From Propositional Model Counting to SAT Solving and Back

Sibylle Möhle-Rotondi

Institute for Formal Models and Verification
LIT Secure and Correct Systems Lab

JOHANNES KEPLER
UNIVERSITY LINZ

Who Wants the Model Count Anyway?

Planning

Software Verification

Cryptography

Hardware Verification

Bayesian Networks

Probabilistic Reasoning

Product Configuration

Planning

Software Verification

Cryptography

Hardware Verification

???

Bayesian Networks

Probabilistic Reasoning

Product Configuration

State of the Art in Exact Propositional Model Counting (#SAT)

Counting Based on the Davis-Putnam (DP) Algorithm [1]

- Explore the search space in an ordered manner

Component-Based Reasoning [2,3]

- Decompose formula into subformulae with distinct sets of variables, solve them independently and multiply their model counts
- Parallel and distributed version available [4,5]

[1] E. Birnbaum, E.L. Lozinskii, "The Good Old Davis-Putnam Procedure Helps Counting Models", JAIR, 1999.
[2] R.J. Bayardo, J.D. Pehoushek, "Counting Models Using Connected Components", AAAI'00.
[3] M. Thurley, "sharpSAT – Counting Models with Advanced Component Caching and Implicit BCP", SAT'06.
[4] J. Burchard, T. Schubert, B. Becker, "Laissez-Faire Caching for Parallel #SAT Solving", SAT'15.
[5] J. Burchard, T. Schubert, B. Becker, "Distributed Parallel #SAT Solving", CLUSTER'16.

Related Work

Dual Reasoning [6,7]

- Run one SAT solver on the formula and its negation simultaneously
- If the negation of a formula evaluates to true under a variable assignment, the assignment is a model of the formula and vice versa

Chronological Conflict-Driven Clause Learning (CDCL) [8,9]

- Combine chronological backtracking with CDCL
- Fix of several invariants violated by chronological backtracking in combination with CDCL

Chronological Conflict-Driven Clause Learning (CDCL) for Model Counting[10]

- Without the use of blocking clauses

[6] A. Biere, S. Hölldobler, S. Möhle, “An Abstract Dual Propositional Model Counter”, YSIP’17.
[7] S. Möhle, A. Biere, “Dualizing Projected Model Counting”, ICTAI’18.
[8] A. Nadel, V. Ryvchin, “Chronological Backtracking”, SAT’18.
[9] S. Möhle, A. Biere, “Backing Backtracking”, SAT’19.
[10] S. Möhle, A. Biere, “Combining Conflict-Driven Clause Learning and Chronological Backtracking for Propositional Model Counting”, GCAI’19.

Challenges in Exact Propositional Model Counting (#SAT) (1)

The Search Space Needs to be Explored Exhaustively

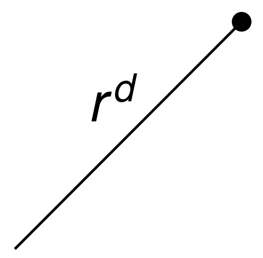
$F = (\overline{p} \vee q) \wedge (p \vee q)$ $\quad M = 0$

•

$V = \{p, q, r\}$

The Search Space Needs to be Explored Exhaustively

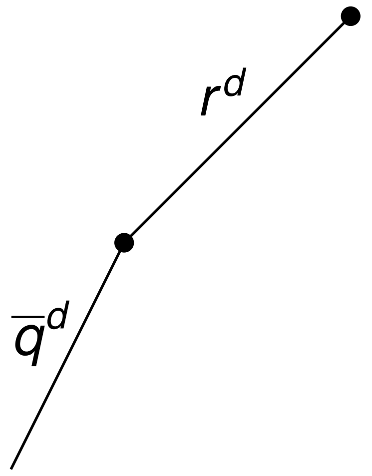
$$F \quad = (\overline{p} \vee q) \wedge (p \vee q) \qquad M = 0$$
$$F|_r \quad = (\overline{p} \vee q) \wedge (p \vee q) \qquad M = 0$$



$V = \{p, q, r\}$

The Search Space Needs to be Explored Exhaustively

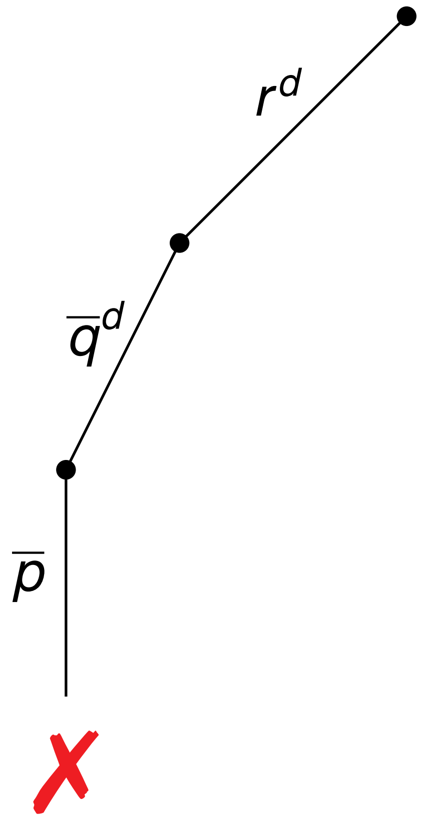
$$
\begin{aligned}
F &= (\overline{p} \vee q) \wedge (p \vee q) & M = 0 \\
F|_r &= (\overline{p} \vee q) \wedge (p \vee q) & M = 0 \\
F|_{r\overline{q}} &= (\overline{p}) \wedge (p) & M = 0
\end{aligned}
$$



$V = \{p, q, r\}$

The Search Space Needs to be Explored Exhaustively

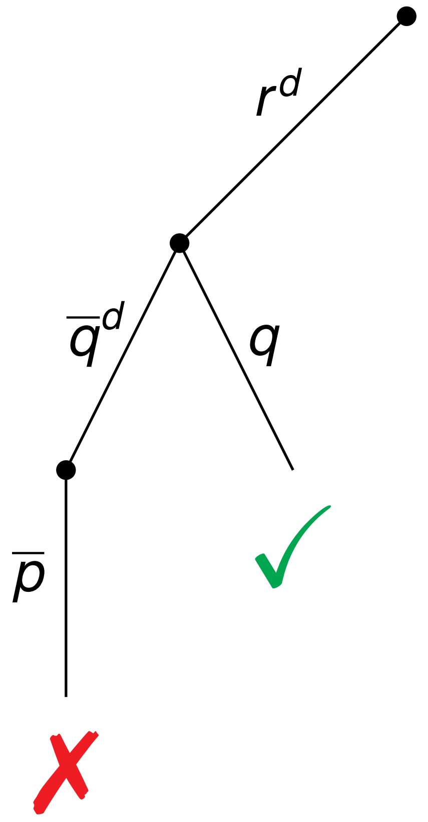
$$\begin{aligned} F &= (\overline{p} \vee q) \wedge (p \vee q) & M = 0 \\ F|_{r} &= (\overline{p} \vee q) \wedge (p \vee q) & M = 0 \\ F|_{r\overline{q}} &= (\overline{p}) \wedge (p) & M = 0 \\ F|_{r\overline{q}\overline{p}} &= \bot & M = 0 \end{aligned}$$



$V = \{p, q, r\}$

The Search Space Needs to be Explored Exhaustively

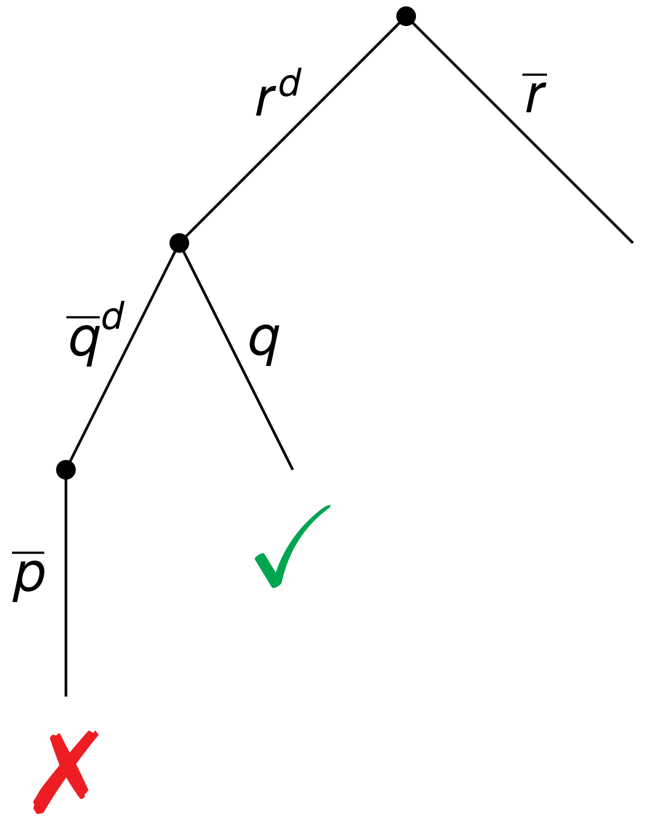
$$
\begin{aligned}
F &= (\overline{p} \vee q) \wedge (p \vee q) & M &= 0 \\
F|_r &= (\overline{p} \vee q) \wedge (p \vee q) & M &= 0 \\
F|_{r\overline{q}} &= (\overline{p}) \wedge (p) & M &= 0 \\
F|_{r\overline{q}\overline{p}} &= \bot & M &= 0 \\
F|_{rq} &= \top & M &= 2
\end{aligned}
$$



