Introduction to the Boolean Satisfiability Problem

Spring 2020
CSCE 235H Introduction to Discrete Structures
URL: cse.unl.edu/~cse235h
All questions: [Piazza]

Satisfiability Study

- 7 weeks
- 30 min lectures in recitation
- ~2 hours of homework per week
- Goals:
  - Exposure to fundamental research in CS
  - Understand how to model problems
  - Learn to use SAT solver, MiniSAT

Boolean Satisfiability Problem

- Given:
  - A Boolean formula
- Question:
  - Is there an assignment of truth values to the Boolean variables such that the formula holds true?

Boolean Satisfiability Problem

$$a \vee (\neg a \wedge b)$$

$$(a \vee \neg a) \to (b \wedge \neg b)$$

Boolean Satisfiability Problem

$$a \vee (\neg a \wedge b)$$

SATISFIABLE
a=true, b=true

$$(a \vee \neg a) \rightarrow (b \wedge \neg b)$$

Boolean Satisfiability Problem

$$a \vee (\neg a \wedge b)$$

SATISFIABLE
a=true, b=true

$$(a \vee \neg a) \rightarrow (b \wedge \neg b)$$

UNSATISFIABLE
Left side of implication is a tautology.
Right side of implication is a contradiction.
True cannot imply false.

Applications of SAT

- Scheduling
- Resource allocation
- Hardware/software verification
- Planning
- Cryptography

Conjunctive Normal Form

- Variable $$a, b, p, q, x_1, x_2$$
- Literal $$a, \neg a, q, \neg q, x_1, \neg x_1$$
- Clause $$(a \vee \neg b \vee c)$$
- Formula $$\begin{aligned}&(a \vee \neg b \vee c)\\ &\wedge (b \vee c)\\ &\wedge (\neg a \vee \neg c)\end{aligned}$$

Converting to CNF

- All Boolean formulas can be converted to CNF
- The $\rightarrow, \leftrightarrow, \bigoplus$ operators can be rewritten in terms of $\neg, \vee, \wedge$
- $\neg, \vee, \wedge$ can be rearranged using
  - De Morgan's Laws
  - Distributive Laws
  - Double Negative
- May result in exponential size increase of the formula

Converting to CNF

$$(a \vee \neg a) \rightarrow (b \wedge \neg b) \equiv$$

Converting to CNF

$$(a \vee \neg a) \rightarrow (b \wedge \neg b) \equiv$$

Implication $\neg(a \vee \neg a) \vee (b \wedge \neg b) \equiv$

Converting to CNF

$$(a \vee \neg a) \rightarrow (b \wedge \neg b) \equiv$$

Implication $\neg(a \vee \neg a) \vee (b \wedge \neg b) \equiv$

DeMorgan's $(\neg a \wedge a) \vee (b \wedge \neg b) \equiv$

Converting to CNF

$$(a \vee \neg a) \rightarrow (b \wedge \neg b) \equiv$$

Implication $\neg(a \vee \neg a) \vee (b \wedge \neg b) \equiv$

DeMorgan's $(\neg a \wedge a) \vee (b \wedge \neg b) \equiv$

$$(\neg a \vee b) \wedge (\neg a \vee \neg b) \wedge (a \vee b) \wedge (a \vee \neg b)$$

Distributive

Interpretation of CNF

- Every clause must be satisfied by at least one true literal
- Total possible number of solutions increases as number of variables increases
- Clauses constrain the possible solutions
- Smaller clauses are more constraining

Interpretation of CNF

$$(a \vee \neg b \vee \neg c)$$
$$\wedge (b \vee c)$$
$$\wedge (\neg a)$$

a	b	C
0	0	0
0	0	1
0	1	0
0	1	1
1	0	0
1	0	1
1	1	0
1	1	1

Interpretation of CNF

$$(a \vee \neg b \vee \neg c) \equiv \neg(\neg a \wedge b \wedge c)$$

$$\wedge (b \vee c)$$

$$\wedge (\neg a)$$

a	b	C
0	0	0
0	0	1
0	1	0
0	1	1
1	0	0
1	0	1
1	1	0
1	1	1

Interpretation of CNF

$$(a \vee \neg b \vee \neg c)$$
$$\wedge (b \vee c) \equiv \neg(\neg b \wedge \neg c)$$
$$\wedge (\neg a)$$

a	b	C
0	0	0
0	0	1
0	1	0
0	1	1
1	0	0
1	0	1
1	1	0
1	1	1

Interpretation of CNF

$$(a \vee \neg b \vee \neg c)$$
$$\wedge (b \vee c)$$
$$\wedge (\neg a)$$

$$\equiv$$

$$\neg(a)$$

a	b	C
0	0	0
0	0	1
0	1	0
0	1	1
1	0	0
1	0	1
1	1	0
1	1	1

Interpretation of CNF

$$(a \vee \neg b \vee \neg c)$$
$$\wedge (b \vee c)$$
$$\wedge (\neg a)$$

a	b	C
0	0	0
0	0	1
0	1	0
0	1	1
1	0	0
1	0	1
1	1	0
1	1	1

Determining SAT/UNSAT

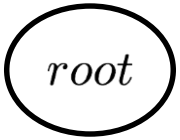
- All that is required to show satisfiability is to find a valid solution
- Many techniques available:
  - Guessing and checking
  - Systematic search
  - Inference

Systematic Search with Backtracking

- Construct a binary tree of all combinations
- Proceeds in a depth first manner
- Each level corresponds to a variable
- Each branch corresponds to a truth assignment
- Branches of the tree are 'pruned' when the assignment cannot be extended in a satisfiable manner

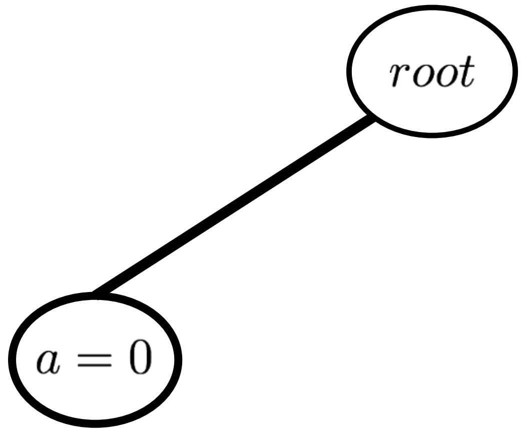
Systematic Search with Backtracking

$$
\begin{aligned}
&(a \vee b \vee c) \\
\wedge&(\neg a \vee \neg b) \\
\wedge&(\neg b \vee \neg c) \\
\wedge&(\neg c \vee \neg a)
\end{aligned}
$$



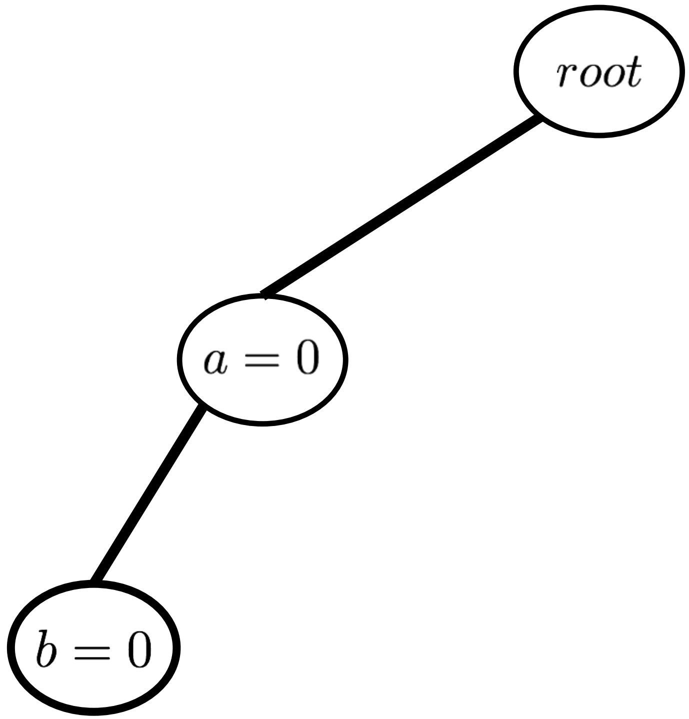
Systematic Search with Backtracking

$$
\begin{aligned}
&(\underline{a\,} \vee b \vee c)\\
\wedge&(\underline{\neg a} \vee \neg b)\\
\wedge&(\neg b \vee \neg c)\\
\wedge&(\neg c \vee \underline{\neg a})
\end{aligned}
$$



