84	0	84	379	0	379	1183	1171	12	59	-10945
symbiotic	84	0	84	379	0	379	1183	1171	12	59	-10945
bubaak-split	84	0	84	379	0	379	1182	1170	12	59	-10946
veriabs	70	0	70	391	0	391	1117	1117	0	59	-11395
veriabsl	70	0	70	391	0	391	1113	1113	0	59	-11399
goblint	71	0	71	391	0	391	1101	1101	0	59	-11411

Table 3. Non-safeguarded transformation (all tasks)

	False						True			Unconf.	Points
	Common			Tool							
	All	+	-	All	+	-	All	+	-		
uautomizer	24	0	24	39	38	1	1142	769	373	5	1110
ukojak	23	0	23	39	38	1	1097	739	358	3	1065
utaipan	24	0	24	36	36	0	1028	690	338	5	1028
cpachecker	22	0	22	78	78	0	792	451	341	5	792
esbmc-kind	22	0	22	60	57	3	827	444	383	8	731
mopsa	22	0	22	1	0	1	212	212	0	0	180
2ls	0	0	0	3	3	0	98	81	17	0	98
infer	0	0	0	0	0	0	0	0	0	0	0
cpv	0	0	0	0	0	0	0	0	0	0	0
theta	67	0	67	208	0	208	1355	1158	197	66	-5301
emergentheta	68	0	68	210	0	210	1344	1147	197	59	-5376
symbiotic	65	0	65	352	1	351	1190	1139	51	173	-10042
bubaak	67	0	67	355	1	354	1229	1176	53	236	-10099
bubaak-split	68	0	68	375	0	375	1201	1170	31	59	-10799
goblint	66	0	66	396	0	396	1120	1120	0	59	-11552
veriabs	65	0	65	407	0	407	1169	1169	0	59	-11855
veriabsl	65	0	65	407	0	407	1169	1169	0	59	-11855

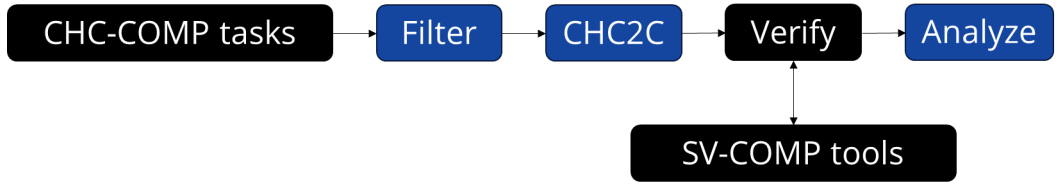
Table 4. Safeguarded transformation (CHC-COMP'23)

	False						True			Unconf.	Points
	Common			Tool							
	All	+	-	All	+	-	All	+	-		
utaipan	8	0	8	4	4	0	103	82	21	9	103
uautomizer	8	0	8	6	6	0	94	73	21	7	94
cpachecker	8	0	8	6	6	0	91	71	20	11	91
ukojak	7	0	7	6	6	0	87	68	19	9	87
mopsa	10	0	10	0	0	0	56	56	0	9	56
esbmc-kind	9	0	9	1	0	1	86	67	19	14	54
2ls	0	0	0	0	0	0	17	15	2	0	17
infer	0	0	0	0	0	0	0	0	0	0	0
cpv	0	0	0	0	0	0	0	0	0	0	0
emergentheta	32	0	32	13	0	13	168	163	5	48	-248
theta	37	0	37	14	0	14	198	190	8	48	-250
bubaak	39	0	39	23	0	23	234	234	0	52	-502
symbiotic	37	0	37	23	0	23	208	208	0	51	-528
bubaak-split	34	0	34	23	0	23	198	198	0	50	-538
veriabsl	30	0	30	23	0	23	190	190	0	50	-546
veriabs	31	0	31	23	0	23	189	189	0	50	-547
goblint	28	0	28	23	0	23	182	182	0	50	-554

Table 5. Non-safeguarded transformation (CHC-COMP'23)

	False						True			Unconf.	Points
	Common			Tool							
	All	+	-	All	+	-	All	+	-		
utaipan	8	0	8	4	4	0	133	108	25	10	133
cpachecker	12	0	12	15	15	0	117	90	27	10	117
uautomizer	8	0	8	7	6	1	116	93	23	10	84
ukojak	7	0	7	7	6	1	114	91	23	9	82
mopsa	12	0	12	0	0	0	76	76	0	9	76
esbmc-kind	9	0	9	15	14	1	93	72	21	14	61
2ls	0	0	0	0	0	0	17	15	2	0	17
infer	0	0	0	0	0	0	0	0	0	0	0
cpv	0	0	0	0	0	0	0	0	0	0	0
bubaak	34	0	34	20	0	20	258	247	11	70	-382
symbiotic	29	0	29	20	0	20	219	209	10	63	-421
emergentheta	31	0	31	23	0	23	226	218	8	51	-510
theta	29	0	29	23	0	23	212	204	8	50	-524
goblint	28	0	28	25	0	25	190	190	0	50	-610
bubaak-split	28	0	28	28	0	28	207	204	3	50	-689
veriabs	29	0	29	31	0	31	203	203	0	51	-789
veriabsl	29	0	29	31	0	31	202	202	0	51	-790

Results – Verdicts



- True +/-: **+1** points
- False +/-: **-16/-32** points
  - *Common* false results
  - *Tool-specific* false results
- *Unconfirmed*: **no** points

Table 2. Safeguarded transformation (all tasks)

	False						True			Unconf.	Points
	Common			Tool							
	All	+	-	All	+	-	All	+	-		
uautomizer	25	0	25	38	38	0	1054	686	368	4	1054
ukojak	24	0	24	38	38	0	1036	680	356	3	1036
utaipan	25	0	25	35	35	0	952	621	331	4	952
cpachecker	23	0	23	39	39	0	765	444	321	6	765
esbmc-kind	23	0	23	4	1	3	805	427	378	8	709
mopsa	20	0	20	1	0	1	210	210	0	0	178
2ls	0	0	0	0	0	0	101	84	17	0	101
infer	0	0	0	0	0	0	0	0	0	0	0
cpv	0	0	0	0	0	0	0	0	0	0	0
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	0	70	391	0	391	1113	1113	0	59	-11399
[illegible]	71	0	71	391	0	391	1101	1101	0	59	-11411

Table 3. Non-safeguarded transformation (all tasks)

	False						True			Unconf.	Points
	Common			Tool							
	All	+	-	All	+	-	All	+	-		
uautomizer	24	0	24	39	38	1	1142	769	373	5	1110
ukojak	23	0	23	39	38	1	1097	739	358	3	1065
utaipan	24	0	24	36	36	0	1028	690	338	5	1028
cpachecker	22	0	22	78	78	0	792	451	341	5	792
esbmc-kind	22	0	22	60	57	3	827	444	383	8	731
mopsa	22	0	22	1	0	1	212	212	0	0	180
2ls	0	0	0	3	3	0	98	81	17	0	98
infer	0	0	0	0	0	0	0	0	0	0	0
cpv	0	0	0	0	0	0	0	0	0	0	0
theta	67	0	67	208	0	208	1355	1158	197	66	-5301
ergentheta	68	0	68	210	0	210	1344	1147	197	59	-5376
symbiotic	65	0	65	352	1	351	1190	1139	51	173	-10042
bubaak	67	0	67	355	1	354	1229	1176	53	236	-10099
baak-split	68	0	68	375	0	375	1201	1170	31	59	-10799
goblint	66	0	66	396	0	396	1120	1120	0	59	-11552
veriabs	65	0	65	407	0	407	1169	1169	0	59	-11855
veriabsl	65	0	65	407	0	407	1169	1169	0	59	-11855