$V = \{p, q, r\}$

The Search Space Needs to be Explored Exhaustively

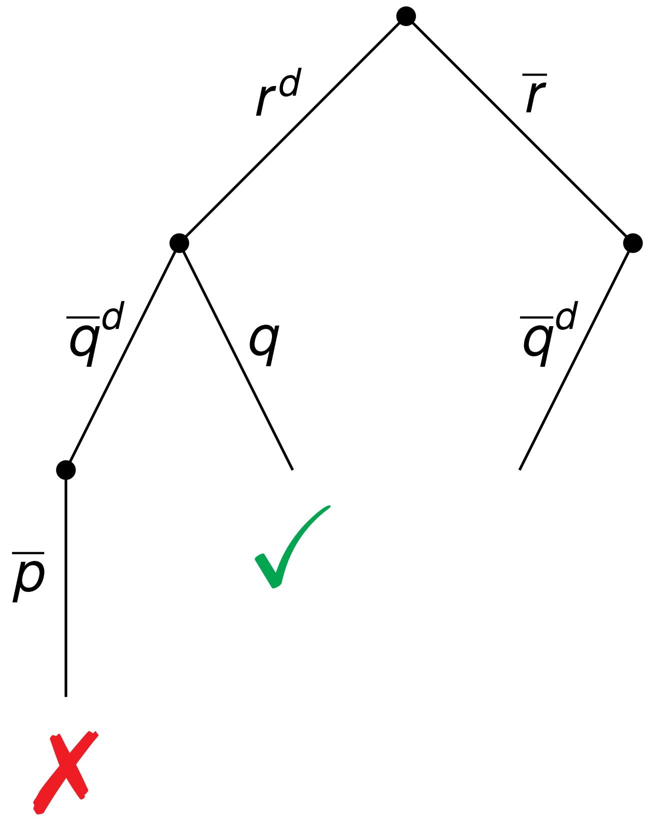
$$
\begin{aligned}
F \quad &= (\overline{p} \vee q) \wedge (p \vee q) & M = 0 \\
F|_r \quad &= (\overline{p} \vee q) \wedge (p \vee q) & M = 0 \\
F|_{r\overline{q}} \quad &= (\overline{p}) \wedge (p) & M = 0 \\
F|_{r\overline{q}\overline{p}} &= \bot & M = 0 \\
F|_{rq} \quad &= \top & M = 2 \\
F|_{\overline{r}} \quad &= (\overline{p} \vee q) \wedge (p \vee q) & M = 2
\end{aligned}
$$



$V = \{p, q, r\}$

The Search Space Needs to be Explored Exhaustively

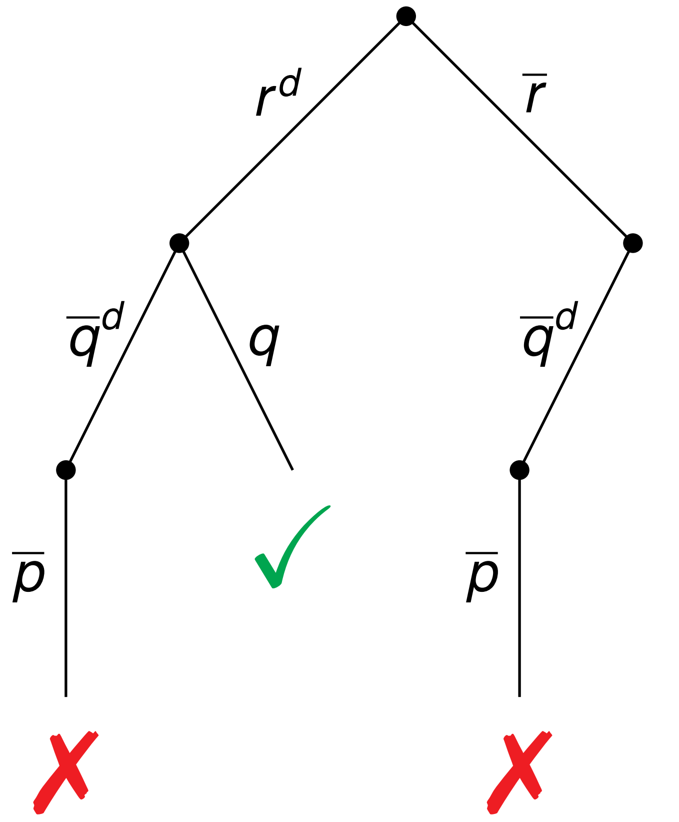
$$
\begin{aligned}
F &= (\overline{p} \vee q) \wedge (p \vee q) & M = 0 \\
F|_{r} &= (\overline{p} \vee q) \wedge (p \vee q) & M = 0 \\
F|_{r\overline{q}} &= (\overline{p}) \wedge (p) & M = 0 \\
F|_{r\overline{q}\overline{p}} &= \bot & M = 0 \\
F|_{rq} &= \top & M = 2 \\
F|_{\overline{r}} &= (\overline{p} \vee q) \wedge (p \vee q) & M = 2 \\
F|_{\overline{r}\overline{q}} &= (\overline{p}) \wedge (p) & M = 2
\end{aligned}
$$



$V = \{p, q, r\}$

The Search Space Needs to be Explored Exhaustively

$$
\begin{aligned}
F &= (\overline{p} \lor q) \land (p \lor q) & M &= 0\\
F|_r &= (\overline{p} \lor q) \land (p \lor q) & M &= 0\\
F|_{r\overline{q}} &= (\overline{p}) \land (p) & M &= 0\\
F|_{r\overline{q}\overline{p}} &= \bot & M &= 0\\
F|_{rq} &= \top & M &= 2\\
F|_{\overline{r}} &= (\overline{p} \lor q) \land (p \lor q) & M &= 2\\
F|_{\overline{r}\overline{q}} &= (\overline{p}) \land (p) & M &= 2\\
F|_{\overline{r}\overline{q}\overline{p}} &= \bot & M &= 2
\end{aligned}
$$

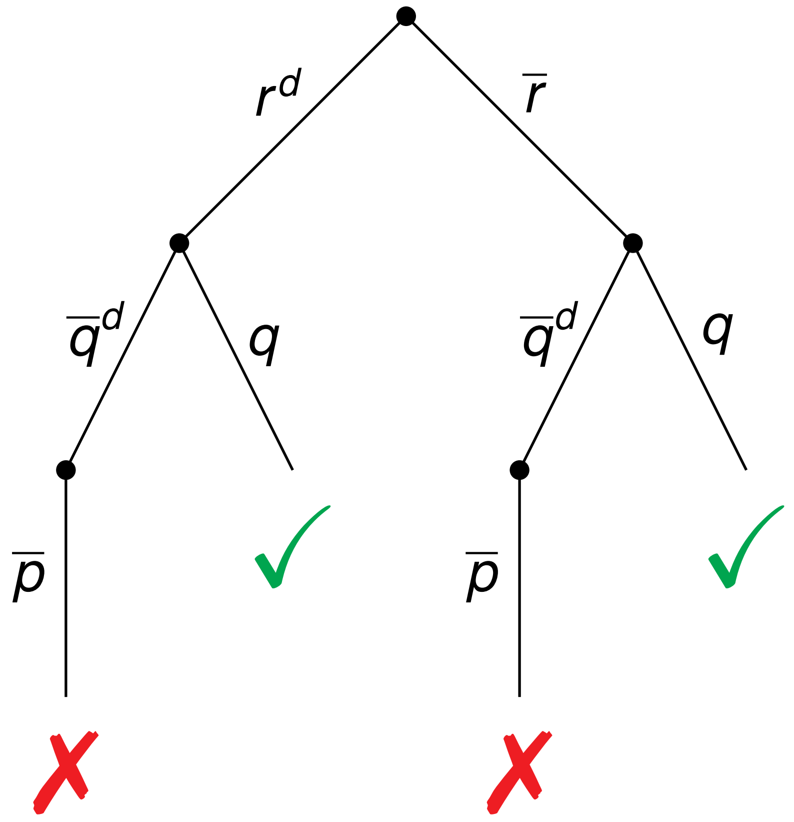


$V = \{p, q, r\}$

The Search Space Needs to be Explored Exhaustively

$$
\begin{aligned}
F &= (\overline{p} \vee q) \wedge (p \vee q) & M = 0\\
F|_r &= (\overline{p} \vee q) \wedge (p \vee q) & M = 0\\
F|_{r\overline{q}} &= (\overline{p}) \wedge (p) & M = 0\\
F|_{r\overline{q}\overline{p}} &= \bot & M = 0\\
F|_{rq} &= \top & M = 2\\
F|_{\overline{r}} &= (\overline{p} \vee q) \wedge (p \vee q) & M = 2\\
F|_{\overline{r}\overline{q}} &= (\overline{p}) \wedge (p) & M = 2\\
F|_{\overline{r}\overline{q}\overline{p}} &= \bot & M = 2\\
F|_{\overline{r}q} &= \top & M = 4
\end{aligned}
$$

$V = \{p, q, r\}$



And CDCL is biased towards conflicts!