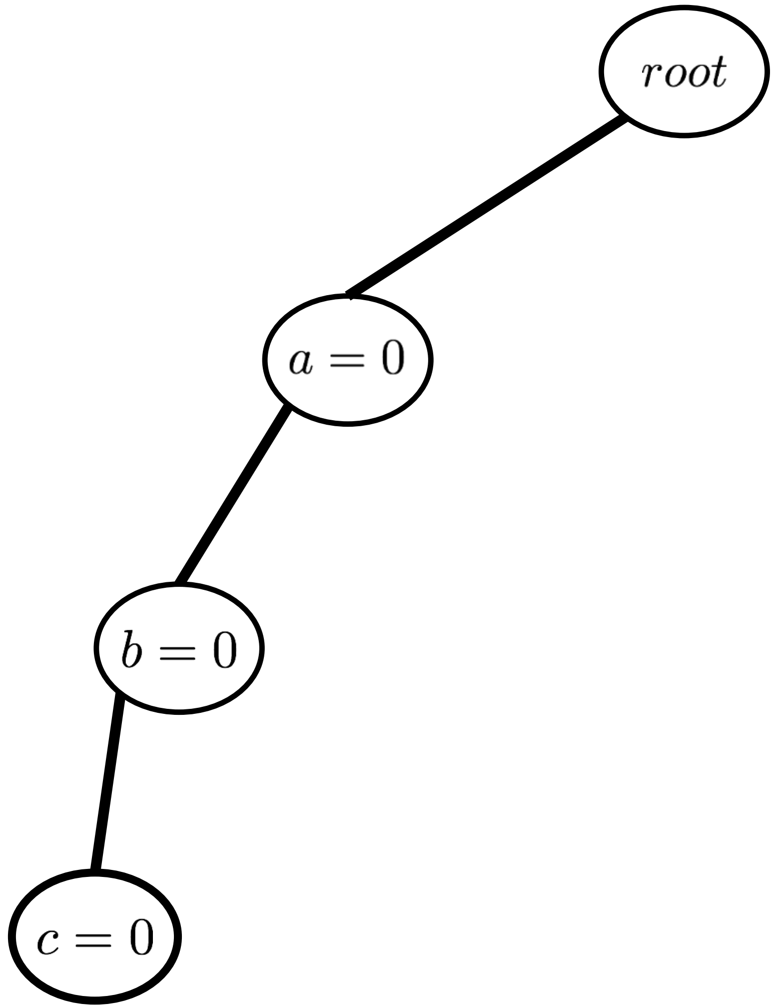
Systematic Search with Backtracking

$$(\underline{a \vee} \underline{b \vee} c)$$
$$\wedge(\underline{\neg a} \vee \underline{\neg b})$$
$$\wedge(\underline{\neg b} \vee \neg c)$$
$$\wedge(\neg c \vee \underline{\neg a})$$



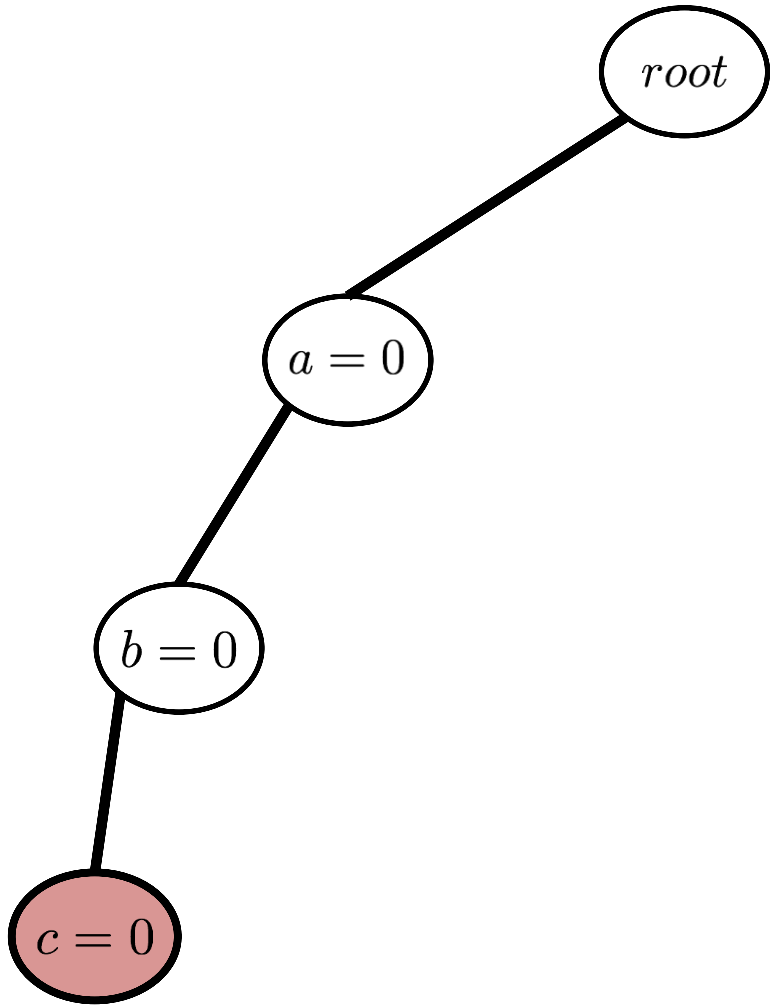
Systematic Search with Backtracking

$$
\begin{aligned}
&(a \vee b \vee c) \\
\wedge&(\neg a \vee \neg b) \\
\wedge&(\neg b \vee \neg c) \\
\wedge&(\neg c \vee \neg a)
\end{aligned}
$$



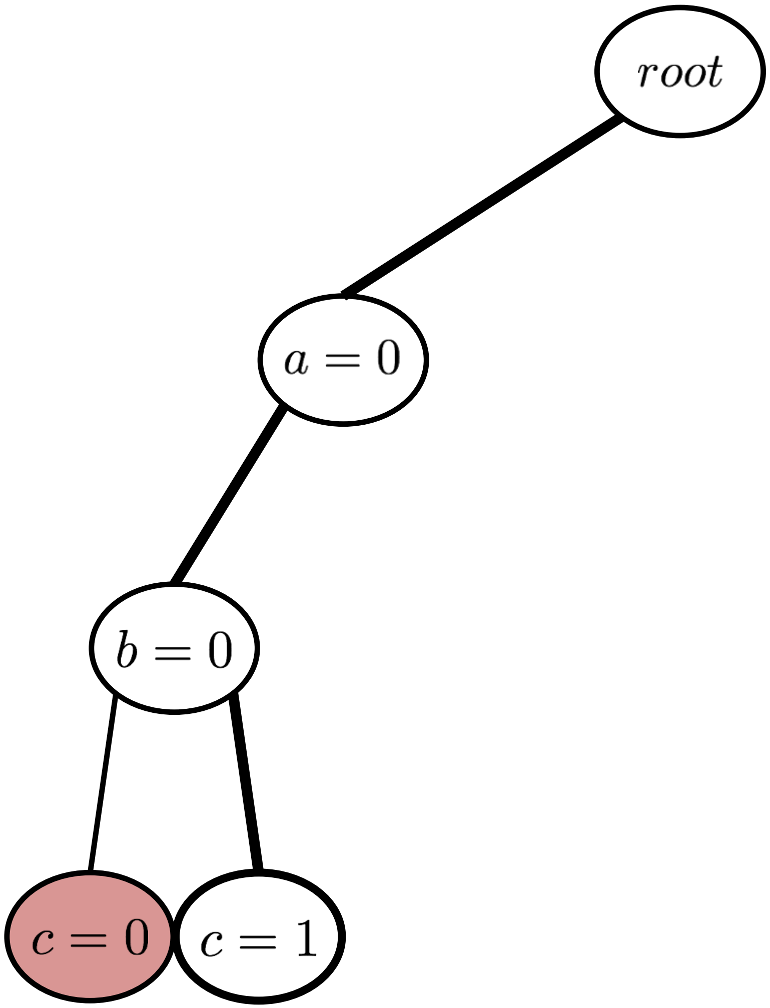
Systematic Search with Backtracking

$$(\underline{a} \lor \underline{b} \lor \underline{c})$$
$$\land(\underline{\neg a} \lor \underline{\neg b})$$
$$\land(\underline{\neg b} \lor \underline{\neg c})$$
$$\land(\underline{\neg c} \lor \underline{\neg a})$$