Unbounded integers

Table 4. Safeguarded transformation (CHC-COMP'23)

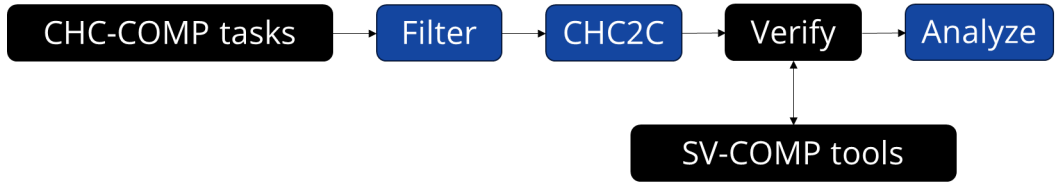
	False						True			Unconf.	Points
	Common			Tool							
	All	+	-	All	+	-	All	+	-		
utaipan	8	0	8	4	4	0	103	82	21	9	103
uautomizer	8	0	8	6	6	0	94	73	21	7	94
cpachecker	8	0	8	6	6	0	91	71	20	11	91
ukojak	7	0	7	6	6	0	87	68	19	9	87
mopsa	10	0	10	0	0	0	56	56	0	9	56
esbmc-kind	9	0	9	1	0	1	86	67	19	14	54
2ls	0	0	0	0	0	0	17	15	2	0	17
infer	0	0	0	0	0	0	0	0	0	0	0
cpv	0	0	0	0	0	0	0	0	0	0	0
emergentheta	32	0	32	13	0	13	168	163	5	48	-248
theta	37	0	37	14	0	14	198	190	8	48	-250
bubaak	39	0	39	23	0	23	234	234	0	52	-502
symbiotic	37	0	37	23	0	23	208	208	0	51	-528
bubaak-split	34	0	34	23	0	23	198	198	0	50	-538
veriabsl	30	0	30	23	0	23	190	190	0	50	-546
veriabs	31	0	31	23	0	23	189	189	0	50	-547
goblint	28	0	28	23	0	23	182	182	0	50	-554

Table 5. Non-safeguarded transformation (CHC-COMP'23)

	False						True			Unconf.	Points
	Common			Tool							
	All	+	-	All	+	-	All	+	-		
utaipan	8	0	8	4	4	0	133	108	25	10	133
cpachecker	12	0	12	15	15	0	117	90	27	10	117
uautomizer	8	0	8	7	6	1	116	93	23	10	84
ukojak	7	0	7	7	6	1	114	91	23	9	82
mopsa	12	0	12	0	0	0	76	76	0	9	76
esbmc-kind	9	0	9	15	14	1	93	72	21	14	61
2ls	0	0	0	0	0	0	17	15	2	0	17
infer	0	0	0	0	0	0	0	0	0	0	0
cpv	0	0	0	0	0	0	0	0	0	0	0
bubaak	34	0	34	20	0	20	258	247	11	70	-382
symbiotic	29	0	29	20	0	20	219	209	10	63	-421
emergentheta	31	0	31	23	0	23	226	218	8	51	-510
theta	29	0	29	23	0	23	212	204	8	50	-524
goblint	28	0	28	25	0	25	190	190	0	50	-610
bubaak-split	28	0	28	28	0	28	207	204	3	50	-689
veriabs	29	0	29	31	0	31	203	203	0	51	-789
veriabsl	29	0	29	31	0	31	202	202	0	51	-790

No common false positives
(low number of common false negatives)

Results – Verdicts



- True +/-: **+1** points
- False +/-: **-16/-32** points
  - *Common* false results
  - *Tool-specific* false results
- *Unconfirmed*: **no** points

Table 2. Safeguarded transformation (all tasks)

	False						True			Unconf.	Points
	Common			Tool							
	All	+	-	All	+	-	All	+	-		
uautomizer	25	0	25	38	38	0	1054	686	368	4	1054
ukojak	24	0	24	38	38	0	1036	680	356	3	1036
utaipan	25	0	25	35	35	0	952	621	331	4	952
cpachecker	23	0	23	39	39	0	765	444	321	6	765
esbmc-kind	23	0	23	4	1	3	805	427	378	8	709
mopsa	20	0	20	1	0	1	210	210	0	0	178
2ls	0	0	0	0	0	0	101	84	17	0	101
infer	0	0	0	0	0	0	0	0	0	0	0
cpv	0	0	0	0	0	0	0	0	0	0	0
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	0	70	391	0	391	1113	1113	0	59	-11399
[illegible]	71	0	71	391	0	391	1101	1101	0	59	-11411

Table 3. Non-safeguarded transformation (all tasks)

	False						True			Unconf.	Points
	Common			Tool							
	All	+	-	All	+	-	All	+	-		
uautomizer	24	0	24	39	38	1	1142	769	373	5	1110
ukojak	23	0	23	39	38	1	1097	739	358	3	1065
utaipan	24	0	24	36	36	0	1028	690	338	5	1028
cpachecker	22	0	22	78	78	0	792	451	341	5	792
esbmc-kind	22	0	22	60	57	3	827	444	383	8	731
mopsa	22	0	22	1	0	1	212	212	0	0	180
2ls	0	0	0	3	3	0	98	81	17	0	98
infer	0	0	0	0	0	0	0	0	0	0	0
cpv	0	0	0	0	0	0	0	0	0	0	0
theta	67	0	67	208	0	208	1355	1158	197	66	-5301
ergentheta	68	0	68	210	0	210	1344	1147	197	59	-5376
symbiotic	65	0	65	352	1	351	1190	1139	51	173	-10042
bubaak	67	0	67	355	1	354	1229	1176	53	236	-10099
baak-split	68	0	68	375	0	375	1201	1170	31	59	-10799
goblint	66	0	66	396	0	396	1120	1120	0	59	-11552
veriabs	65	0	65	407	0	407	1169	1169	0	59	-11855
veriabsl	65	0	65	407	0	407	1169	1169	0	59	-11855

Unbounded integers

No common false positives
(low number of common false negatives)

Table 4. Safeguarded transformation (CHC-COMP'23)

