Deriving Small Unsatisfiable Cores with Dominators by Roman Gershman, Maya Koifman, Ofer Strichman

Tobias Ambühl

December 7, 2006

"Logic is the art of going wrong with confidence." (Joseph Wood Krutch)

Motivation

The following CNF formula is not satisfiable!

$L = \{\{p,r\}, \{q,\neg r\}, \{\neg q\}, \{p,s\}, \{\neg s\}, \{\neg p,t\}, \{s,\neg t\}\}$

Definition: unsatisfiable core UC

An unsatisfiable core UC is any subset of the clauses of L that is still unsatisfiable.

Motivation

The following CNF formula is not satisfiable!

L = {{p,r}, {q,¬ r}, {¬q}, {p,s}, {¬s}, {¬p,t}, {s,¬t}}

Definition: unsatisfiable core UC

An unsatisfiable core UC is any subset of the clauses of L that is still unsatisfiable.

Finding the minimal UC

- No algorithm that scales found by now for finding the minimal UC.
- Approach: Find a non-minimal UC

Finding the minimal UC

- No algorithm that scales found by now for finding the minimal UC.
- Approach: Find a non-minimal UC

Summary

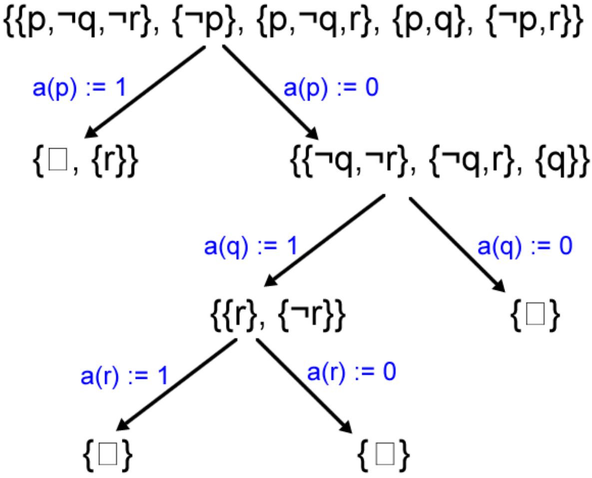
- Describe a heuristic called *Trimmer*.
- *Trimmer* tries to find a UC.

Usages

- UC reflects a more precise and focused explanation of the unsatisfiability of a CNF
- Used in several contexts of **verification** and **model-checking**
- *find papers in the reference section!*

Outline

SAT based on Davis-Putnam algorithm



Resolution

Proof system for CNF formulas

with one inference rule: $\frac{(A \vee x)(B \vee \neg x)}{(A \vee B)}$

- The clause $(A \vee B)$ is the *resolvent*
- $(A \vee x)$ and $(B \vee \neg x)$ are the *resolving clauses*
- The resolvent of the clauses (x) and (¬x) is the empty clause

Proof of unsatisfiability

Definition: Proof of unsatisfiability P for a set of clauses L

- Directed acyclic graph G(V,E)
- Every v $\in$ V either element of L (root) or the resolvent of two predecessors v1,v2 $\in$ V
- The empty clause is the sink.

Proof of unsatisfiability

Definition: Proof of unsatisfiability P for a set of clauses L

- Directed acyclic graph G(V,E)
- Every v $\in$ V either element of L (root) or the resolvent of two predecessors v1,v2 $\in$ V
- The empty clause is the sink.

Resolution graph

- A proof of unsatisfiability can be depicted in a *resolution graph*.
- Modern SAT solvers can output a proof of unsatisfiability.

Dominators

Flow graph

- Directed graph G = (V,E,r)
- Every vertex is reachable from root vertex $r \in V$

- Vertex $d \in V$ **dominates** $v \in V$, $v \neq d$, if every path from r to v includes d
- d **immediately dominates** v if it dominates v and there is no other node on the path between them that dominates v
- We name v a **minion** of d.
- M(d) is the set of minions of d.
- A node is called a **dominator** if it dominates at least one node.