Systematic Search with Backtracking

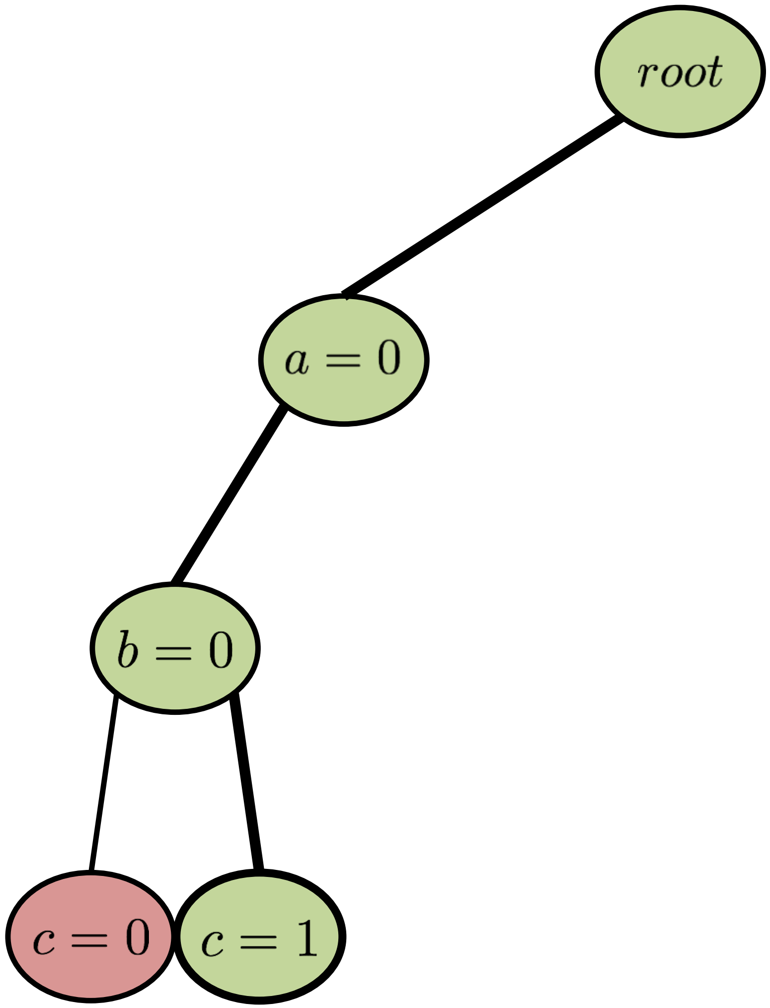
$$(\underline{a} \vee \underline{b} \vee \underline{c})$$
$$\wedge(\underline{\neg a} \vee \underline{\neg b})$$
$$\wedge(\underline{\neg b} \vee \underline{\neg c})$$
$$\wedge(\underline{\neg c} \vee \underline{\neg a})$$



Systematic Search with Backtracking

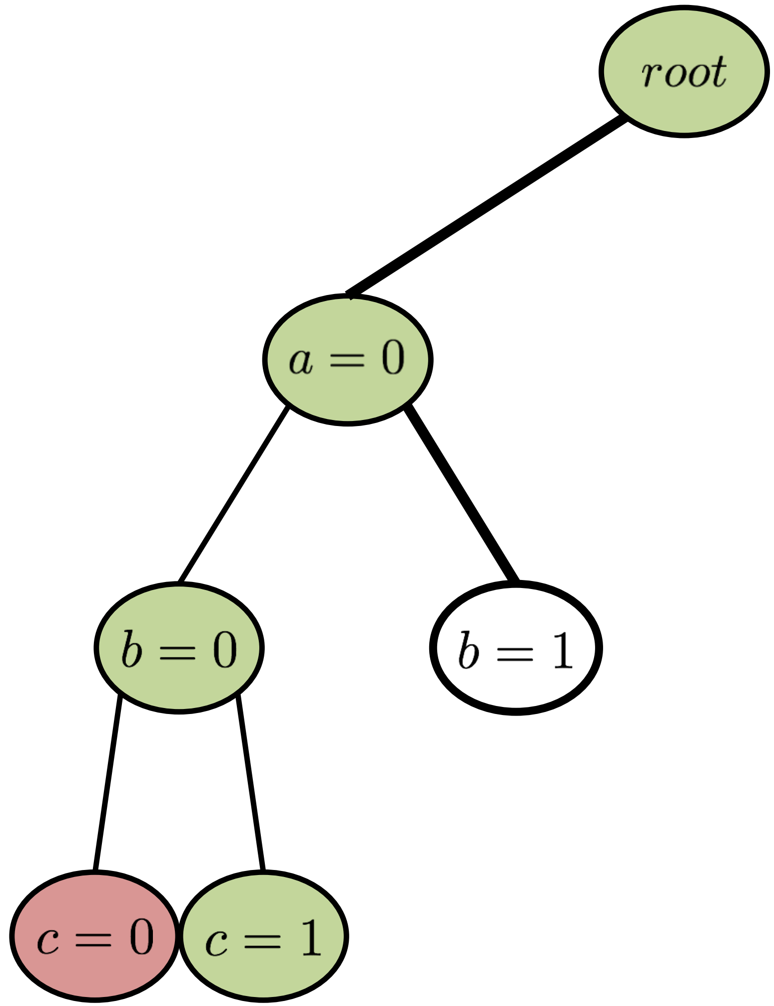
$$(a \vee b \vee c)$$
$$\wedge(\neg a \vee \neg b)$$
$$\wedge(\neg b \vee \neg c)$$
$$\wedge(\neg c \vee \neg a)$$

Satisfiable



Systematic Search with Backtracking

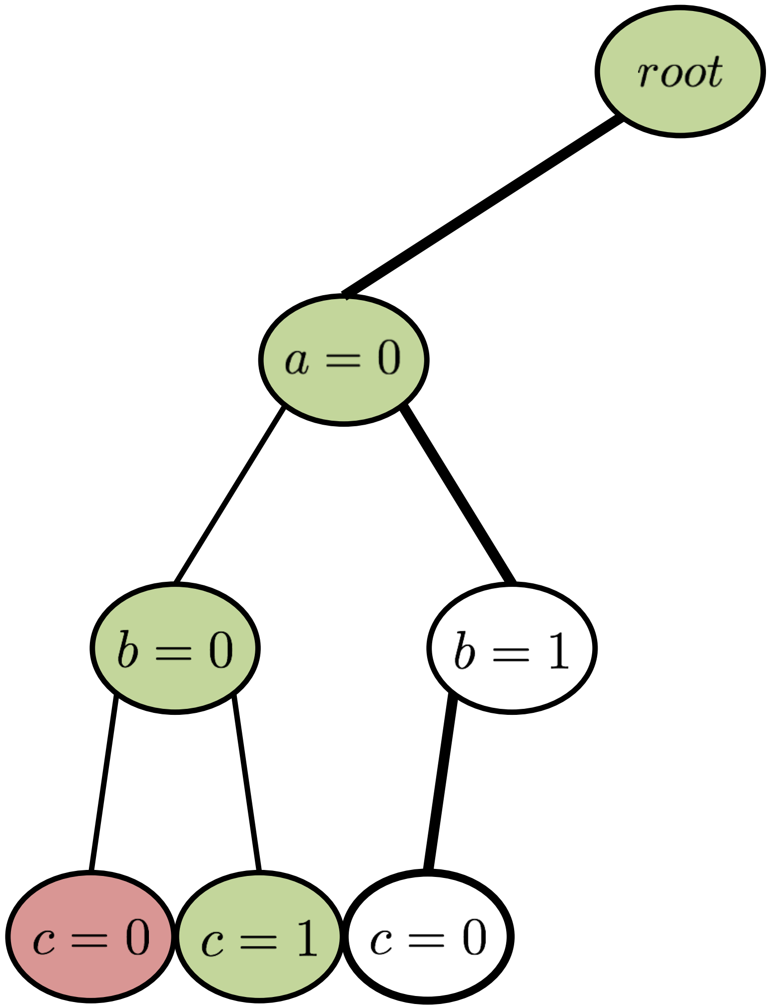
$$(\underline{a} \vee \underline{b} \vee c)$$
$$\wedge(\underline{\neg a} \vee \underline{\neg b})$$
$$\wedge(\underline{\neg b} \vee \neg c)$$
$$\wedge(\neg c \vee \underline{\neg a})$$