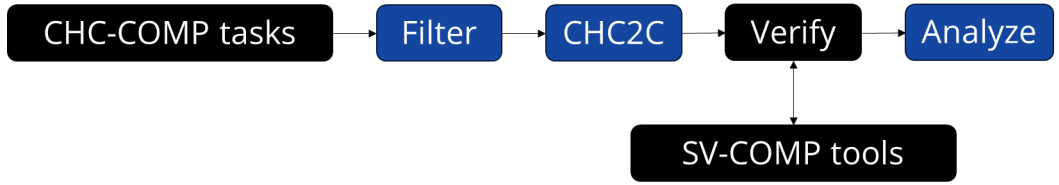
	False						True			Unconf.	Points
	Common			Tool							
	All	+	-	All	+	-	All	+	-		
utaipan	8	0	8	4	4	0	103	82	21	9	103
uautomizer	8	0	8	6	6	0	94	73	21	7	94
cpachecker	8	0	8	6	6	0	91	71	20	11	91
ukojak	7	0	7	6	6	0	87	68	19	9	87
mopsa	10	0	10	0	0	0	56	56	0	9	56
esbmc-kind	9	0	9	1	0	1	86	67	19	14	54
2ls	0	0	0	0	0	0	17	15	2	0	17
infer	0	0	0	0	0	0	0	0	0	0	0
cpv	0	0	0	0	0	0	0	0	0	0	0
emergentheta	32	0	32	13	0	13	168	163	5	48	-248
theta	37	0	37	14	0	14	198	190	8	48	-250
bubaak	39	0	39	23	0	23	234	234	0	52	-502
symbiotic	37	0	37	23	0	23	208	208	0	51	-528
bubaak-split	34	0	34	23	0	23	198	198	0	50	-538
veriabsl	30	0	30	23	0	23	190	190	0	50	-546
veriabs	31	0	31	23	0	23	189	189	0	50	-547
goblint	28	0	28	23	0	23	182	182	0	50	-554

Table 5. Non-safeguarded transformation (CHC-COMP'23)

	False						True			Unconf.	Points
	Common			Tool							
	All	+	-	All	+	-	All	+	-		
utaipan	8	0	8	4	4	0	133	108	25	10	133
cpachecker	12	0	12	15	15	0	117	90	27	10	117
uautomizer	8	0	8	7	6	1	116	93	23	10	84
ukojak	7	0	7	7	6	1	114	91	23	9	82
mopsa	12	0	12	0	0	0	76	76	0	9	76
esbmc-kind	9	0	9	15	14	1	93	72	21	14	61
2ls	0	0	0	0	0	0	17	15	2	0	17
infer	0	0	0	0	0	0	0	0	0	0	0
cpv	0	0	0	0	0	0	0	0	0	0	0
bubaak	34	0	34	20	0	20	258	247	11	70	-382
symbiotic	29	0	29	20	0	20	219	209	10	63	-421
emergentheta	31	0	31	23	0	23	226	218	8	51	-510
theta	29	0	29	23	0	23	212	204	8	50	-524
goblint	28	0	28	25	0	25	190	190	0	50	-610
bubaak-split	28	0	28	28	0	28	207	204	3	50	-689
veriabs	29	0	29	31	0	31	203	203	0	51	-789
veriabsl	29	0	29	31	0	31	202	202	0	51	-790

ULTIMATE family, CPACHECKER, ESBMC work best

Results – Verdicts



- True +/-: **+1** points
- False +/-: **-16/-32** points
  - *Common* false results
  - *Tool-specific* false results
- *Unconfirmed*: **no** points

Table 2. Safeguarded transformation (all tasks)

	False						True			Unconf.	Points
	Common			Tool							
	All	+	-	All	+	-	All	+	-		
uautomizer	25	0	25	38	38	0	1054	686	368	4	1054
ukojak	24	0	24	38	38	0	1036	680	356	3	1036
utaipan	25	0	25	35	35	0	952	621	331	4	952
cpachecker	23	0	23	39	39	0	765	444	321	6	765
esbmc-kind	23	0	23	4	1	3	805	427	378	8	709
mopsa	20	0	20	1	0	1	210	210	0	0	178
2ls	0	0	0	0	0	0	101	84	17	0	101
infer	0	0	0	0	0	0	0	0	0	0	0
cpv	0	0	0	0	0	0	0	0	0	0	0
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	0	70	391	0	391	1113	1113	0	59	-11399
[illegible]	71	0	71	391	0	391	1101	1101	0	59	-11411

Table 3. Non-safeguarded transformation (all tasks)

	False						True			Unconf.	Points
	Common			Tool							
	All	+	-	All	+	-	All	+	-		
uautomizer	24	0	24	39	38	1	1142	769	373	5	1110
ukojak	23	0	23	39	38	1	1097	739	358	3	1065
utaipan	24	0	24	36	36	0	1028	690	338	5	1028
cpachecker	22	0	22	78	78	0	792	451	341	5	792
esbmc-kind	22	0	22	60	57	3	827	444	383	8	731
mopsa	22	0	22	1	0	1	212	212	0	0	180
2ls	0	0	0	3	3	0	98	81	17	0	98
infer	0	0	0	0	0	0	0	0	0	0	0
cpv	0	0	0	0	0	0	0	0	0	0	0
theta	67	0	67	208	0	208	1355	1158	197	66	-5301
ergentheta	68	0	68	210	0	210	1344	1147	197	59	-5376
symbiotic	65	0	65	352	1	351	1190	1139	51	173	-10042
bubaak	67	0	67	355	1	354	1229	1176	53	236	-10099
baak-split	68	0	68	375	0	375	1201	1170	31	59	-10799
goblint	66	0	66	396	0	396	1120	1120	0	59	-11552
veriabs	65	0	65	407	0	407	1169	1169	0	59	-11855
veriabsl	65	0	65	407	0	407	1169	1169	0	59	-11855

Unbounded integers

Table 4. Safeguarded transformation (CHC-COMP'23)

	False						True			Unconf.	Points
	Common			Tool							
	All	+	-	All	+	-	All	+	-		
utaipan	8	0	8	4	4	0	103	82	21	9	103
uautomizer	8	0	8	6	6	0	94	73	21	7	94
cpachecker	8	0	8	6	6	0	91	71	20	11	91
ukojak	7	0	7	6	6	0	87	68	19	9	87
mopsa	10	0	10	0	0	0	56	56	0	9	56
esbmc-kind	9	0	9	1	0	1	86	67	19	14	54
2ls	0	0	0	0	0	0	17	15	2	0	17
infer	0	0	0	0	0	0	0	0	0	0	0
cpv	0	0	0	0	0	0	0	0	0	0	0
emergentheta	32	0	32	13	0	13	168	163	5	48	-248
theta	37	0	37	14	0	14	198	190	8	48	-250
bubaak	39	0	39	23	0	23	234	234	0	52	-502
symbiotic	37	0	37	23	0	23	208	208	0	51	-528
bubaak-split	34	0	34	23	0	23	198	198	0	50	-538
veriabsl	30	0	30	23	0	23	190	190	0	50	-546
veriabs	31	0	31	23	0	23	189	189	0	50	-547
goblint	28	0	28	23	0	23	182	182	0	50	-554

Table 5. Non-safeguarded transformation (CHC-COMP'23)