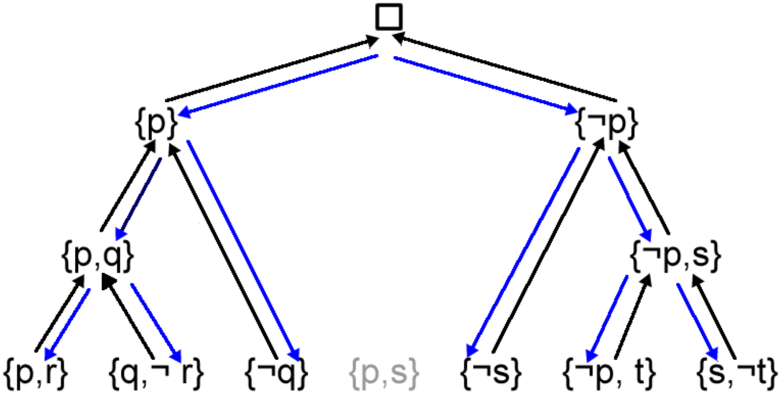
Dominators

Flow graph

- Directed graph G = (V,E,r)
- Every vertex is reachable from root vertex $r \in V$

- Vertex $d \in V$ **dominates** $v \in V$, $v \neq d$, if every path from r to v includes d
- d **immediately dominates** v if it dominates v and there is no other node on the path between them that dominates v
- We name v a **minion** of d.
- M(d) is the set of minions of d.
- A node is called a **dominator** if it dominates at least one node.

Example



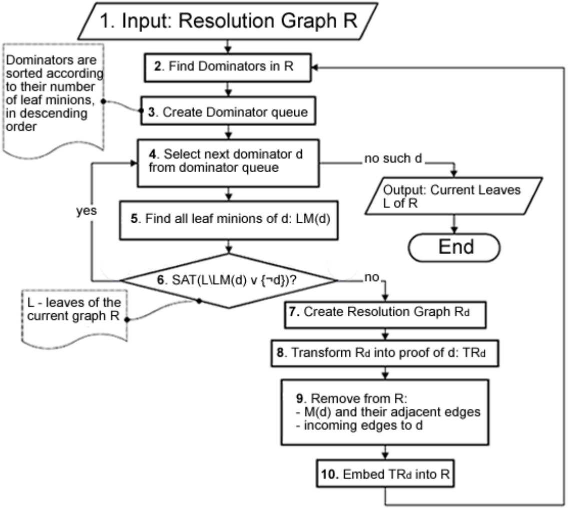
Refutation

Refutation methods are based on the following theorem

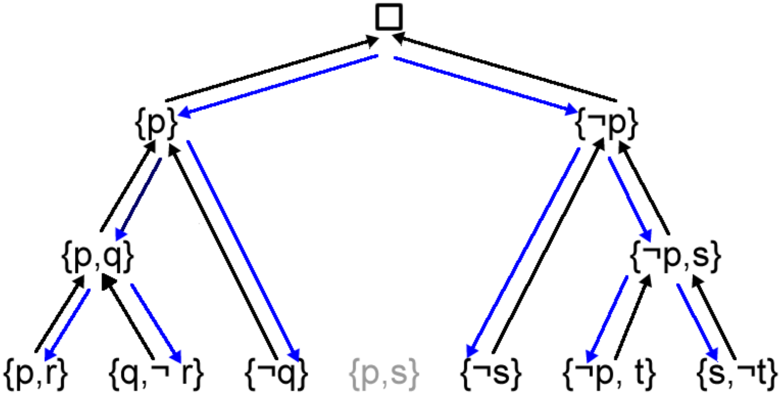
Theorem

$\Phi \models \mathrm{d}$ *if and only if* $\Phi \cup \{\neg \mathrm{d}\}$ *is unsatisfiable.*