Dualizing Projected Model Counting (ICTAI'18)

Projected Model Counting

$F(X, Y)$ (arbitrary) propositional formula over variables X and Y with $X \cap Y = \emptyset$

X *relevant* input variables
Y *irrelevant* input variables

We are interested in the number of models projected onto X:

$$\#\exists Y.F(X, Y)$$

Projected Model Counting

$F(X, Y)$ (arbitrary) propositional formula over variables X and Y with $X \cap Y = \emptyset$

X *relevant* input variables
Y *irrelevant* input variables

We are interested in the number of models projected onto X:

$$\#\exists Y.F(X, Y)$$

Example $F(X, Y) = x \vee y$

$X = \{x\}$ $Y = \{y\}$ $\mathcal{M}(\exists Y.F(X, Y)) = \{x, \neg x\}$ $\#\exists Y.F(X, Y) = 2$
$X = \{x, y\}$ $Y = \emptyset$ $\mathcal{M}(\exists Y.F(X, Y)) = \{xy, x\neg y, \neg xy\}$ $\#\exists Y.F(X, Y) = 3 = \#F(X, Y)$

Our Dual Approach Facilitates the Detection of Partial Models

```
$ cat clause.form
p | q | r | s
$ dualiza -e -r p,r,s clause.form
ALL SATISFYING ASSIGNMENTS
s
r !s
!r !s
$ dualiza -r p,r,s clause.form
NUMBER SATISFYING ASSIGNMENTS
8
```

```
$ dualiza -r p,r,s clause.form -l | grep RULE
c LOG 1 RULE UNX 1 -4
c LOG 1 RULE UNX 2 -4
c LOG 1 RULE BNOF 1 -4
c LOG 2 RULE UNX 3 -3
c LOG 2 RULE BNOF 2 -3
c LOG 3 RULE UNY 1 -2
c LOG 3 RULE ENO 1
```

Dual Representation of $F(X, Y)$

$$P(X, Y) \qquad\qquad N(X, Y)$$

$$\equiv \qquad\qquad \equiv$$

$$F(X, Y) \qquad\qquad \neg F(X, Y)$$

Dual Representation of $F(X, Y)$

$\exists S. P(X, Y, S)$	$\exists T. N(X, Y, T)$
$\equiv$	$\equiv$
$F(X, Y)$	$\neg F(X, Y)$

The General Case — Duality with Projection onto Relevant Input Variables

$\exists Y, S. P(X, Y, S)$

$\equiv$

$\exists Y. F(X, Y)$

$\exists Y, T. N(X, Y, T)$

$\equiv$

$\exists Y. \neg F(X, Y)$

A First Example

$$F(X, Y) = (p \vee q \vee r \vee s) \qquad X = \{p, r, s\} \qquad Y = \{q\}$$

$$P(X, Y, S) = (p \vee q \vee r \vee s) \qquad S = \emptyset$$

$$N(X, Y, T) = (\neg p) \wedge (\neg q) \wedge (\neg r) \wedge (\neg s) \qquad T = \emptyset$$

A First Example

$F(X, Y) = (p \vee q \vee r \vee s)$ $\quad X = \{p, r, s\}$ $\quad Y = \{q\}$

$P(X, Y, S) = (p \vee q \vee r \vee s)$ $\quad S = \emptyset$

$N(X, Y, T) = (\neg p) \wedge (\neg q) \wedge (\neg r) \wedge (\neg s)$ $\quad T = \emptyset$

Step	Rule	I	$P\|_I$	$N\|_I$	M	Found
0		$()$	$(p \vee q \vee r \vee s)$	$(\neg p) \wedge (\neg q) \wedge (\neg r) \wedge (\neg s)$	0	
1	UNXY	s	$\emptyset$	$(\neg p) \wedge (\neg q) \wedge (\neg r) \wedge ()$	0	
2	BN0F	$\neg s$	$(p \vee q \vee r)$	$(\neg p) \wedge (\neg q) \wedge (\neg r)$	4	s
3	UNXY	$\neg s r$	$\emptyset$	$(\neg p) \wedge (\neg q) \wedge ()$	4	
4	BN0F	$\neg s \neg r$	$(p \vee q)$	$(\neg p) \wedge (\neg q)$	6	$\neg s r$
5	UNXY	$\neg s \neg r q$	$\emptyset$	$(\neg p) \wedge ()$	6	
6	EN0	$\neg s \neg r q$	$\emptyset$	$(\neg p) \wedge ()$	8	$\neg s \neg r$

Can We Compete with State-of-the-Art #SAT Solvers?

```
$ cat clause_n.form
(x1 | x2 | ... | xn)
```

Can We Compete with State-of-the-Art #SAT Solvers?

```
$ cat clause_n.form
(x1 | x2 | ... | xn)
```

n	Mode	sharpSAT [s]	Dualiza [s]
10	dual	$< 1 \cdot 10^{-2}$	$< 1 \cdot 10^{-2}$
	block	$< 1 \cdot 10^{-2}$	$2 \cdot 10^{-2}$
	flip	$< 1 \cdot 10^{-2}$	$< 1 \cdot 10^{-2}$
20	block	$1 \cdot 10^{-2}$	$9 \cdot 10^{-1}$
	flip	$1 \cdot 10^{-2}$	$2 \cdot 10^{-1}$
30	block	$1 \cdot 10^{-2}$	$4 \cdot 10^{4}$
	flip	$1 \cdot 10^{-2}$	$2 \cdot 10^{2}$
100	dual	$< 1 \cdot 10^{-2}$	$< 1 \cdot 10^{-2}$
1000	dual	$8 \cdot 10^{-2}$	$2 \cdot 10^{-2}$
10000	dual	$1 \cdot 10^{1}$	$2 \cdot 10^{-1}$

Where Our Dual Approach Really Wins

```
$ cat nrp4.form
(x1 | x2 | x3 | x4) |
(x5 = x2 ^ x3 ^ x4) |
(x6 = x1 ^ x3 ^ x4) |
(x7 = x1 ^ x2 ^ x4) |
(x8 = x1 ^ x2 ^ x3)
```

Where Our Dual Approach Really Wins

```
$ cat nrp4.form
(x1 | x2 | x3 | x4) |
(x5 = x2 ^ x3 ^ x4) |
(x6 = x1 ^ x3 ^ x4) |
(x7 = x1 ^ x2 ^ x4) |
(x8 = x1 ^ x2 ^ x3)
```

n	Method	sharpSAT [s]	DUALIZA [s]
10	dual	$9 \cdot 10^{-2}$	$< 1 \cdot 10^{-2}$
20	dual	$7 \cdot 10^{2}$	$1 \cdot 10^{-2}$
21	dual	$2 \cdot 10^{3}$	$1 \cdot 10^{-2}$
22	dual	*	$1 \cdot 10^{-2}$
100	dual	*	$8 \cdot 10^{-2}$
1000	dual	*	$1 \cdot 10^{1}$
5000	dual	*	$2 \cdot 10^{2}$

Calculus

EP0: $(P, N, I, M) \rightsquigarrow_{\text{EP0}} M$ if $\emptyset \in P|_I$ and $\text{decs}(I) = \emptyset$

EP1: $(P, N, I, M) \rightsquigarrow_{\text{EP1}} M + 2^{|X-I|}$ if $P|_I = \emptyset$ and $V(\text{decs}(I)) \cap X = \emptyset$

EN0: $(P, N, I, M) \rightsquigarrow_{\text{EN0}} M + 2^{|X-I|}$ if $\emptyset \in N|_I$ and $V(\text{decs}(I)) \cap X = \emptyset$

BP0F: $(P, N, I\ell^d I', M) \rightsquigarrow_{\text{BP0F}} (P, N, I\bar{\ell}^{f(m')}, M)$ if $\emptyset \in P|_{I\ell I'}$ and $V(\text{decs}(I')) = \emptyset$ and $m' = \sum \{m \mid \ell^{f(m)} \in I'\}$

JP0: $(P, N, II', M) \rightsquigarrow_{\text{JP0}} (P \wedge C^r, N, I\ell', M - m')$ if $\emptyset \in P|_{II'}$ and $P \models C$ and $C|_I = \{\ \ell'\ \}$ and $m' = \sum \{m \mid \ell^{f(m)} \in I'\}$

BP1F: $(P, N, I\ell^d I', M) \rightsquigarrow_{\text{BP1F}} (P, N, I\bar{\ell}^{f(m'+m'')}, M + m'')$ if $P|_{I\ell I'} = \emptyset$ and $V(\ell) \in X$ and $V(\text{decs}(I')) \cap X = \emptyset$ and $m' = \sum \{m \mid \ell^{f(m)} \in I'\}$ and $m'' = 2^{|X-I\ell I'|}$