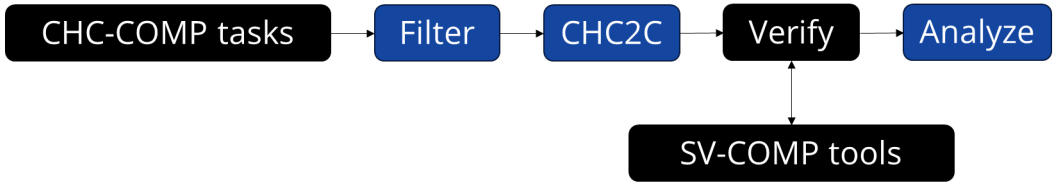
	False						True			Unconf.	Points
	Common			Tool							
	All	+	-	All	+	-	All	+	-		
utaipan	8	0	8	4	4	0	133	108	25	10	133
cpachecker	12	0	12	15	15	0	117	90	27	10	117
uautomizer	8	0	8	7	6	1	116	93	23	10	84
ukojak	7	0	7	7	6	1	114	91	23	9	82
mopsa	12	0	12	0	0	0	76	76	0	9	76
esbmc-kind	9	0	9	15	14	1	93	72	21	14	61
2ls	0	0	0	0	0	0	17	15	2	0	17
infer	0	0	0	0	0	0	0	0	0	0	0
cpv	0	0	0	0	0	0	0	0	0	0	0
bubaak	34	0	34	20	0	20	258	247	11	70	-382
symbiotic	29	0	29	20	0	20	219	209	10	63	-421
emergentheta	31	0	31	23	0	23	226	218	8	51	-510
theta	29	0	29	23	0	23	212	204	8	50	-524
goblint	28	0	28	25	0	25	190	190	0	50	-610
bubaak-split	28	0	28	28	0	28	207	204	3	50	-689
veriabs	29	0	29	31	0	31	203	203	0	51	-789
veriabsl	29	0	29	31	0	31	202	202	0	51	-790

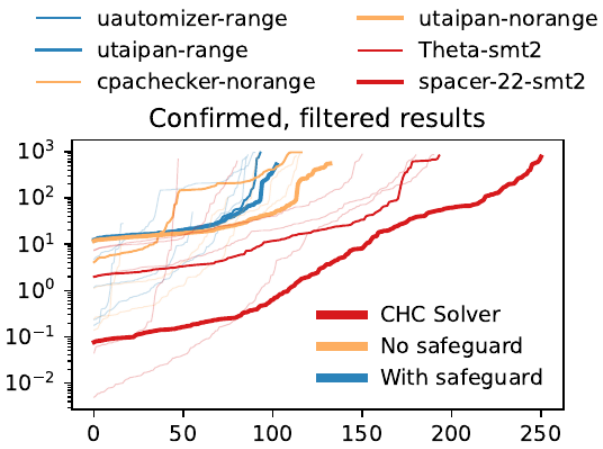
No common false positives
(low number of common false negatives)

ULTIMATE family, CPACHECKER, ESBMC work best

2LS produced no wrong results

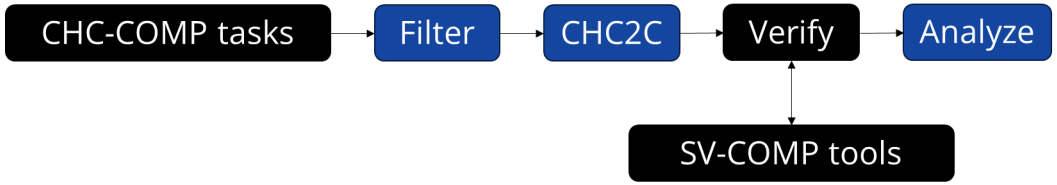
Results – Performance





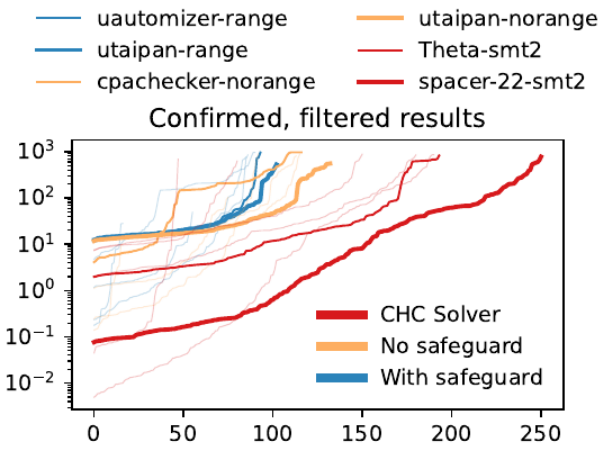
Filtered:
No negative scoring tools
Unconfirmed:
No CHC solver succeeded