Satisfiable

Systematic Search with Backtracking

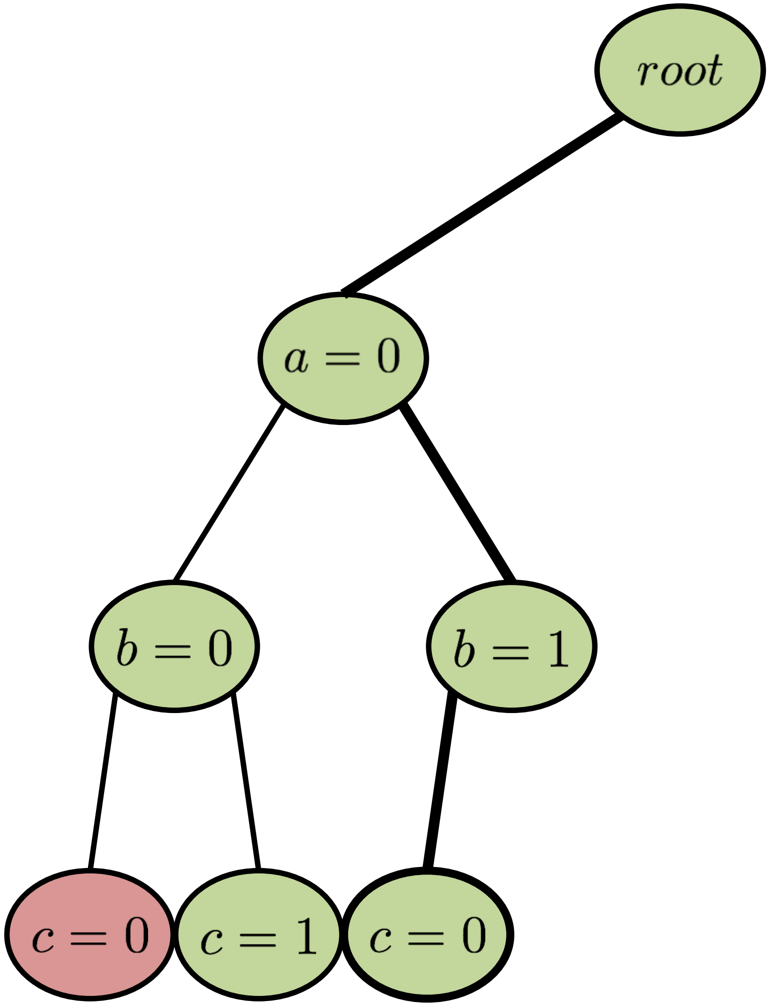
$$
\begin{aligned}
&(a \vee b \vee c) \\
\wedge&(\neg a \vee \neg b) \\
\wedge&(\neg b \vee \neg c) \\
\wedge&(\neg c \vee \neg a)
\end{aligned}
$$



Satisfiable

Systematic Search with Backtracking

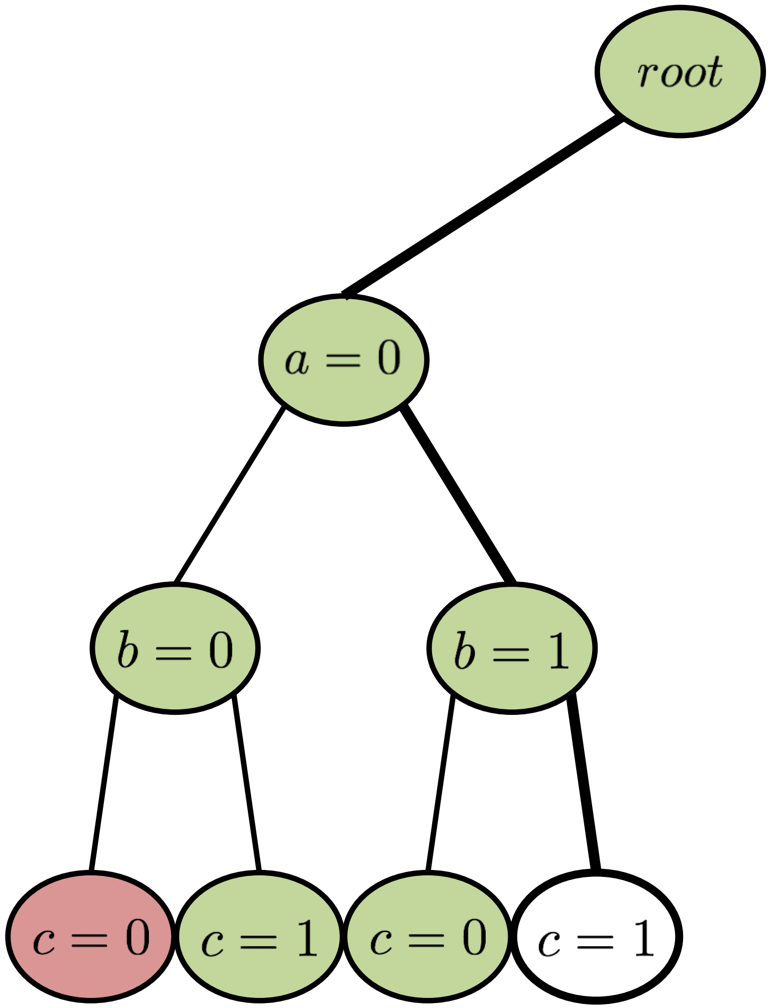
$$(a \lor b \lor c)$$
$$\land(\neg a \lor \neg b)$$
$$\land(\neg b \lor \neg c)$$
$$\land(\neg c \lor \neg a)$$



Satisfiable

Systematic Search with Backtracking

$$(\underline{a} \vee \underline{b} \vee \underline{c})$$
$$\wedge(\underline{\neg a} \vee \underline{\neg b})$$
$$\wedge(\underline{\neg b} \vee \underline{\neg c})$$
$$\wedge(\underline{\neg c} \vee \underline{\neg a})$$