BP1L: $(P, N, I\ell^d I', M) \rightsquigarrow_{\text{BP1L}} (P \wedge D, N, I\bar{\ell}, M + m'')$ if $P|_{I\ell I'} = \emptyset$ and $V(\ell) \in X$ and $V(\text{decs}(I')) \cap X = \emptyset$ and $m'' = 2^{|X-I\ell I'|}$ and $D = \pi(\neg\text{decs}(I\ell), X)$

Calculus

BN0F: $(P, N, I\ell^d I', M) \leadsto_{\text{BN0F}} (P, N, I\bar{\ell}^{f(m'+m'')}, M + m'')$ if $\emptyset \in N|_{I\ell I'}$ and $V(\ell) \in X$ and $V(\text{decs}(I')) \cap X = \emptyset$ and $m' = \sum \{m \mid \ell^{f(m)} \in I'\}$ and $m'' = 2^{|X - I\ell I'|}$

BN0L: $(P, N, I\ell^d I', M) \leadsto_{\text{BN0L}} (P \wedge D, N, I\bar{\ell}, M + m'')$ if $\emptyset \in N|_{I\ell I'}$ and $V(\ell) \in X$ and $V(\text{decs}(I')) \cap X = \emptyset$ and $m'' = 2^{|X - I\ell I'|}$ and $D = \pi(\neg\text{decs}(I\ell), X)$

DX: $(P, N, I, M) \leadsto_{\text{DX}} (P, N, I\ell^d, M)$ if $\emptyset \notin (P \wedge N)|_I$ and $\text{units}((P \wedge N)|_I) = \emptyset$ and $V(\ell) \in X - I$

DYS: $(P, N, I, M) \leadsto_{\text{DYS}} (P, N, I\ell^d, M)$ if $\emptyset \notin (P \wedge N)|_I$ and $\text{units}((P \wedge N)|_I) = \emptyset$ and $V(\ell) \in (Y \cup S) - I$ and $X - I = \emptyset$

UP: $(P, N, I, M) \leadsto_{\text{UP}} (P, N, I\ell, M)$ if $\{\ell\} \in P|_I$

UNXY: $(P, N, I, M) \leadsto_{\text{UNXY}} (P, N, I\bar{\ell}^d, M)$ if $\{\ell\} \in N|_I$ and $V(\ell) \in X \cup Y$ and $\emptyset \notin P|_I$ and $\text{units}(P|_I) = \emptyset$

UNT: $(P, N, I, M) \leadsto_{\text{UNT}} (P, N, I\ell, M)$ if $\{\ell\} \in N|_I$ and $V(\ell) \in T$ and $\emptyset \notin P|_I$ and $\text{units}(P|_I) = \emptyset$

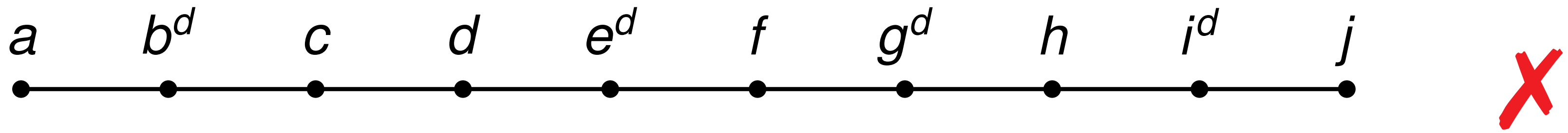
FP: $(P \wedge C^r, N, I, M) \leadsto_{\text{FP}} (P, N, I, M)$ if $\emptyset \notin P|_I$

Our Contribution — the First Dual Calculus for Exact Projected Model Counting

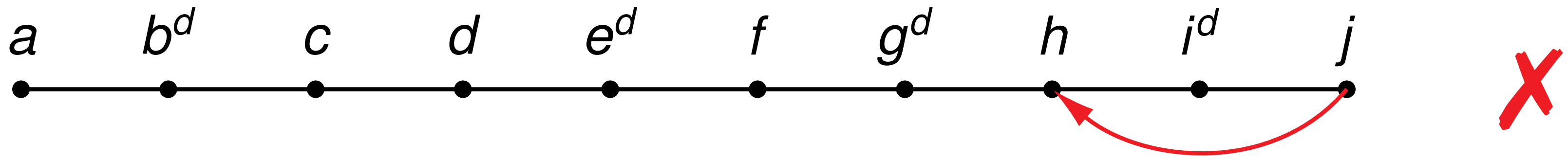
- dual representation of the formula enabling the detection of partial models and subsequent pruning of the search space
- good learning mechanism exempt from satisfiability checks and clause watching mechanisms
- significant performance gain compared to non-dual variant
- accepts arbitrary formulae and circuits as argument
- novel techniques for preventing multiple model counts: *flipping* and *discounting*
- models state-of-the-art techniques: conflict analysis and conflict-driven backjumping
- robust and carefully tested implementation: DUALIZA
  - competitive on some CNF formulae
  - outperforms state-of-the-art #SAT solvers on another class of formulae

Challenges in Exact Propositional Model Counting (#SAT) (2)

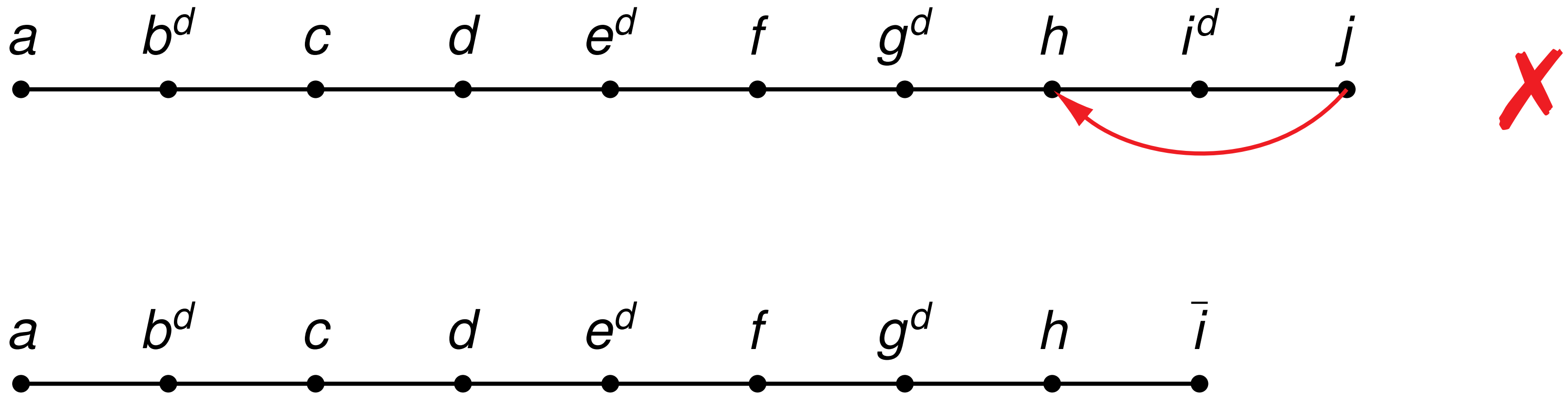
Chronological Backtracking Without Conflict-Driven Clause Learning (CDCL)



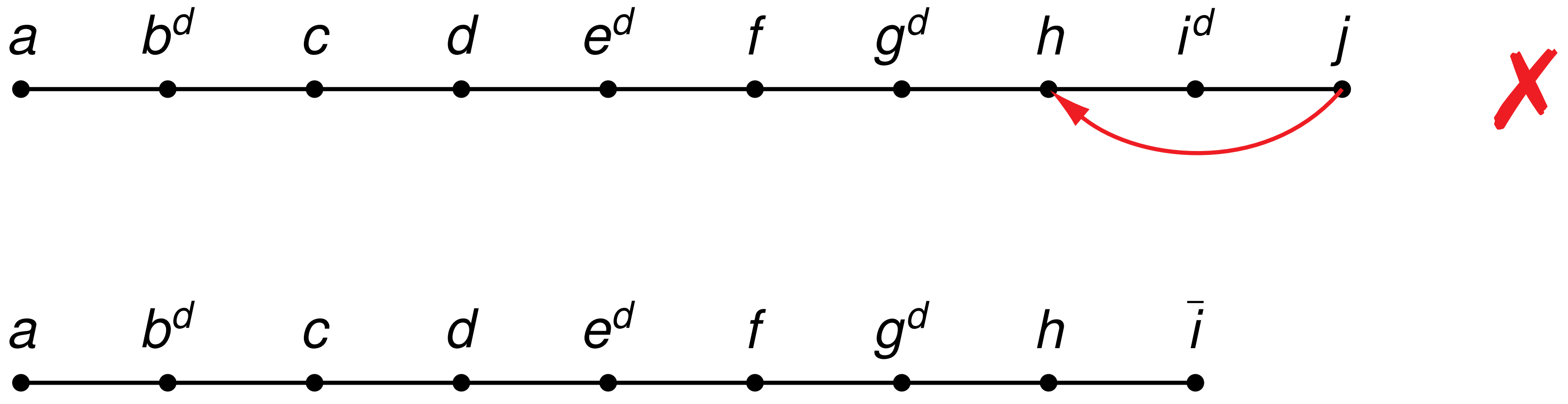
Chronological Backtracking Without Conflict-Driven Clause Learning (CDCL)