Results – Performance



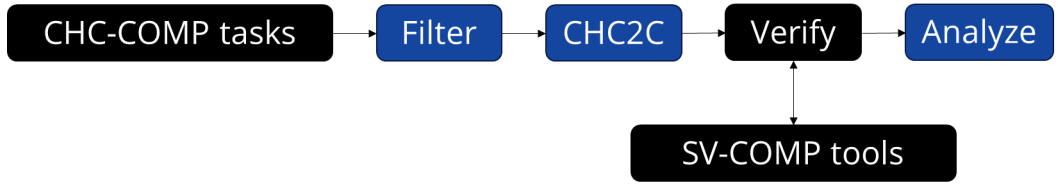
Favors CHC solvers

Favors CHC solvers



Filtered:
No negative scoring tools
Unconfirmed:
No CHC solver succeeded

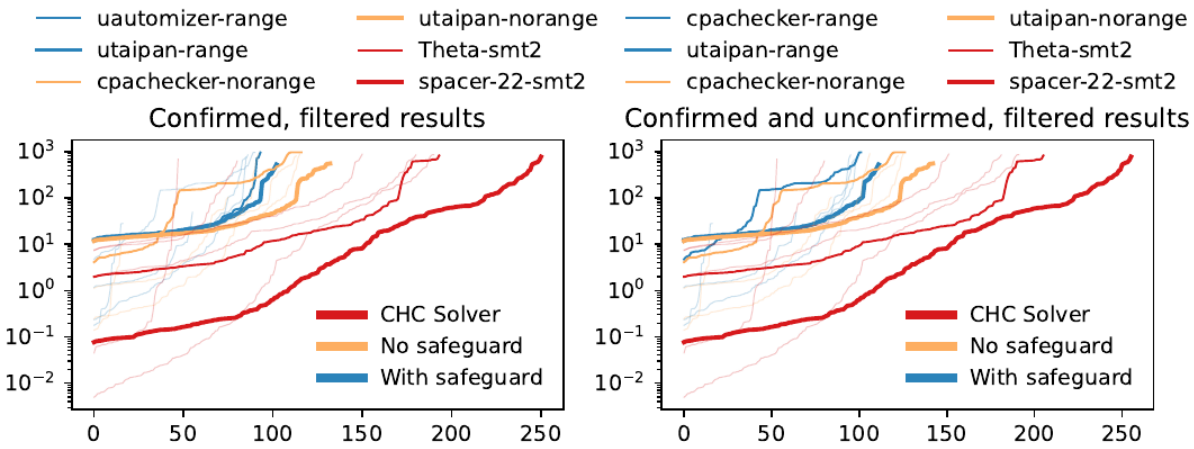
Results – Performance



Favors CHC solvers

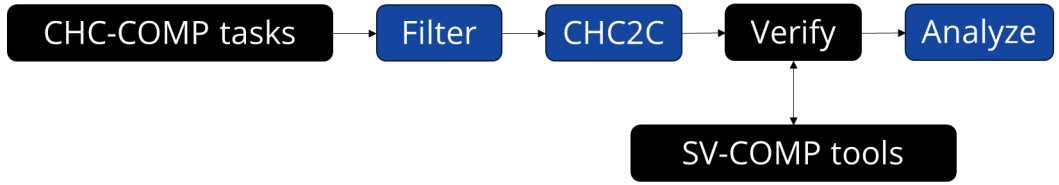
Favors SW verifiers

Favors CHC solvers



Filtered:
No negative scoring tools
Unconfirmed:
No CHC solver succeeded

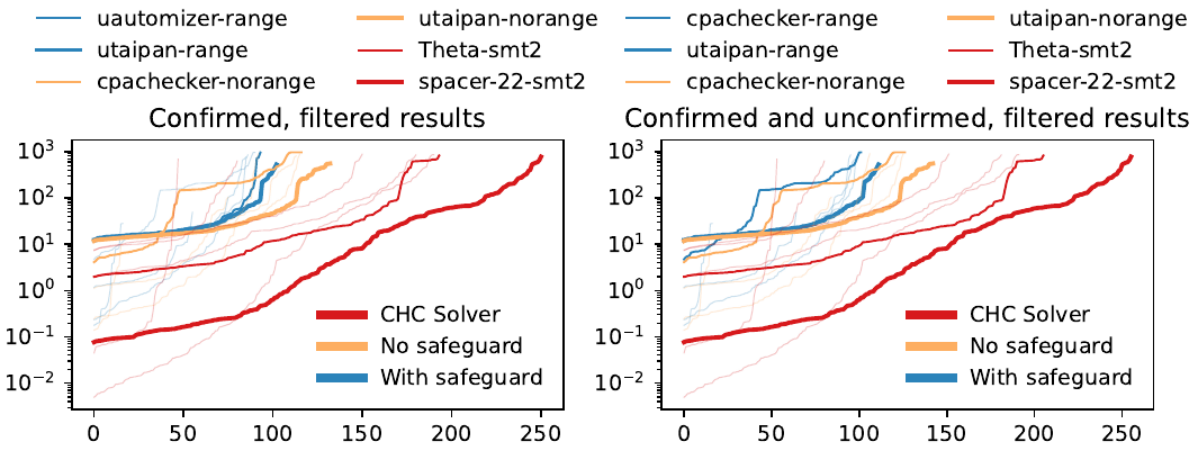
Results – Performance



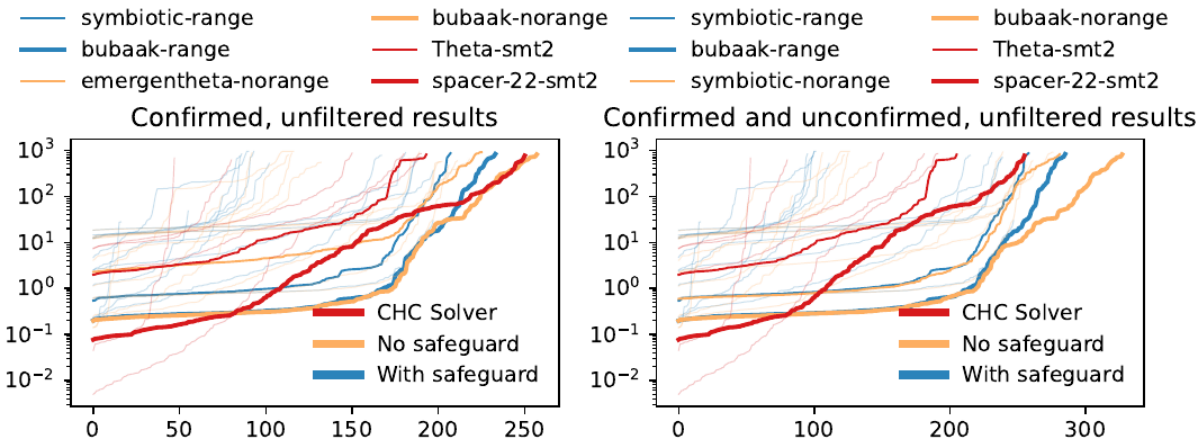
Favors CHC solvers

Favors SW verifiers

Favors CHC solvers

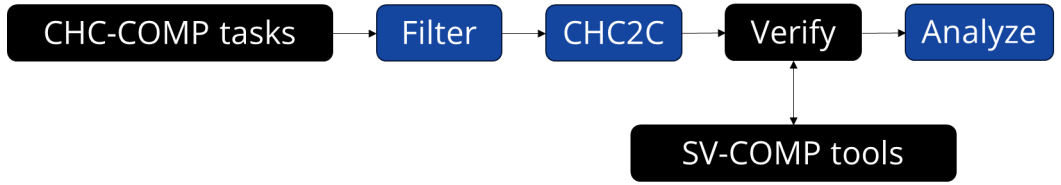


Favors SW verifiers



Filtered:
No negative scoring tools
Unconfirmed:
No CHC solver succeeded

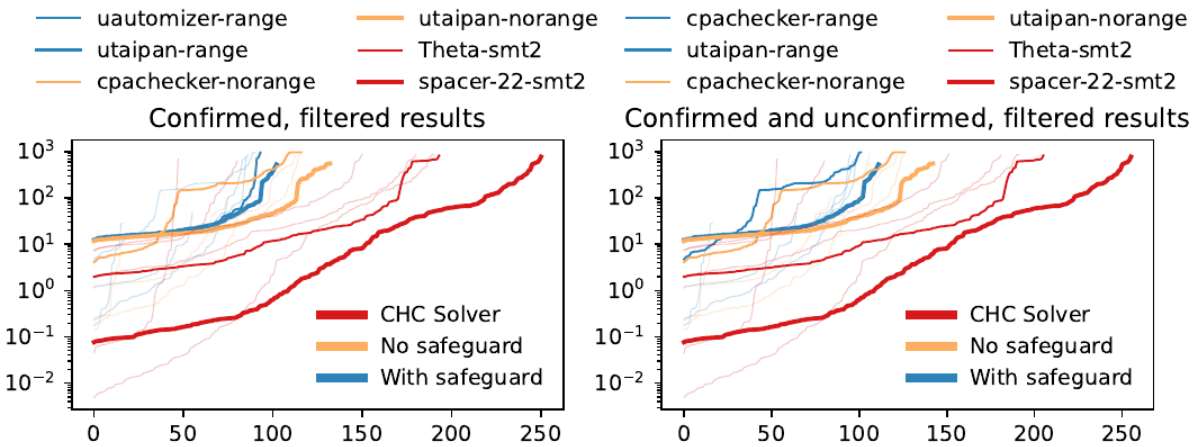
Results – Performance



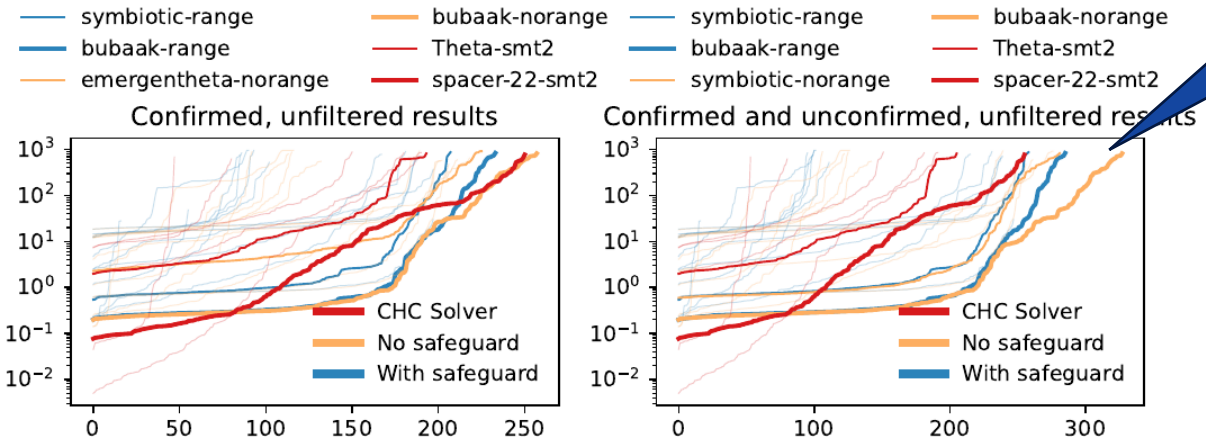
Favors CHC solvers

Favors SW verifiers

Favors CHC solvers



Favors SW verifiers



Some SW verifiers outperform dedicated CHC solvers

Filtered:
No negative scoring tools
Unconfirmed:
No CHC solver succeeded

Significance & Summary

Why should you care?

Has this benefitted CHC solving?

Has this benefitted CHC solving?

- We believe so…

Has this benefitted CHC solving?

- We believe so…

New solvers (for LIA-lin out-of-the-box)

Has this benefitted CHC solving?

- We believe so…

New solvers (for LIA-lin out-of-the-box)

Previously unsolved tasks (within time)