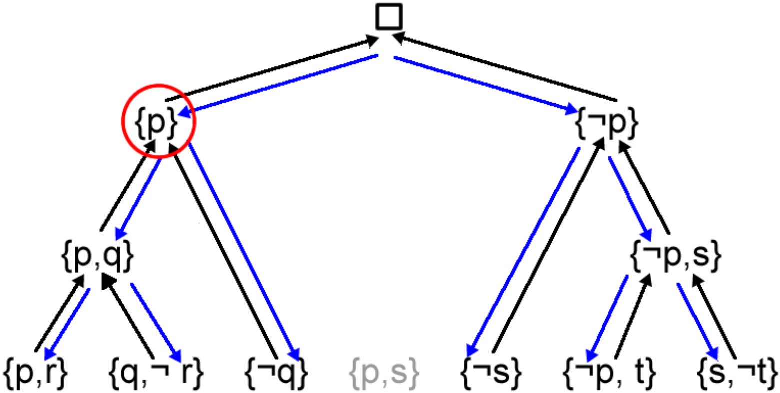
The Trimmer algorithm



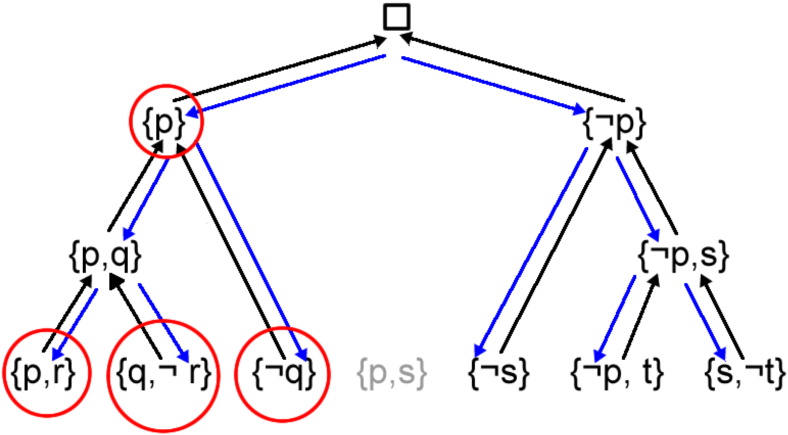
The Resolution Graph



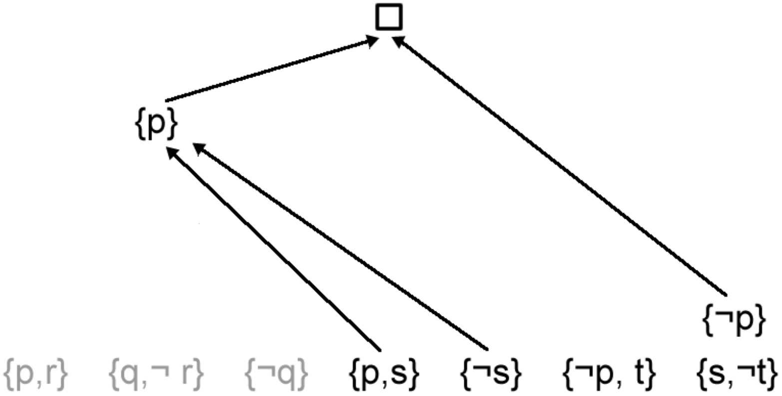
Select next dominator d



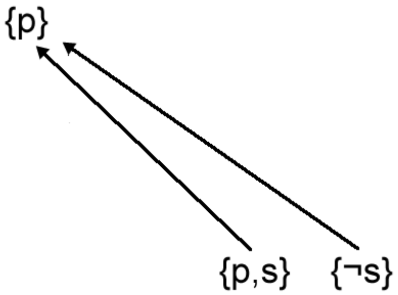
Find all the leaf minions of d



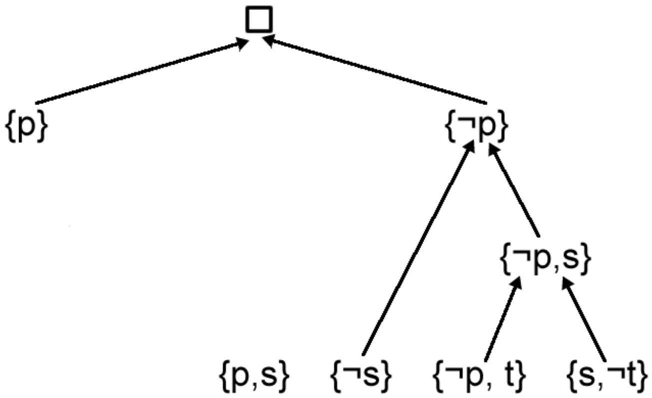
Create Resolution Graph



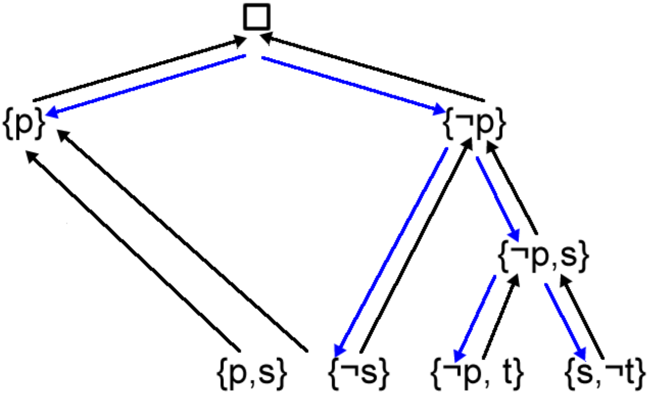
Transform R into proof of d



Removal



Embed TR into R



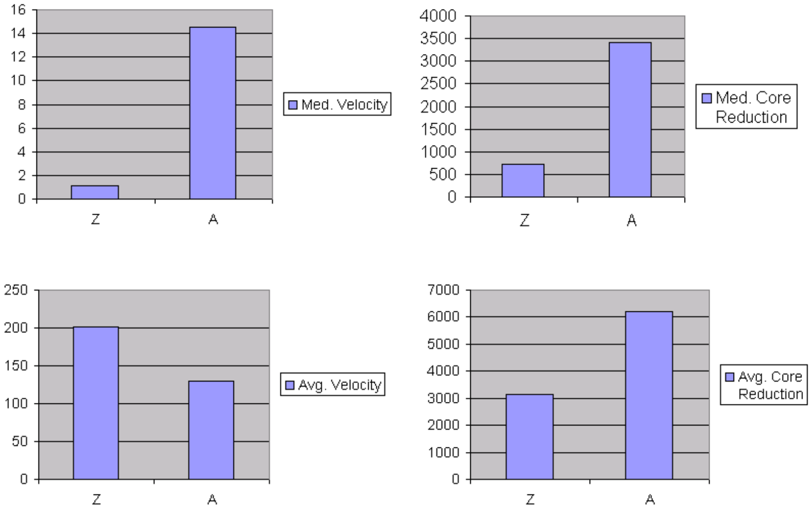
Implementation and Benchmark

- Benchmark composed of 75 unsatisfiable CNF
- Initial number of clauses ranges from 1'300 to 800'000 clauses

Comparison with...

- A: TrimTillFix
- Z: RunTillFix

Result


16
14
12
10
8
6
4
2
0
Z
A
Med. Velocity
4000
3500
3000
2500
2000
1500
1000
500
0
Z
A
Med. Core Reduction
250
200
150
100
50
0
Z
A
Avg. Velocity
7000
6000
5000
4000
3000
2000
1000
0
Z
A
Avg. Core Reduction

Conclusion

- Given an unsatisfiable CNF formula
- Want to find an UC, which does not have to be minimal
- *Trimmer* finds such an UC

References

- D.Kroening, J.Ouaknine, S.Seshia, O.Strichman. *Abstraction-based satisfiability solving of Presburger arithmetic.*
- R.Gershman, M.Koifman, O.Strichman. *Deriving Small Unsatisfiable Cores with Dominators*. Technion, Haifa, Israel
- Prof. Dr. Robert Stärk. *Logik für Informatiker*. ETH Zürich
- N.Amla, K.McMillan. *Auomatic abstraction without counterexamples.*
- Grumberg, Lerda, Strichman, Theobald. *Proof-guided underapproximation-widening for multi-process systems.*

Questions

- Any questions?
- Thank you for your attention!

Questions

- Any questions?
- Thank you for your attention!