Chronological Backtracking Without Conflict-Driven Clause Learning (CDCL)



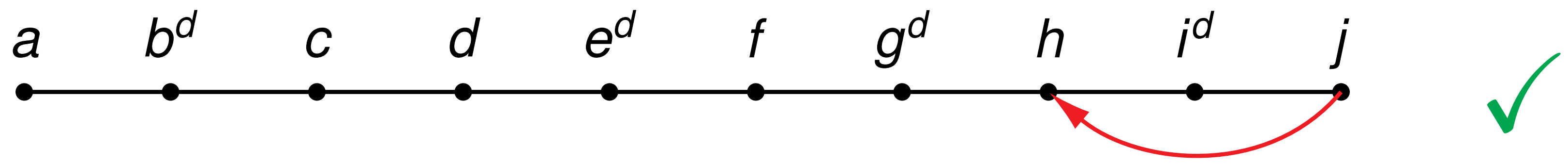
Chronological Backtracking Without Conflict-Driven Clause Learning (CDCL)



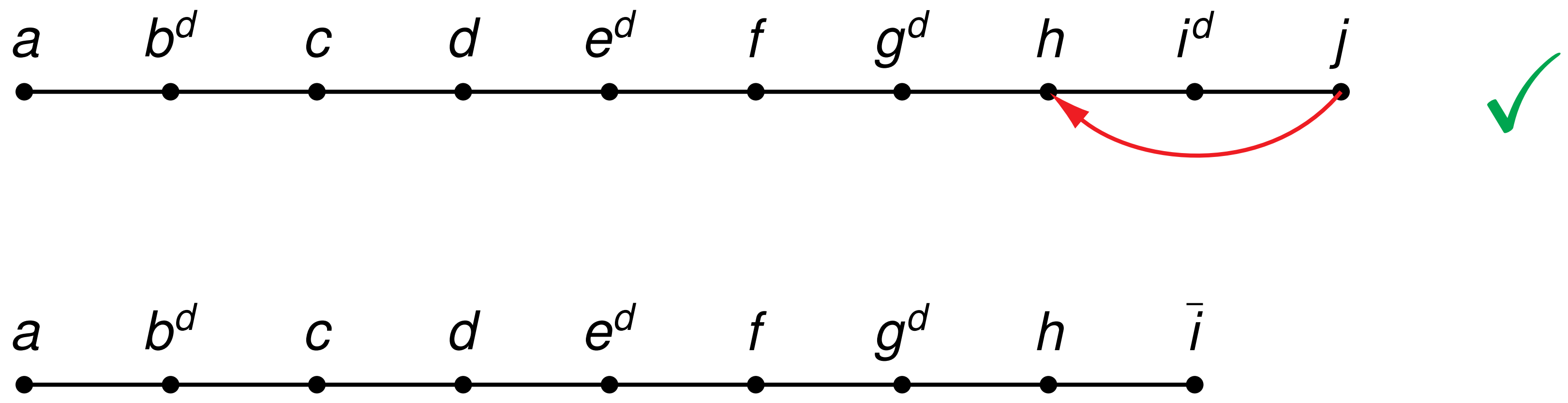
Suitability for #SAT

+ Search space is traversed in an ordered manner
+ The correct model count is returned
– Regions of the search space with no solution can not be escaped easily
– Inefficient in terms of execution time

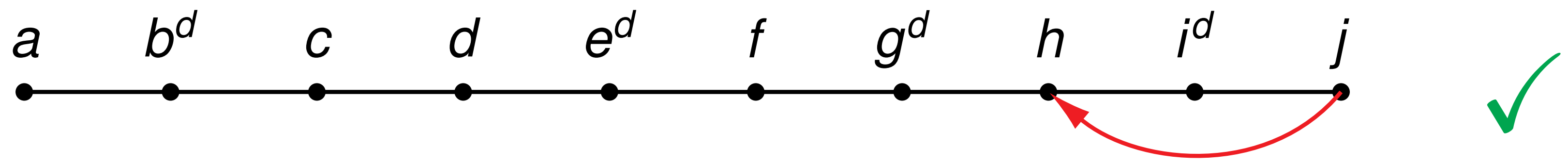
Non-Chronological Backtracking with Conflict-Driven Clause Learning (CDCL)

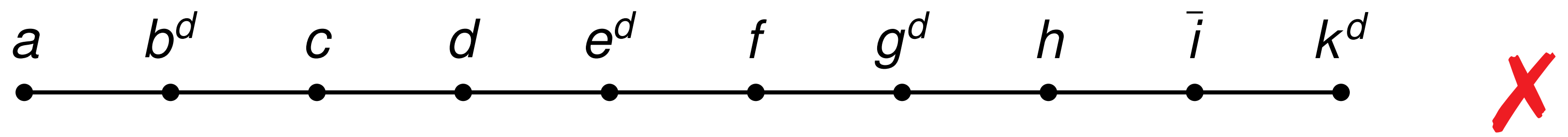


Non-Chronological Backtracking with Conflict-Driven Clause Learning (CDCL)

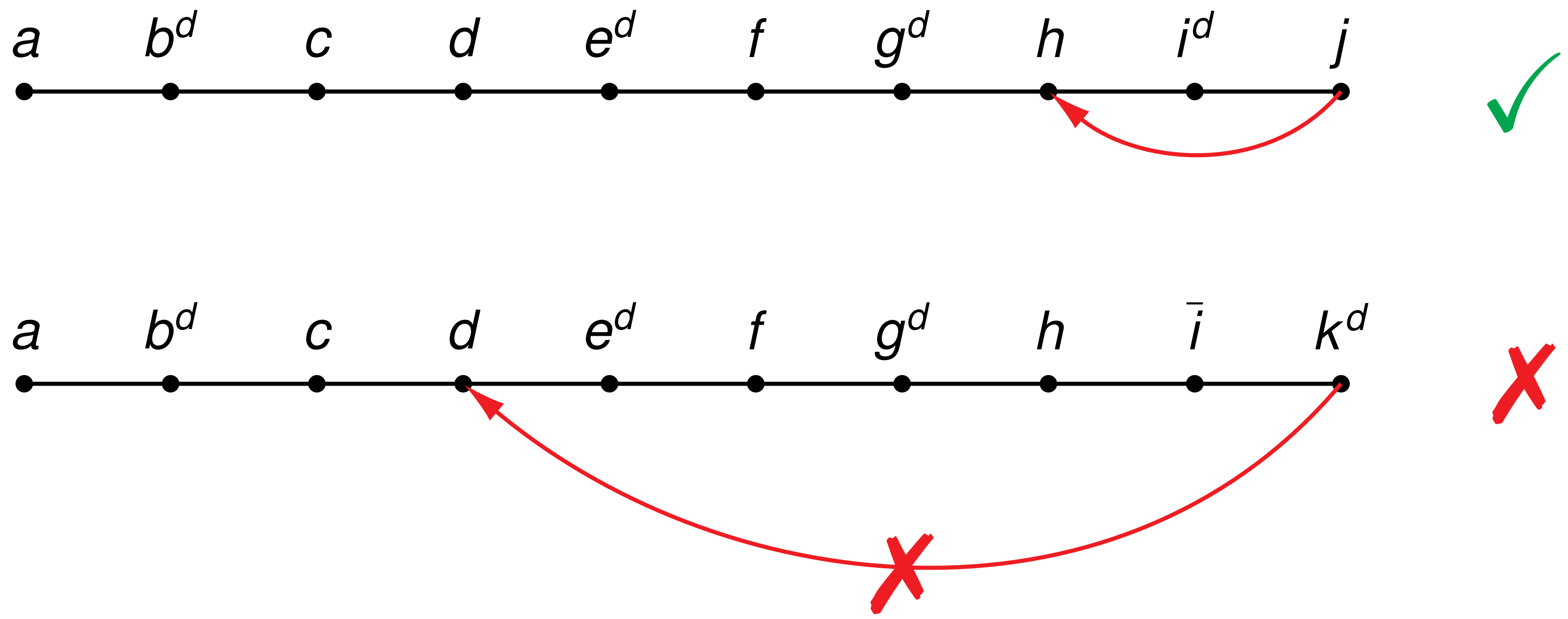


Non-Chronological Backtracking with Conflict-Driven Clause Learning (CDCL)