Has this benefitted CHC solving?

- We believe so…

New solvers (for LIA-lin out-of-the-box)

Previously unsolved tasks (within time)

More competition, more visibility

And software verification?

- We are sure!

And software verification?

- We are sure!

ISO/IEC 9899:202x

6.3.1.2 Boolean type

1 When any scalar value is converted to `_Bool`, the result is 0 if the value compares equal to 0; otherwise, the result is 1.[60)]

And software verification?

- We are sure!

ISO/IEC 9899:202x

6.3.1.2 Boolean type

1 When any scalar value is converted to **_Bool**, the result is 0 if the value compares equal to 0; otherwise, the result is 1.[60)]

```
extern _Bool __VERIFIER_nondet_Bool();
extern void reach_error();
int main(){
  _Bool b = __VERIFIER_nondet_Bool();
  switch(b) {
    case 0: return 0;
    case 1: return 0;
  }
  reach_error(); // never called?
}
```

And software verification?

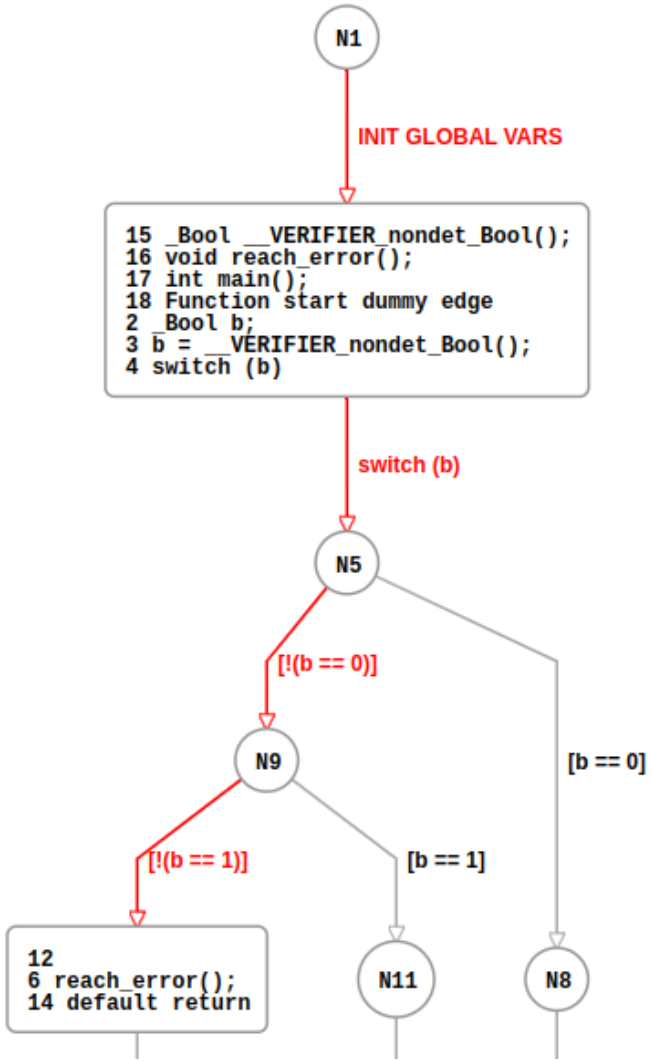
- We are sure!

ISO/IEC 9899:202x

6.3.1.2 Boolean type

1 When any scalar value is converted to **_Bool**, the result is 0 if the value compares equal to 0; otherwise, the result is 1.[60)]

```
extern _Bool __VERIFIER_nondet_Bool();
extern void reach_error();
int main(){
  _Bool b = __VERIFIER_nondet_Bool();
  switch(b) {
    case 0: return 0;
    case 1: return 0;
  }
  reach_error(); // never called?
}
```



And software verifi

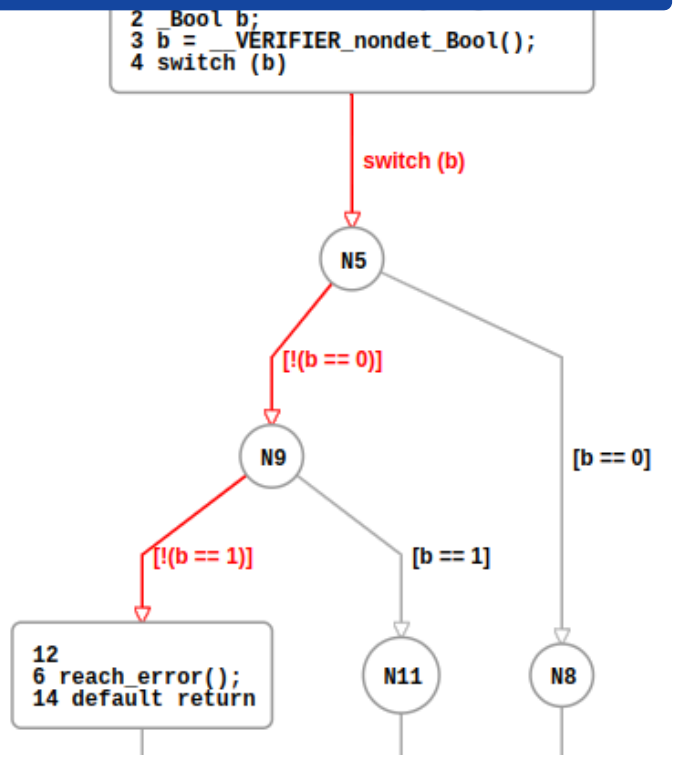
- We are sure!