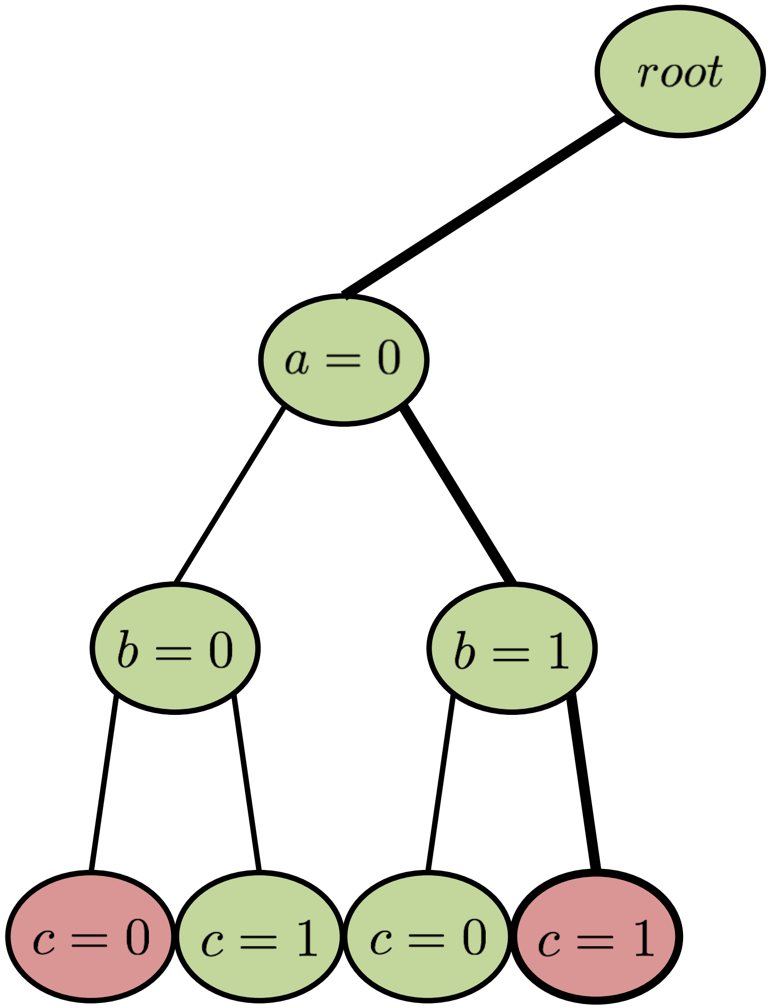


Satisfiable

Systematic Search with Backtracking

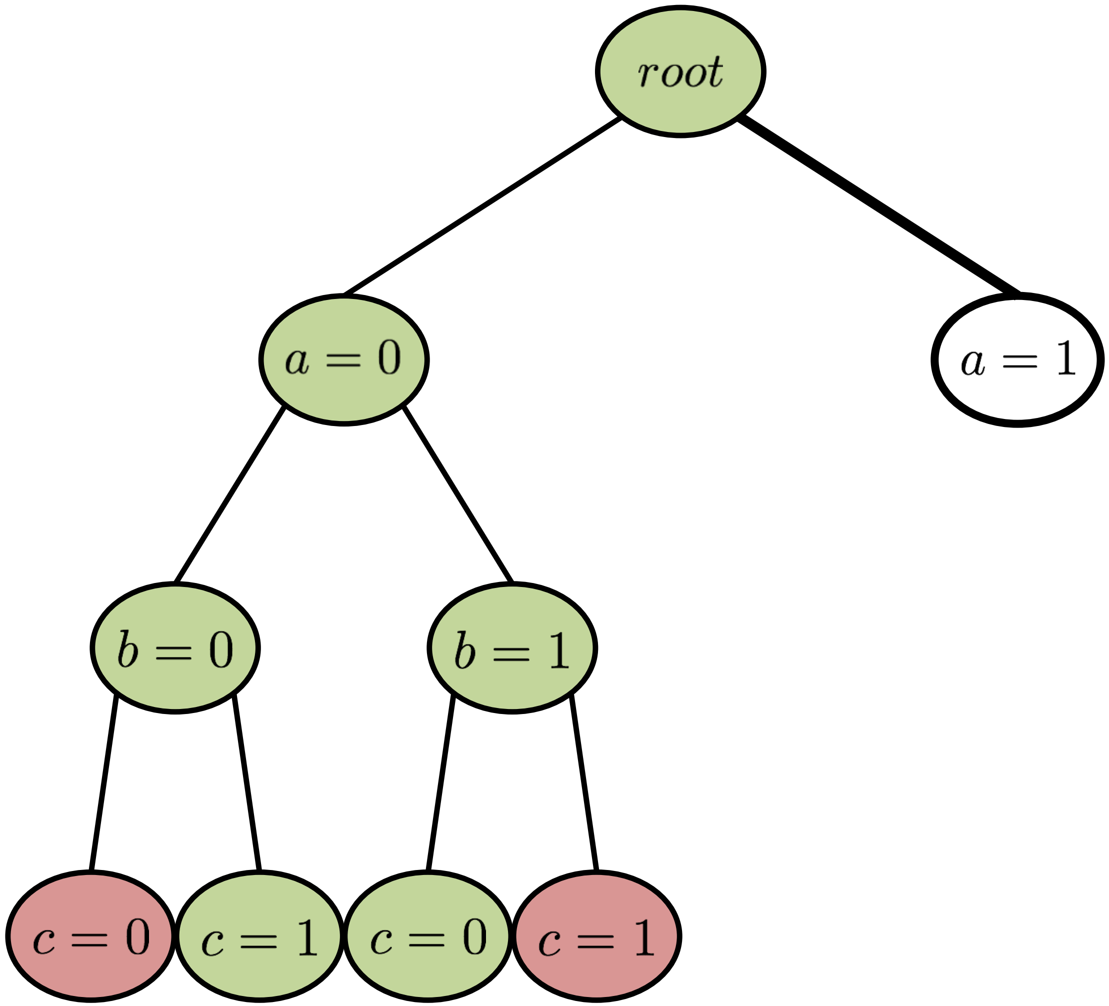
$$(a \vee b \vee c)$$
$$\wedge(\neg a \vee \neg b)$$
$$\wedge(\neg b \vee \neg c)$$
$$\wedge(\neg c \vee \neg a)$$

Satisfiable



Systematic Search with Backtracking

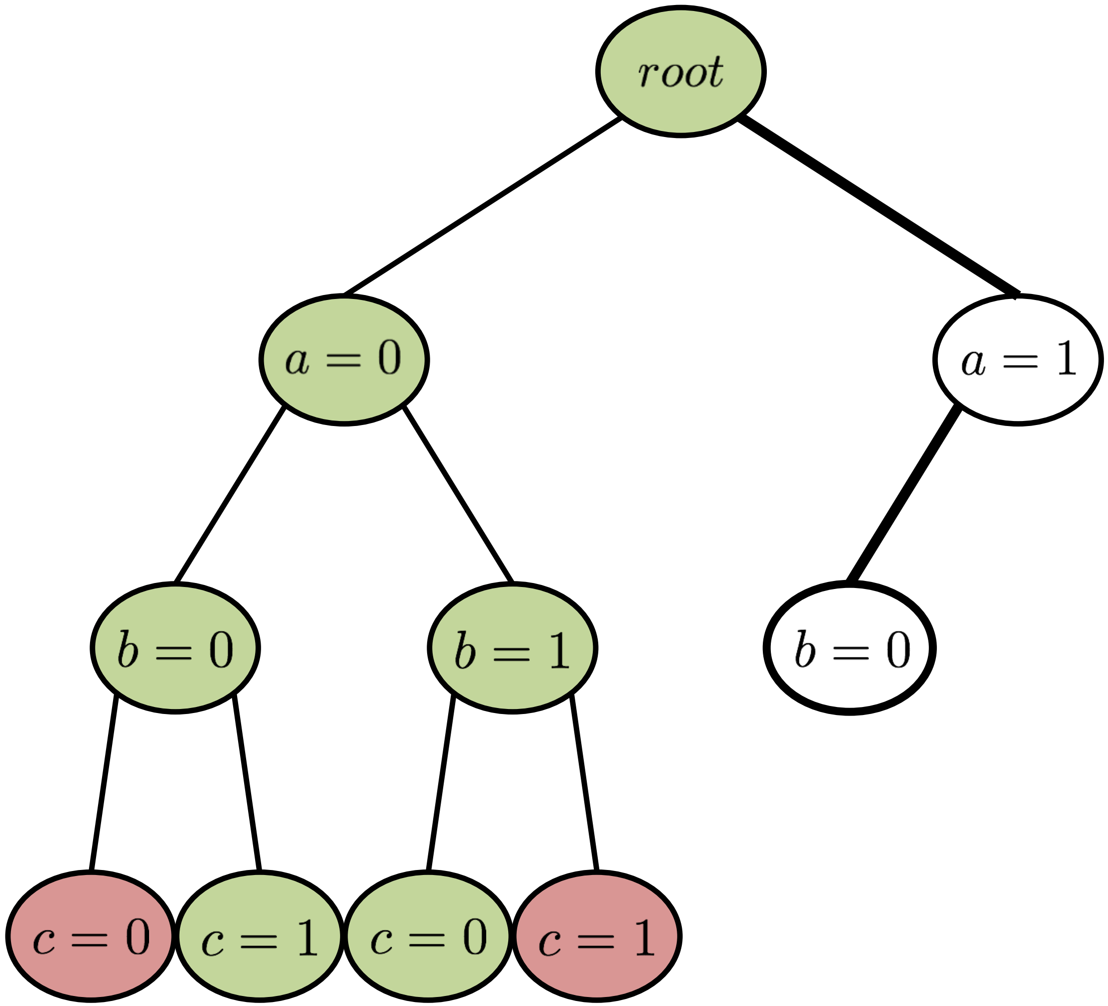
$$(a \lor b \lor c)$$
$$\land(\neg a \lor \neg b)$$
$$\land(\neg b \lor \neg c)$$
$$\land(\neg c \lor \neg a)$$