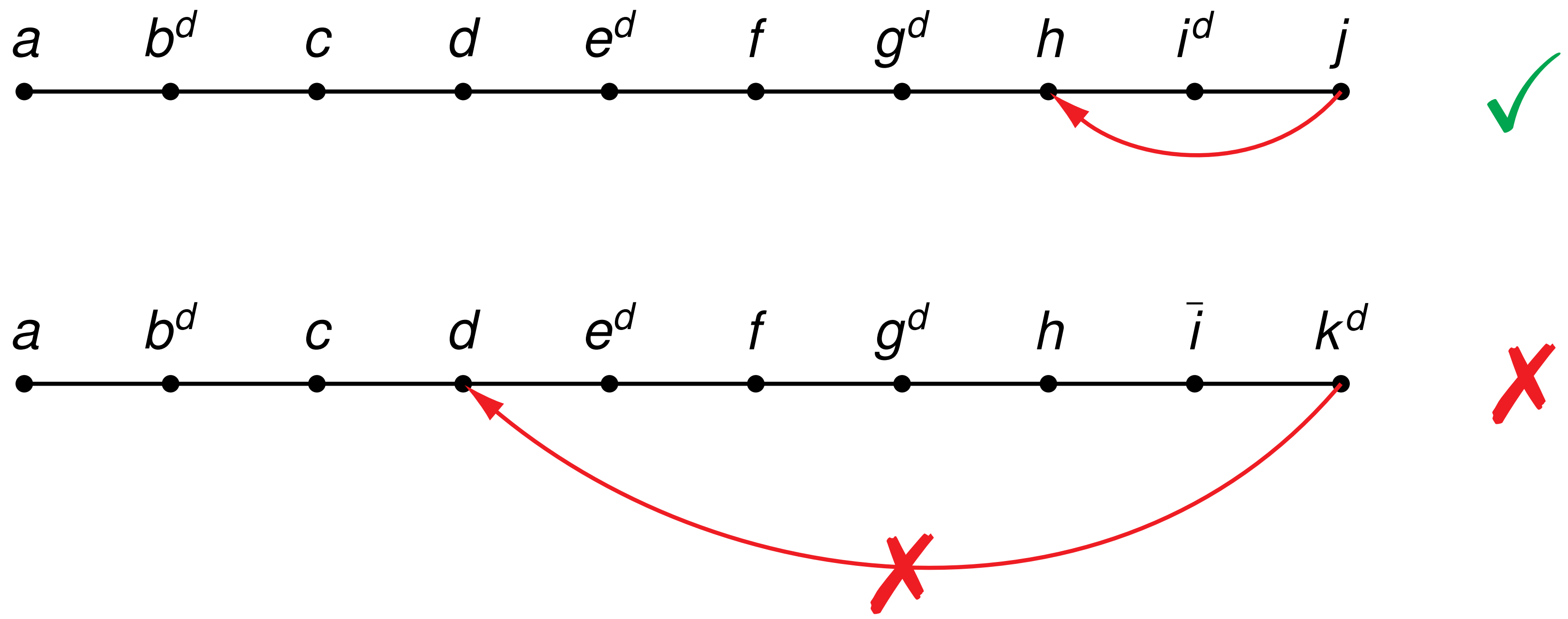




Non-Chronological Backtracking with Conflict-Driven Clause Learning (CDCL)



Non-Chronological Backtracking with Conflict-Driven Clause Learning (CDCL)



Suitability for #SAT

- \+ Enables the solver to escape regions of the search space with no solution
- \+ Gain in performance (for SAT)
- – Might result in a wrong model count
- – Might lead to redundant work

Chronological Backtracking with Conflict-Driven Clause Learning (CDCL)

Suitability for #SAT

+ Enables the solver to escape regions of the search space with no solution
+ Returns the correct model count
+ Avoids (at least some) redundant work
+ Does not significantly degrade solver performance for SAT

Backing Backtracking (SAT'19)

CDCL Invariants

Trail:	The assignment trail contains neither complementary pairs of literals nor duplicates.
ConflictLower:	The assignment trail preceding the current decision level does not falsify the formula.
Propagation:	On every decision level preceding the current decision level all unit clauses are propagated until completion.
LevelOrder:	The literals are ordered on the assignment trail in ascending order with respect to their decision level.
ConflictingClause:	At decision levels greater than zero the conflicting clause contains at least two literals with the current decision level.

CDCL Invariants

Trail:	The assignment trail contains neither complementary pairs of literals nor duplicates.
ConflictLower:	The assignment trail preceding the current decision level does not falsify the formula.
Propagation:	On every decision level preceding the current decision level all unit clauses are propagated until completion.
LevelOrder:	The literals are ordered on the assignment trail in ascending order with respect to their decision level.
ConflictingClause:	At decision levels greater than zero the conflicting clause contains at least two literals with the current decision level.

Combining CDCL with Chronological Backtracking

τ	$\cdots$	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
I	$\cdots$	4	5	30	47	15	18	6	-7	-8	45	9	38	-23	17	44	-16
δ	$\cdots$	3	4	4	4	4	4	5	5	5	5	6	6	6	6	6	6

Combining CDCL with Chronological Backtracking

τ	$\cdots$	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
I	$\cdots$	4	**5**	30	47	15	18	**6**	-7	-8	45	**9**	38	-23	17	44	-16
δ	$\cdots$	3	4	4	4	4	4	5	5	5	5	6	6	6	6	6	6

decision literal

Combining CDCL with Chronological Backtracking

τ	$\cdots$	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
I	$\cdots$	4	**5**	**30**	**47**	**15**	**18**	6	-7	-8	45	9	38	-23	17	44	-16
δ	$\cdots$	3	4	4	4	4	4	5	5	5	5	6	6	6	6	6	6

$\text{block}(I, 4)$

Combining CDCL with Chronological Backtracking

τ	$\cdots$	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
I	$\cdots$	4	**5**	**30**	**47**	**15**	**18**	6	-7	-8	45	9	38	-23	17	44	-16
δ	$\cdots$	3	4	4	4	4	4	5	5	5	5	6	6	6	6	6	6

slice(I, 4)

Combining CDCL with Chronological Backtracking

τ	$\cdots$	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
I	$\cdots$	**4**	**5**	**30**	**47**	**15**	**18**	6	-7	-8	45	9	38	-23	17	44	-16
δ	$\cdots$	3	4	4	4	4	4	5	5	5	5	6	6	6	6	6	6

$I_{\leqslant 4}$

Combining CDCL with Chronological Backtracking

τ	$\cdots$	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
I	$\cdots$	4	5	30	47	15	18	6	-7	-8	45	9	38	-23	17	44	-16
δ	$\cdots$	3	4	4	4	4	4	5	5	5	5	6	6	6	6	6	6

✗

Combining CDCL with Chronological Backtracking

τ	$\cdots$	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
I	$\cdots$	4	5	30	47	15	18	6	-7	-8	45	9	38	-23	17	44	-16
δ	$\cdots$	3	4	4	4	4	4	5	5	5	5	6	6	6	6	6	6

conflicting $\{$ -47, -17, -44 $\}$

conflict level 6

Combining CDCL with Chronological Backtracking

τ	$\cdots$	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
I	$\cdots$	4	5	30	47	15	18	6	-7	-8	45	9	38	-23	17	44	-16
δ	$\cdots$	3	4	4	4	4	4	5	5	5	5	6	6	6	6	6	6

✗

conflicting		{			-47,										-17,	-44	}
learned		{		-30,	-47,		-18,							23			}

jump level 4

Combining CDCL with Chronological Backtracking

τ	$\cdots$	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
I	$\cdots$	4	5	30	47	15	18	6	-7	-8	45	9	38	-23	17	44	-16
δ	$\cdots$	3	4	4	4	4	4	5	5	5	5	6	6	6	6	6	6
conflicting		{			-47,										-17,	-44	}
learned		{		-30,	-47,		-18,							23			}

backtrack level 5

Combining CDCL with Chronological Backtracking

τ	$\cdots$	4	5	6	7	8	9	10	11	12	13
I	$\cdots$	4	5	30	47	15	18	6	-7	-8	45
δ	$\cdots$	3	4	4	4	4	4	5	5	5	5

Combining CDCL with Chronological Backtracking

τ	$\cdots$	4	5	6	7	8	9	10	11	12	13
I	$\cdots$	4	5	30	47	15	18	6	-7	-8	45
δ	$\cdots$	3	4	4	4	4	4	5	5	5	5

τ	$\cdots$	4	5	6	7	8	9	10	11	12	13	14
I	$\cdots$	4	5	30	47	15	18	6	-7	-8	45	**23**
δ	$\cdots$	3	4	4	4	4	4	5	5	5	5	**4**

out of order

Combining CDCL with Chronological Backtracking

τ	$\cdots$	4	5	6	7	8	9	10	11	12	13
I	$\cdots$	4	5	30	47	15	18	6	-7	-8	45
δ	$\cdots$	3	4	4	4	4	4	5	5	5	5

τ	$\cdots$	4	5	6	7	8	9	10	11	12	13	14
I	$\cdots$	4	**5**	**30**	**47**	**15**	**18**	6	-7	-8	45	23
δ	$\cdots$	3	4	4	4	4	4	5	5	5	5	4

block$(I, 4)$

Combining CDCL with Chronological Backtracking

τ	$\cdots$	4	5	6	7	8	9	10	11	12	13
I	$\cdots$	4	5	30	47	15	18	6	-7	-8	45
δ	$\cdots$	3	4	4	4	4	4	5	5	5	5