6.3.1.2 Boolean type

1 When any scalar value is converted to **_Bool**, the result
otherwise, the result is 1.[60)]

```
extern _Bool __VERIFIER_nondet_Bool();
extern void reach_error();
int main(){
  _Bool b = __VERIFIER_nondet_Bool();
  switch(b) {
    case 0: return 0;
    case 1: return 0;
  }
  reach_error(); // never called?
}
```

2ls	bubaak	bubaak-split	cpachecker	cpv	emergentheta	esbmc-kind	goblint	infer	mopsa	symbiotic	theta	uautomizer	ukojak	utaipan	veriabs	veriabsl
✓	✓	✓	×	?	✓	✓	✓	?	?	✓	✓	×	×	×	✓	✓



And software verification?

- We are sure!

Added CHC benchmarks

Open **Levente Bajczi** requested to merge `levente.bajczi/sv-benchm…` into `main` 5 months ago

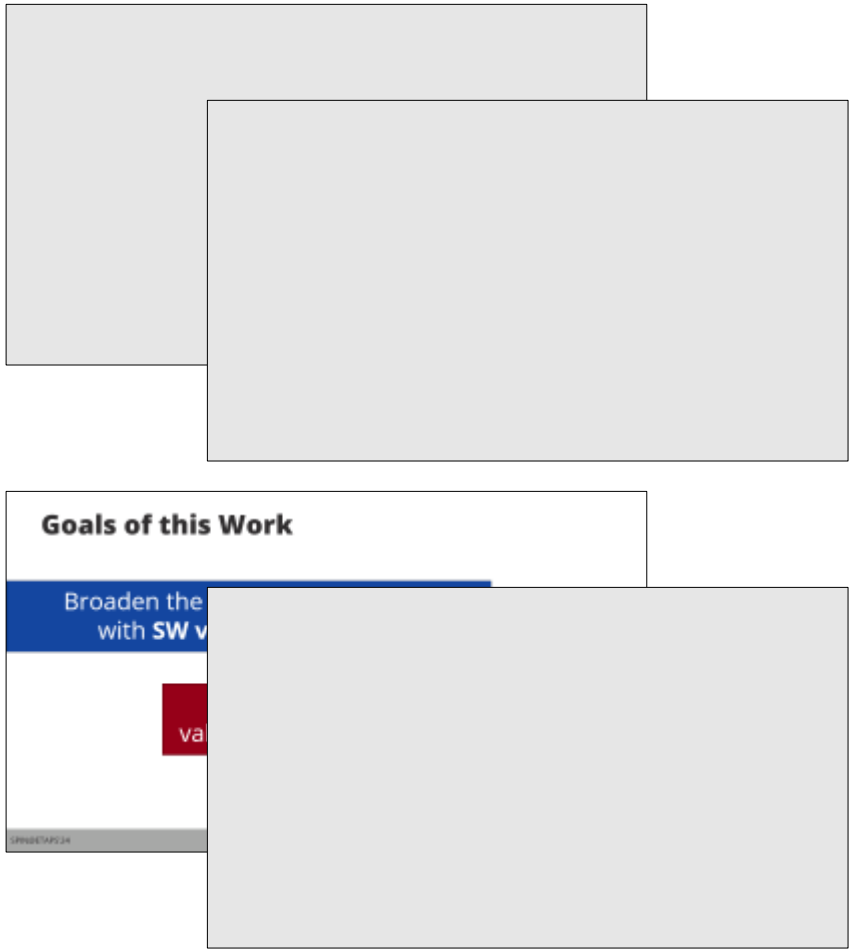
Overview 4 Commits 10 Pipelines 6 Changes 333+

This PR adds 2774 new benchmarks to the repository. These are transformed CHC benchmarks, originally sourced from the https://github.com/chc-comp/ organization to be used for CHC-COMP, which have been converted into CFAs and then to C files. See our (accepted, pending publication) paper at HCVS'23 on the transformation of CHC problems to CFAs: submitted.pdf

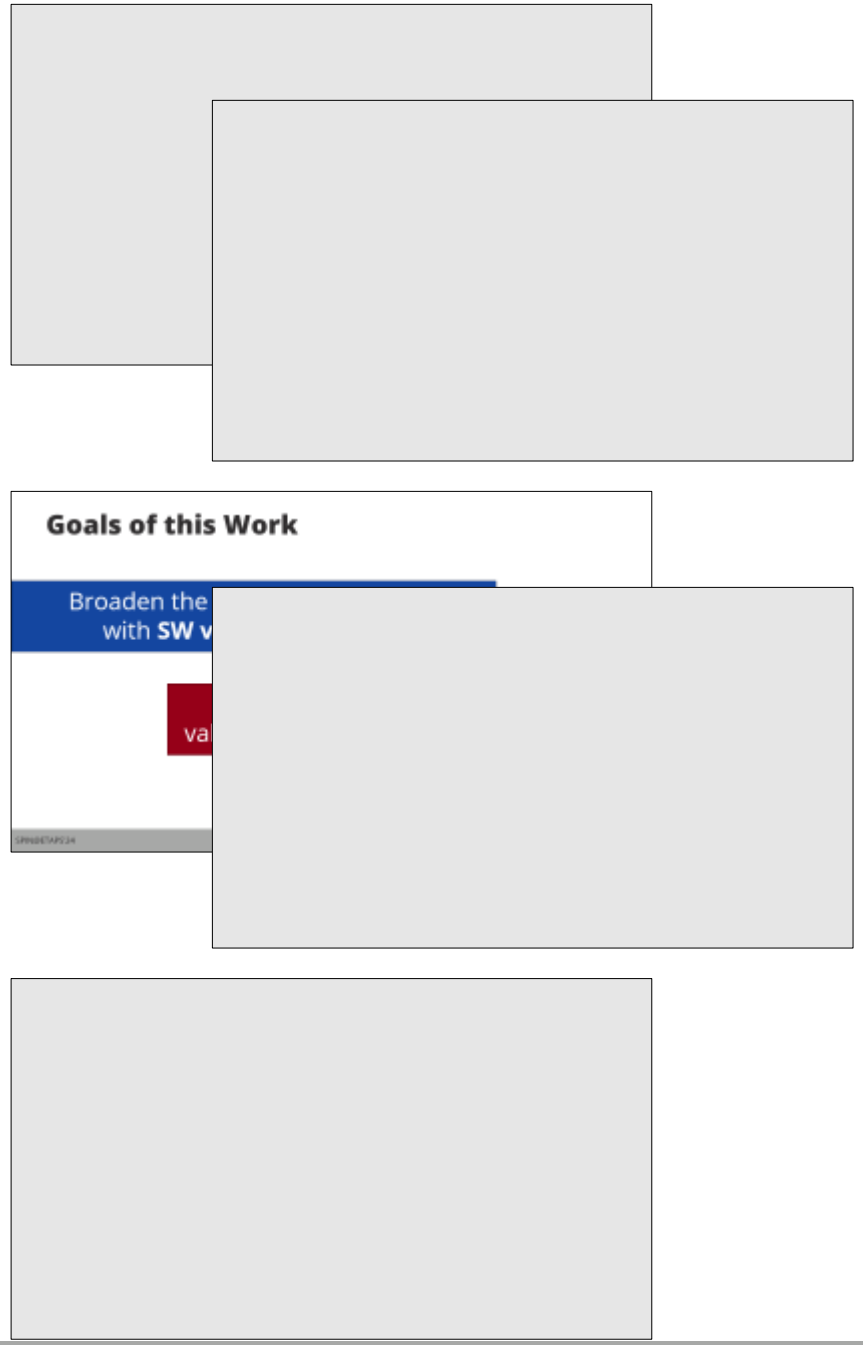
New benchmarks (2774)!