Satisfiable

Systematic Search with Backtracking

$$(a \vee b \vee c)$$
$$\wedge(\neg a \vee \neg b)$$
$$\wedge(\neg b \vee \neg c)$$
$$\wedge(\neg c \vee \neg a)$$

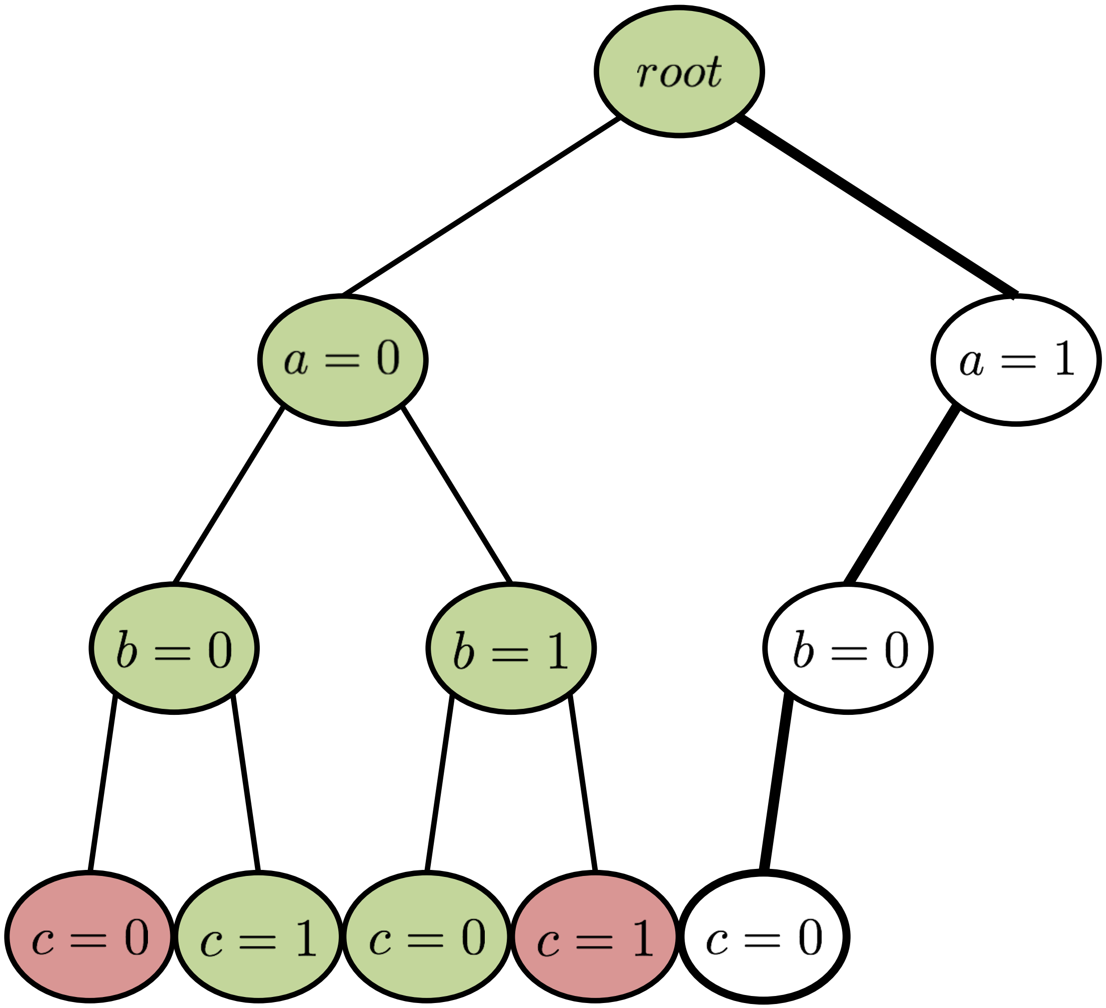


Satisfiable

Systematic Search with Backtracking

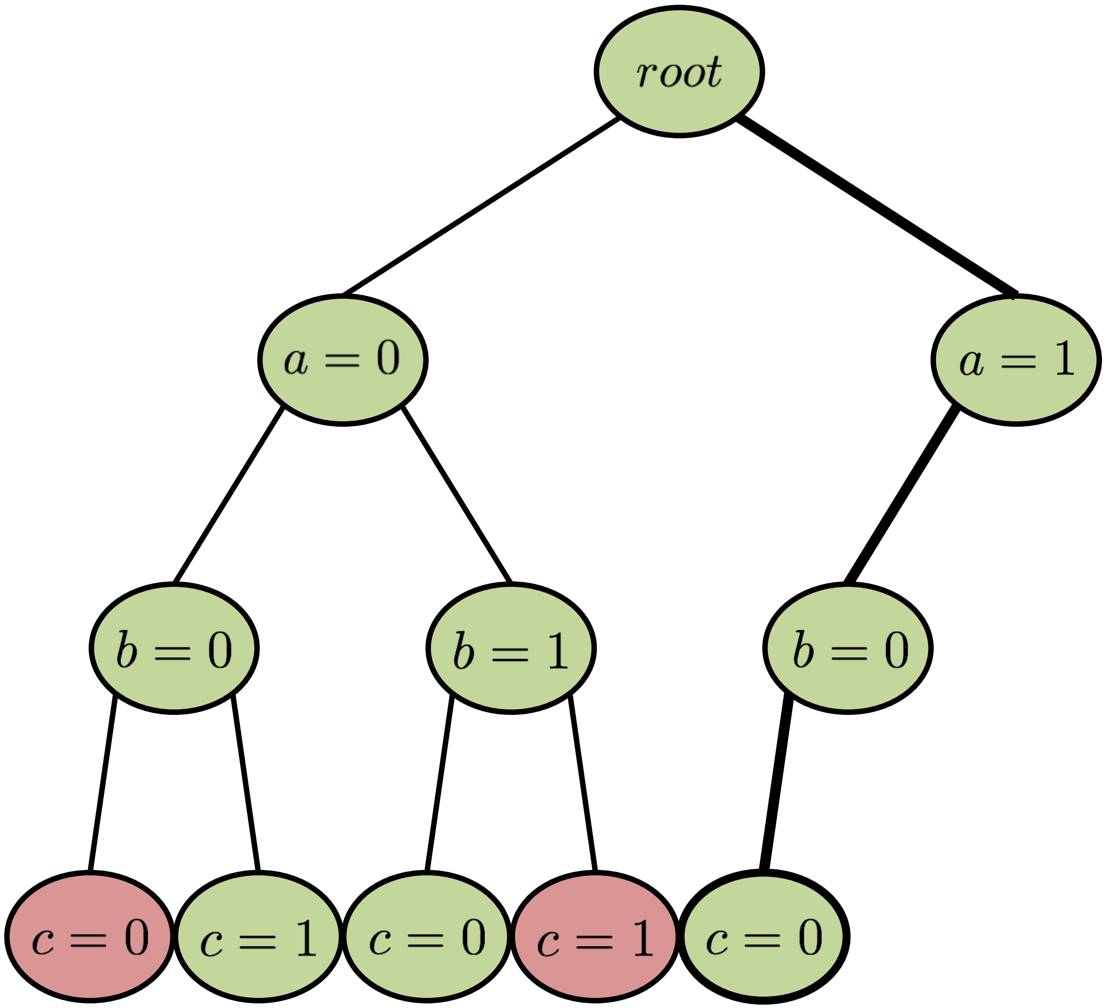
$$(a \lor b \lor c)$$
$$\land(\neg a \lor \neg b)$$
$$\land(\neg b \lor \neg c)$$
$$\land(\neg c \lor \neg a)$$