τ	$\cdots$	4	5	6	7	8	9	10	11	12	13	14
I	$\cdots$	4	**5**	**30**	**47**	**15**	**18**	6	-7	-8	45	**23**
δ	$\cdots$	3	4	4	4	4	4	5	5	5	5	4

slice(I, 4)

Combining CDCL with Chronological Backtracking

τ	$\cdots$	4	5	6	7	8	9	10	11	12	13
I	$\cdots$	4	5	30	47	15	18	6	-7	-8	45
δ	$\cdots$	3	4	4	4	4	4	5	5	5	5

τ	$\cdots$	4	5	6	7	8	9	10	11	12	13	14
I	$\cdots$	**4**	**5**	**30**	**47**	**15**	**18**	6	-7	-8	45	**23**
δ	$\cdots$	3	4	4	4	4	4	5	5	5	5	4

$I_{\leqslant 4}$

Combining CDCL with Chronological Backtracking

τ	$\cdots$	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
I	$\cdots$	18	6	-7	-8	45	23	-38	-9	10	-11	13	16	-17	-25	42	12	-41
δ	$\cdots$	4	5	5	5	5	4	4	5	6	7	5	4	4	4	4	5	5

Combining CDCL with Chronological Backtracking

τ	$\cdots$	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
I	$\cdots$	18	6	-7	-8	45	23	-38	-9	10	-11	13	16	-17	-25	42	12	-41
δ	$\cdots$	4	5	5	5	5	4	4	5	6	7	5	4	4	4	4	5	5
																		✗

conflicting $\{$ 17, -42, -12 $\}$

Combining CDCL with Chronological Backtracking

τ	$\cdots$	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
I	$\cdots$	18	6	-7	-8	45	23	-38	-9	10	-11	13	16	-17	-25	42	12	-41
δ	$\cdots$	4	5	5	5	5	4	4	5	6	7	5	4	4	4	4	5	5

conflicting $\{$ 17, -42, -12 $\}$

backtrack level 4

Combining CDCL with Chronological Backtracking

τ	$\cdots$	4	5	6	7	8	9	10	11
I	$\cdots$	18	23	-38	16	-17	-25	42	-12
δ	$\cdots$	4	4	4	4	4	4	4	4

Calculus

True: $(F,\ I,\ \delta) \rightsquigarrow_{\text{True}}$ SAT if $F|_I = \top$

False: $(F,\ I,\ \delta) \rightsquigarrow_{\text{False}}$ UNSAT if exists $C \in F$ with $C|_I = \bot$ and $\delta(C) = 0$

Unit: $(F,\ I,\ \delta) \rightsquigarrow_{\text{Unit}} (F,\ I\ell,\ \delta[\ell \mapsto a])$ if $F|_I \neq \top$ and $\bot \notin F|_I$ and exists $C \in F$ with $\{\ell\} = C|_I$ and $a = \delta(C \setminus \{\ell\})$

Jump: $(F,\ I,\ \delta) \rightsquigarrow_{\text{Jump}} (F \wedge D,\ PK\ell,\ \delta[L \mapsto \infty][\ell \mapsto j])$ if exists $C \in F$ with $PQ = I$ and $C|_I = \bot$ such that $c = \delta(C) = \delta(D) > 0$ and $\ell \in D$ and $\ell|_Q = \bot$ and $F \models D$ and $j = \delta(D \setminus \{\ell\})$ and $b = \delta(P)$ and $j \leqslant b < c$ and $K = Q_{\leqslant b}$ and $L = Q_{>b}$

Decide: $(F,\ I,\ \delta) \rightsquigarrow_{\text{Decide}} (F,\ I\ell,\ \delta[\ell \mapsto d])$ if $F|_I \neq \top$ and $\bot \notin F|_I$ and $\text{units}(F|_I) = \emptyset$ and $V(\ell) \in V$ and $\delta(\ell) = \infty$ and $d = \delta(I) + 1$

Calculus

True: $(F,\ I,\ \delta) \rightsquigarrow_{\text{True}}$ SAT if $F|_I = \top$

False: $(F,\ I,\ \delta) \rightsquigarrow_{\text{False}}$ UNSAT if exists $C \in F$ with $C|_I = \bot$ and $\delta(C) = 0$

Unit: $(F,\ I,\ \delta) \rightsquigarrow_{\text{Unit}} (F,\ I\ell,\ \delta[\ell \mapsto a])$ if $F|_I \neq \top$ and $\bot \notin F|_I$ and exists $C \in F$ with $\{\ell\} = C|_I$ and $a = \delta(C \setminus \{\ell\})$

Jump: $(F,\ I,\ \delta) \rightsquigarrow_{\text{Jump}} (F \wedge D,\ PK\ell,\ \delta[L \mapsto \infty][\ell \mapsto j])$ if exists $C \in F$ with $PQ = I$ and $C|_I = \bot$ such that $c = \delta(C) = \delta(D) > 0$ and $\ell \in D$ and $\ell|_Q = \bot$ and $F \models D$ and $j = \delta(D \setminus \{\ell\})$ and $b = \delta(P)$ and $b = c - 1$ and $K = Q_{\leqslant b}$ and $L = Q_{>b}$

Decide: $(F,\ I,\ \delta) \rightsquigarrow_{\text{Decide}} (F,\ I\ell,\ \delta[\ell \mapsto d])$ if $F|_I \neq \top$ and $\bot \notin F|_I$ and $\text{units}(F|_I) = \emptyset$ and $V(\ell) \in V$ and $\delta(\ell) = \infty$ and $d = \delta(I) + 1$

Calculus

True: $(F,\ I,\ \delta) \rightsquigarrow_{\text{True}}$ SAT if $F|_I = \top$

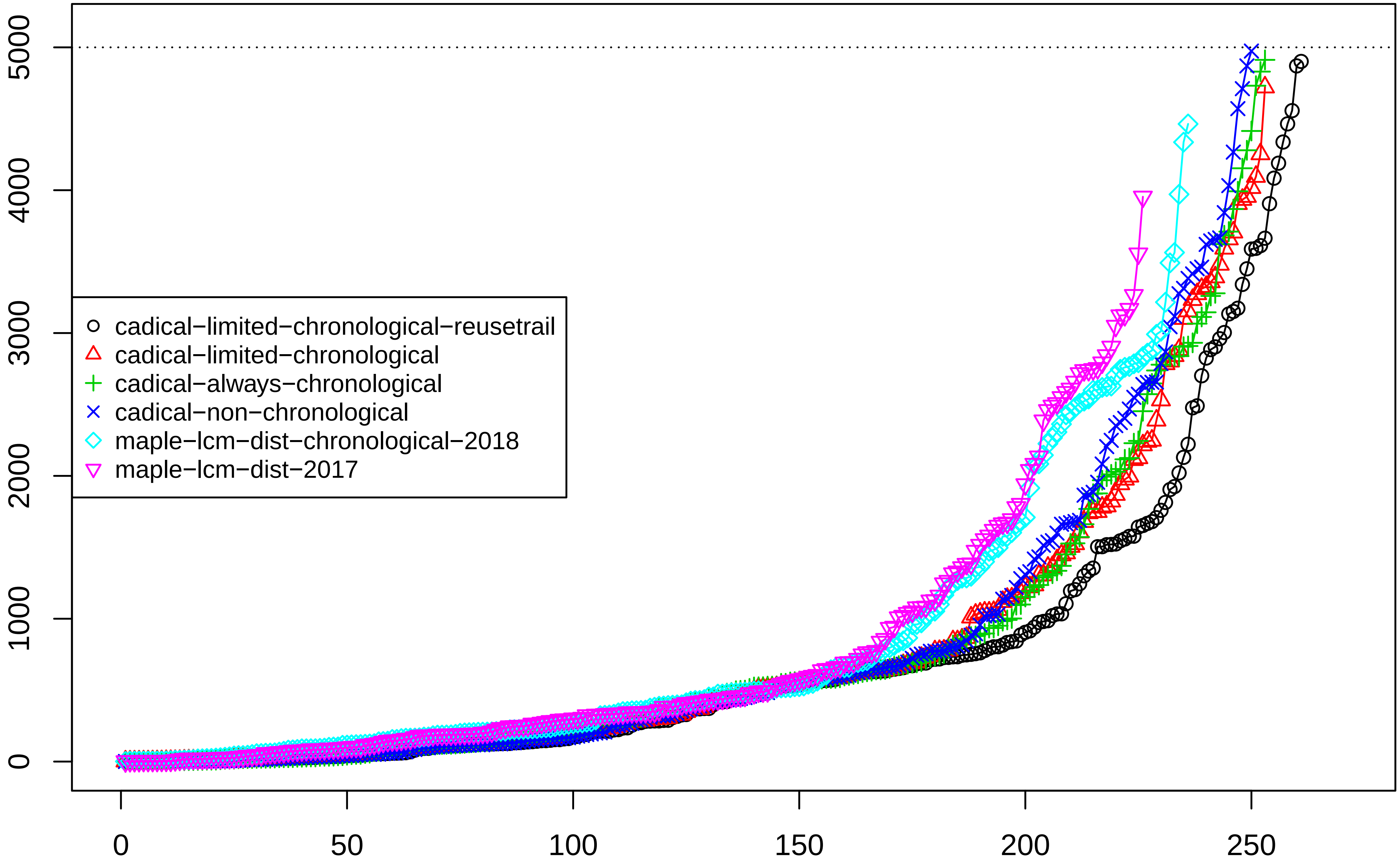
False: $(F,\ I,\ \delta) \rightsquigarrow_{\text{False}}$ UNSAT if exists $C \in F$ with $C|_I = \bot$ and $\delta(C) = 0$