Summary

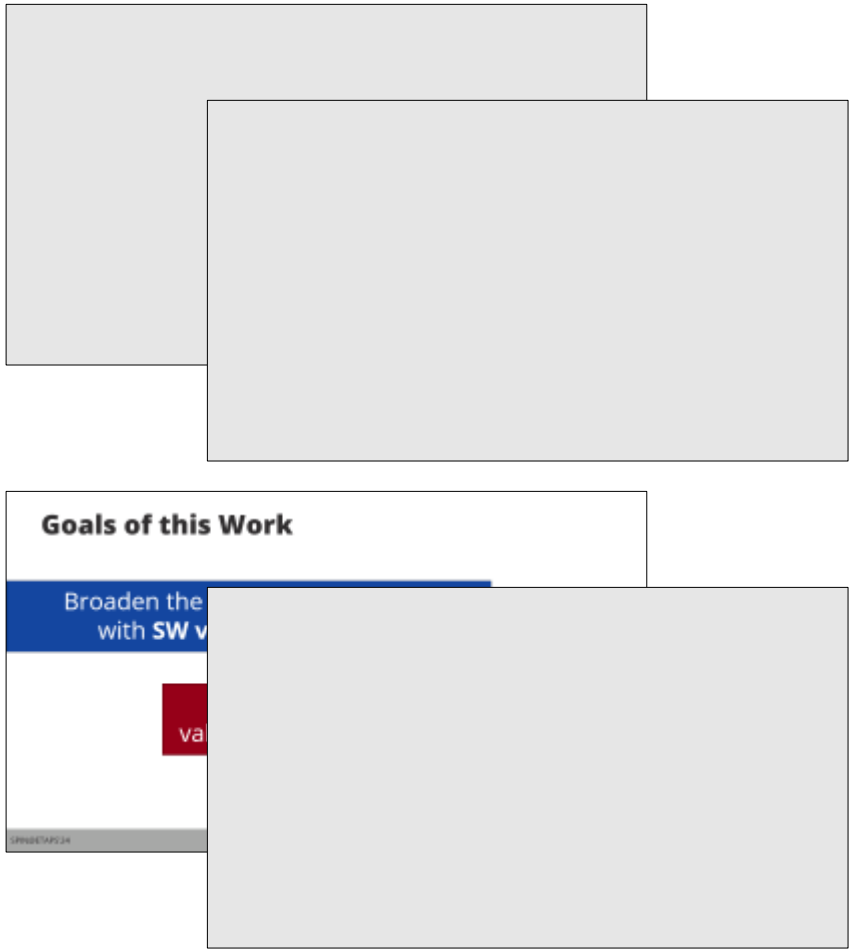
Summary



Summary



Summary



Summary

Published January 18, 2024 | Version v1

Dataset Open

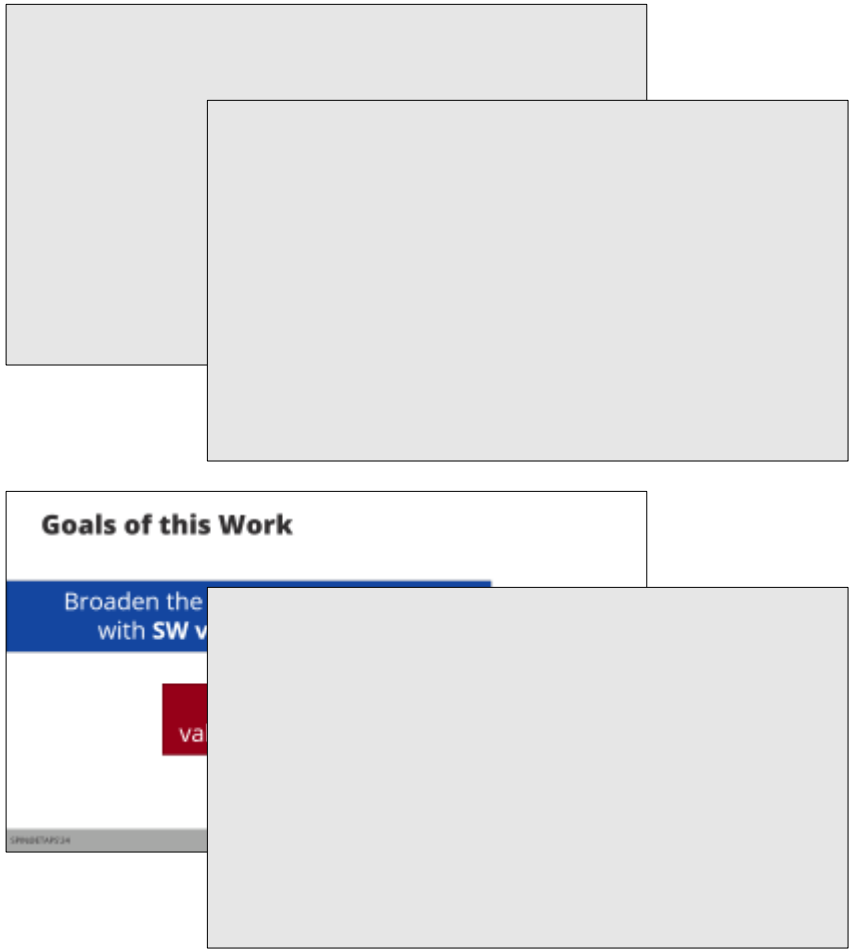
Solving Constrained Horn Clauses as C Programs with CHC2C

Bajczi, Levente[1]; Molnár, Vince[1]

Show affiliations

10.5281/zenodo.10529452

Summary



Published January 18, 2024 | Version v1

Dataset Open

Solving Constrained Horn Clauses as C Programs with CHC2C

Bajczi, Levente[1]; Molnár, Vince[1]

Show affiliations

10.5281/zenodo.10529452

Benchmarks

Results

Analysis scripts

CHC2C