Satisfiable



Systematic Search with Backtracking

$$(a \vee b \vee c)$$
$$\wedge(\neg a \vee \neg b)$$
$$\wedge(\neg b \vee \neg c)$$
$$\wedge(\neg c \vee \neg a)$$

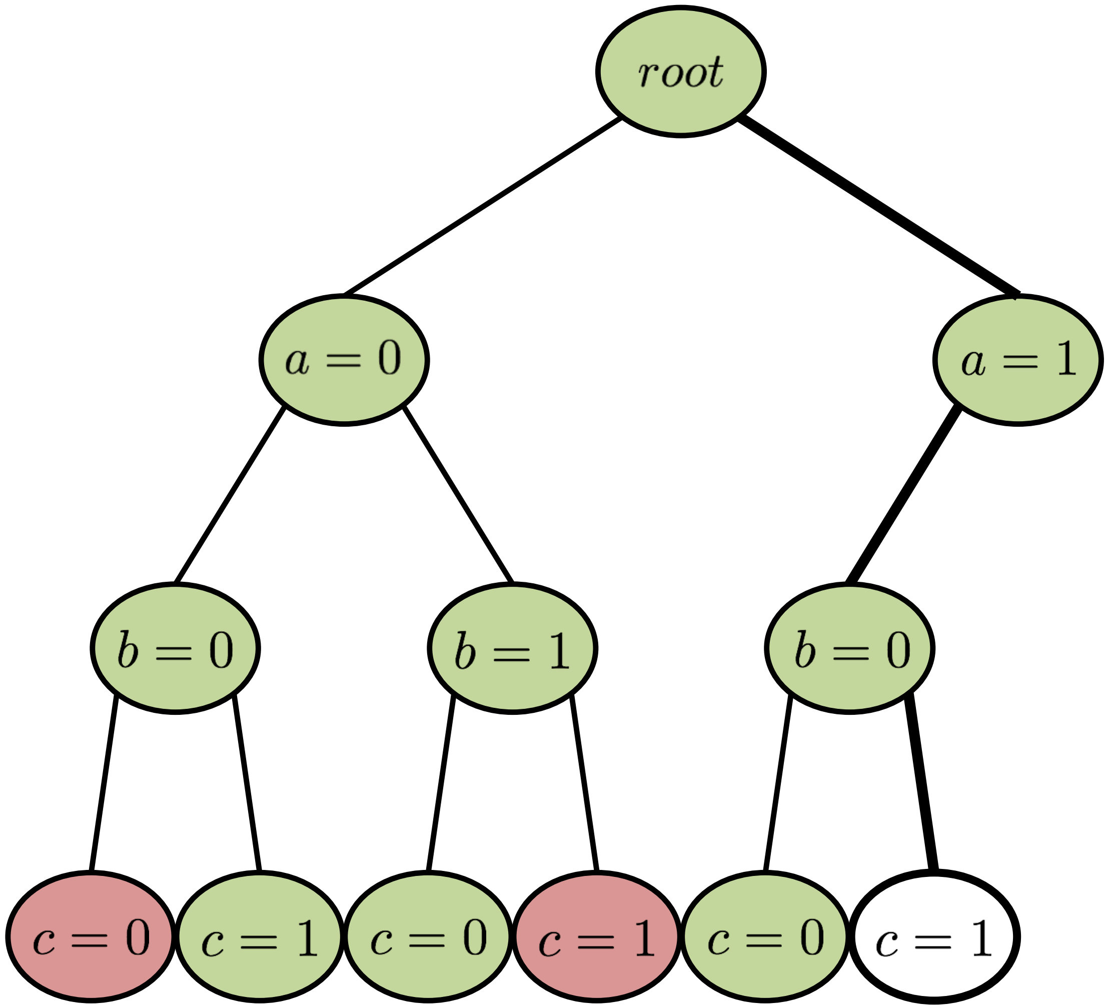


Satisfiable

Systematic Search with Backtracking

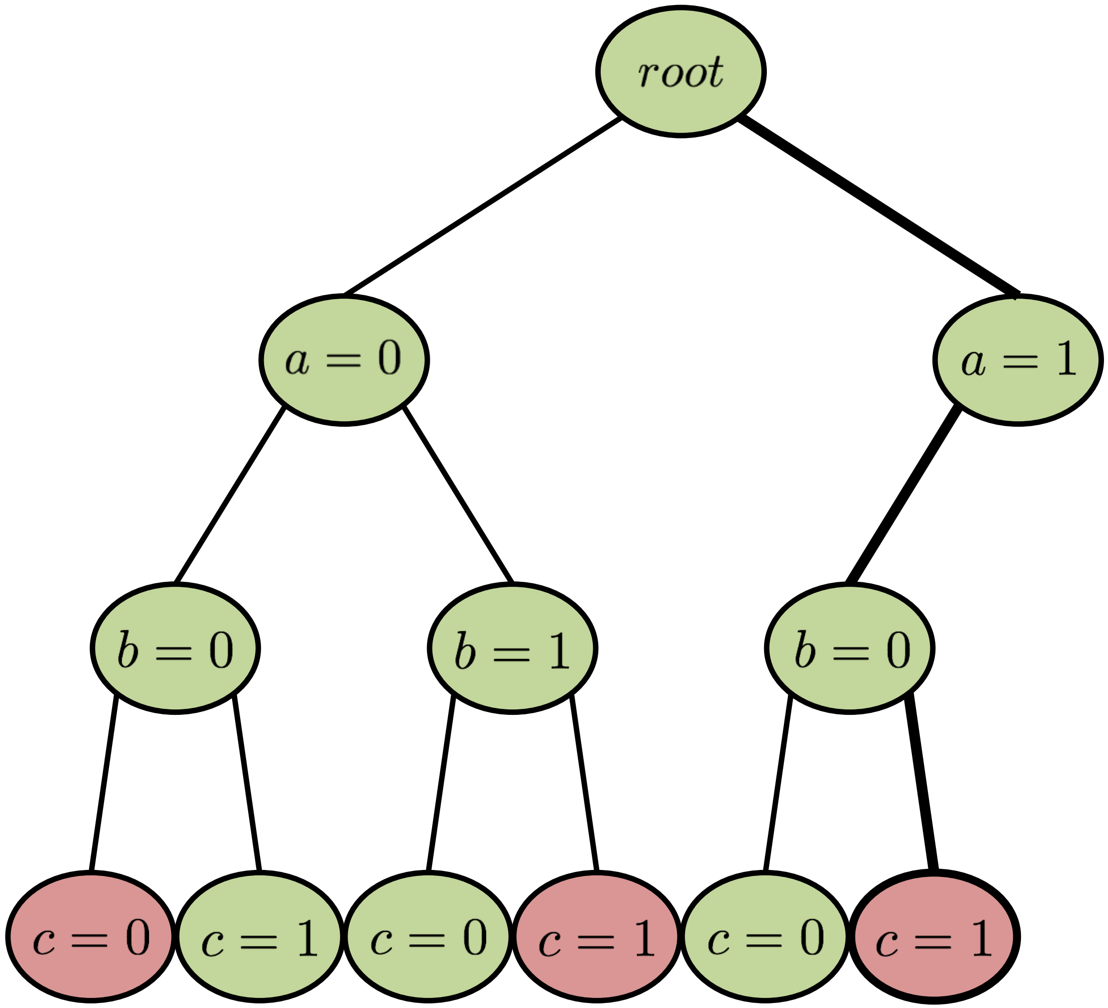
$$(a \lor b \lor c)$$
$$\land(\neg a \lor \neg b)$$
$$\land(\neg b \lor \neg c)$$
$$\land(\neg c \lor \neg a)$$