Unit: $(F,\ I,\ \delta) \rightsquigarrow_{\text{Unit}} (F,\ I\ell,\ \delta[\ell \mapsto a])$ if $F|_I \neq \top$ and $\bot \notin F|_I$ and exists $C \in F$ with $\{\ell\} = C|_I$ and $a = \delta(C \setminus \{\ell\})$

Jump: $(F,\ I,\ \delta) \rightsquigarrow_{\text{Jump}} (F \wedge D,\ PK\ell,\ \delta[L \mapsto \infty][\ell \mapsto j])$ if exists $C \in F$ with $PQ = I$ and $C|_I = \bot$ such that $c = \delta(C) = \delta(D) > 0$ and $\ell \in D$ and $\ell|_Q = \bot$ and $F \models D$ and $j = \delta(D \setminus \{\ell\})$ and $b = \delta(P)$ and $b = j$ and $K = Q_{\leqslant b}$ and $L = Q_{>b}$

Decide: $(F,\ I,\ \delta) \rightsquigarrow_{\text{Decide}} (F,\ I\ell,\ \delta[\ell \mapsto d])$ if $F|_I \neq \top$ and $\bot \notin F|_I$ and $\text{units}(F|_I) = \emptyset$ and $V(\ell) \in V$ and $\delta(\ell) = \infty$ and $d = \delta(I) + 1$

Experiments — Main Track of SAT Competition 2018



Experiments

solver configurations	solved instances		
	total	SAT	UNSAT
cadical-limited-chronological-reusetrail	261	155	106
cadical-limited-chronological	253	147	106
cadical-always-chronological	253	148	105
cadical-non-chronological	250	144	106
maple-lcm-dist-chronological-2018	236	134	102
maple-lcm-dist-2017	226	126	100

Combining Conflict-Driven Clause Learning and Chronological Backtracking for Propositional Model Counting (GCAI’19)

The Main Idea

$F = (\overline{p} \vee q) \wedge (p \vee q)$ → Rules → $M = (r \wedge q) \vee (\overline{r} \wedge p \wedge q) \vee (\overline{r} \wedge \overline{p} \wedge q) = C_1 \vee C_2 \vee C_3$

$V = \{p, q, r\}$

$M \equiv F$ and $\#M = \sum_{i=1}^{3} 2^{|V - C_i|} = 4 = \#F$

Generalizing, $\boxed{\#F = \sum_{C \in M} 2^{|V-C|}}$ and

M is a Disjoint-Sum-of-Products (DSOP) representation of F

- M is a disjunction of conjunctions of literals (cubes)
- The cubes in M are pairwise contradicting
- M is logically equivalent to F
- M is not unique

The Main Idea

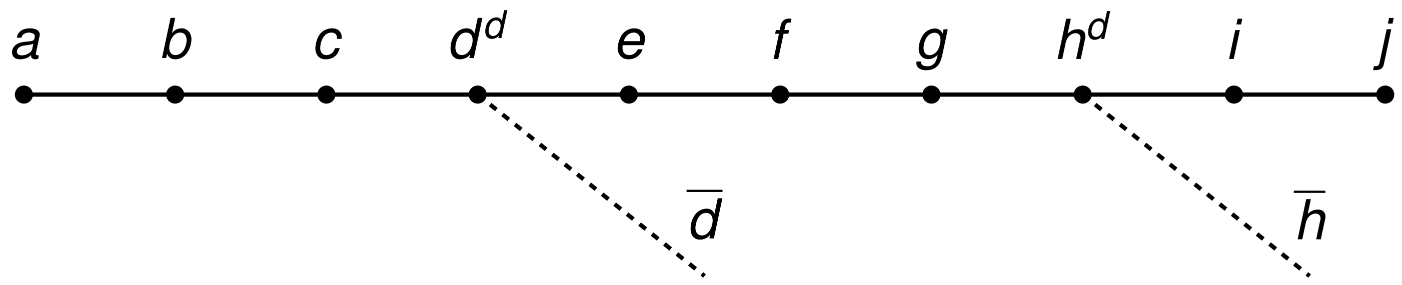
Assignment Trail I

$I = abcd^d efgh^d ij$

Pending Search Space $O(I)$

$O(I) = abc\overline{d} \vee abcdefg\overline{h} \vee I$

$O(I)$ is a DSOP



Pending Models of F $F \wedge O(I)$

Models of F found M

The Main Idea

During execution, we have that

$$O(I) \wedge F \vee M \equiv F \quad \text{and} \quad \#F = \#(F \wedge O(I)) + \sum_{C \in M} 2^{|V-C|}$$

Upon termination, we have $O(I) = \bot$, hence

$$M \equiv F \quad \text{and} \quad \#F = \sum_{C \in M} 2^{|V-C|}$$

Example

$$F = (\overline{p} \vee q) \wedge (p \vee q) \qquad V = \{p, q, r\}$$

Step	Rule	I	$F\|_I$	M
0		ε	$(\overline{p} \vee q) \wedge (p \vee q)$	$\perp$
1	Decide	r^d	$(\overline{p} \vee q) \wedge (p \vee q)$	$\perp$
2	Decide	$r^d q^d$	$\top$	$\perp$
3	BackTrue	$r^d \overline{q}$	$(\overline{p}) \wedge (p)$	rq
4	Unit	$r^d \overline{q}\overline{p}$	$\perp$	rq
5	BackFalse	$\overline{r}$	$(\overline{p} \vee q) \wedge (p \vee q)$	rq
6	Decide	$\overline{r} p^d$	(q)	rq
7	Unit	$\overline{r} p^d q$	$\top$	rq
8	BackTrue	$\overline{r}\overline{p}$	(q)	$rq \vee \overline{r}pq$
9	Unit	$\overline{r}\overline{p}q$	$\top$	$rq \vee \overline{r}pq$
10	EndTrue			$rq \vee \overline{r}pq \vee \overline{r}\overline{p}q$

Calculus

EndTrue: $(F, I, M, \delta) \rightsquigarrow_{\text{EndTrue}} M \vee I$ if $F|_I = \top$ and $\text{decs}(I) = \emptyset$

EndFalse: $(F, I, M, \delta) \rightsquigarrow_{\text{EndFalse}} M$ if exists $C \in F$ and $C|_I = \bot$ and $\delta(C) = 0$

Unit: $(F, I, M, \delta) \rightsquigarrow_{\text{Unit}} (F, I\ell, M, \delta[\ell \mapsto a])$ if $F|_I \neq \top$ and $\bot \notin F|_I$ and exists $C \in F$ with $\{\ell\} = C|_I$ and $a = \delta(C \setminus \{\ell\})$

BackTrue: $(F, I, M, \delta) \rightsquigarrow_{\text{BackTrue}} (F, PK\ell, M \vee I, \delta[L \mapsto \infty][\ell \mapsto e])$ if $F|_I = \top$ and $PQ = I$ and $D = \overline{\text{decs}(I)}$ and $e + 1 = \delta(D) = \delta(I)$ and $\ell \in D$ and $e = \delta(D \setminus \{\ell\}) = \delta(P)$ and $K = Q_{\leqslant e}$ and $L = Q_{>e}$

BackFalse: $(F, I, M, \delta) \rightsquigarrow_{\text{BackFalse}} (F, PK\ell, M, \delta[L \mapsto \infty][\ell \mapsto j])$ if exists $C \in F$ and exists D with $PQ = I$ and $C|_I = \bot$ and $c = \delta(C) = \delta(D) > 0$ such that $\ell \in D$ and $\bar{\ell} \in \text{decs}(I)$ and $\ell|_Q = \bot$ and $F \wedge \overline{M} \models D$ and $j = \delta(D \setminus \{\ell\})$ and $b = \delta(P) = c - 1$ and $K = Q_{\leqslant b}$ and $L = Q_{>b}$

Decide: $(F, I, M, \delta) \rightsquigarrow_{\text{Decide}} (F, I\ell^d, M, \delta[\ell \mapsto d])$ if $F|_I \neq \top$ and $\bot \notin F|_I$ and $\text{units}(F|_I) = \emptyset$ and $V(\ell) \in V$ and $\delta(\ell) = \infty$ and $d = \delta(I) + 1$

Conclusion

Our Contribution

- Combined chronological backtracking with CDCL for propositional model counting
- Formal calculus for propositional model counting based on these ideas
  - enumeration approach
  - no blocking clauses
  - escape search space regions with no solution
- Formal proof of correctness

Further Research

- Implement our rules to experimentally validate their effectiveness
- Investigate possible applications in SMT and QBF
- Extend our approach to projected model counting in combination with dual reasoning
- Target component-based reasoning