Satisfiable



Systematic Search with Backtracking

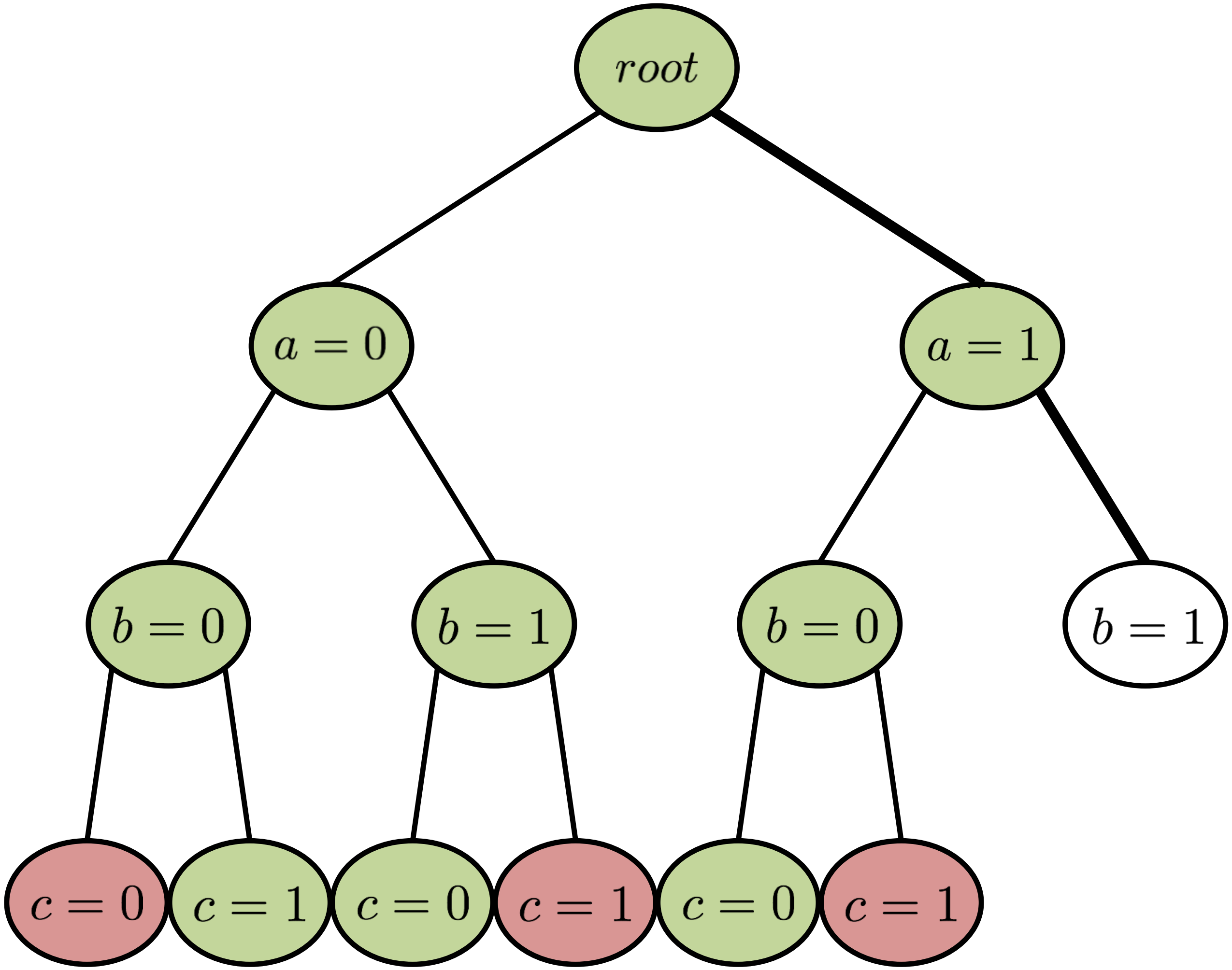
$$(a \vee b \vee c)$$
$$\wedge(\neg a \vee \neg b)$$
$$\wedge(\neg b \vee \neg c)$$
$$\wedge(\neg c \vee \neg a)$$



Satisfiable

Systematic Search with Backtracking

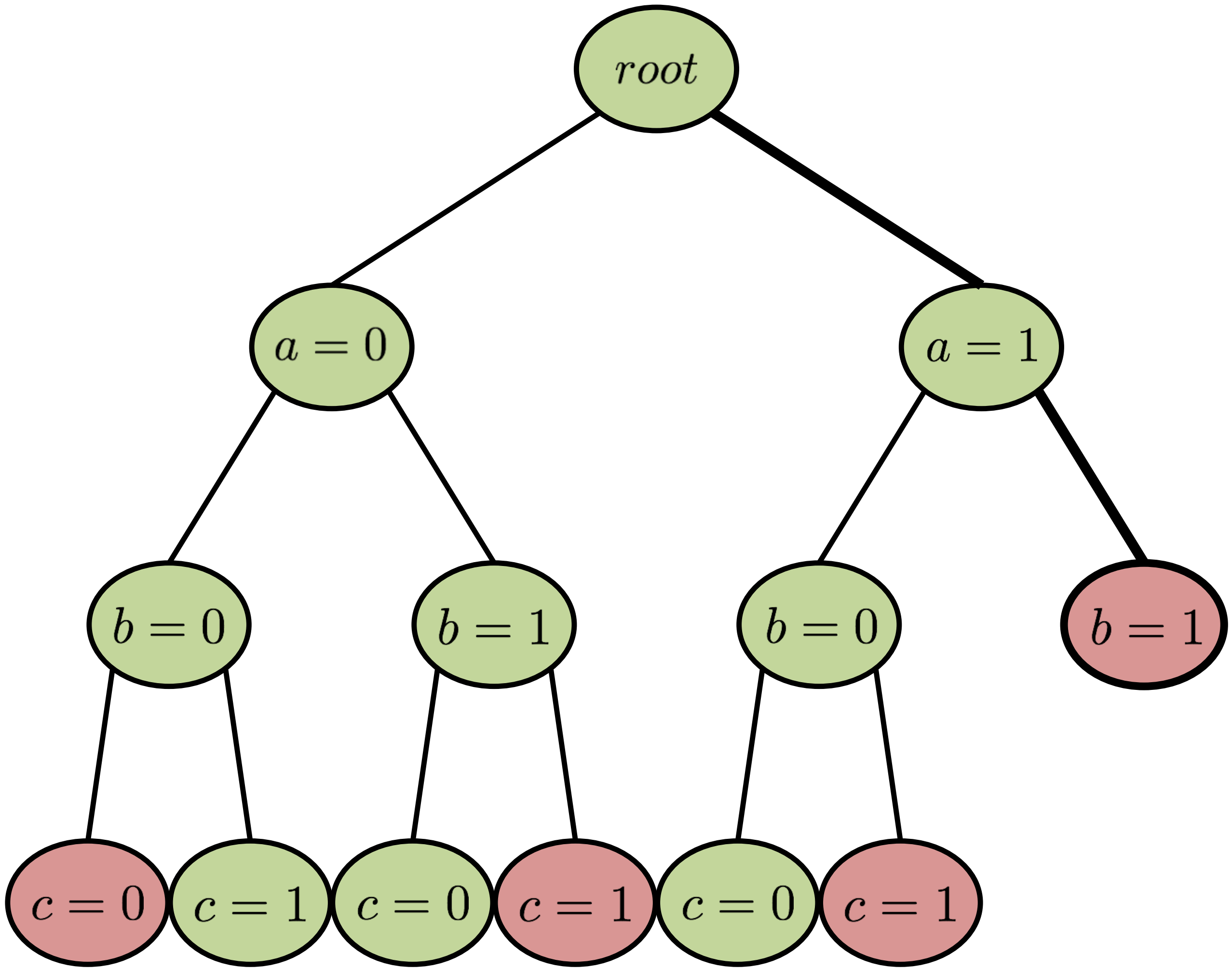
$$(a \lor b \lor c)$$
$$\land(\neg a \lor \neg b)$$
$$\land(\neg b \lor \neg c)$$
$$\land(\neg c \lor \neg a)$$



Satisfiable

Systematic Search with Backtracking

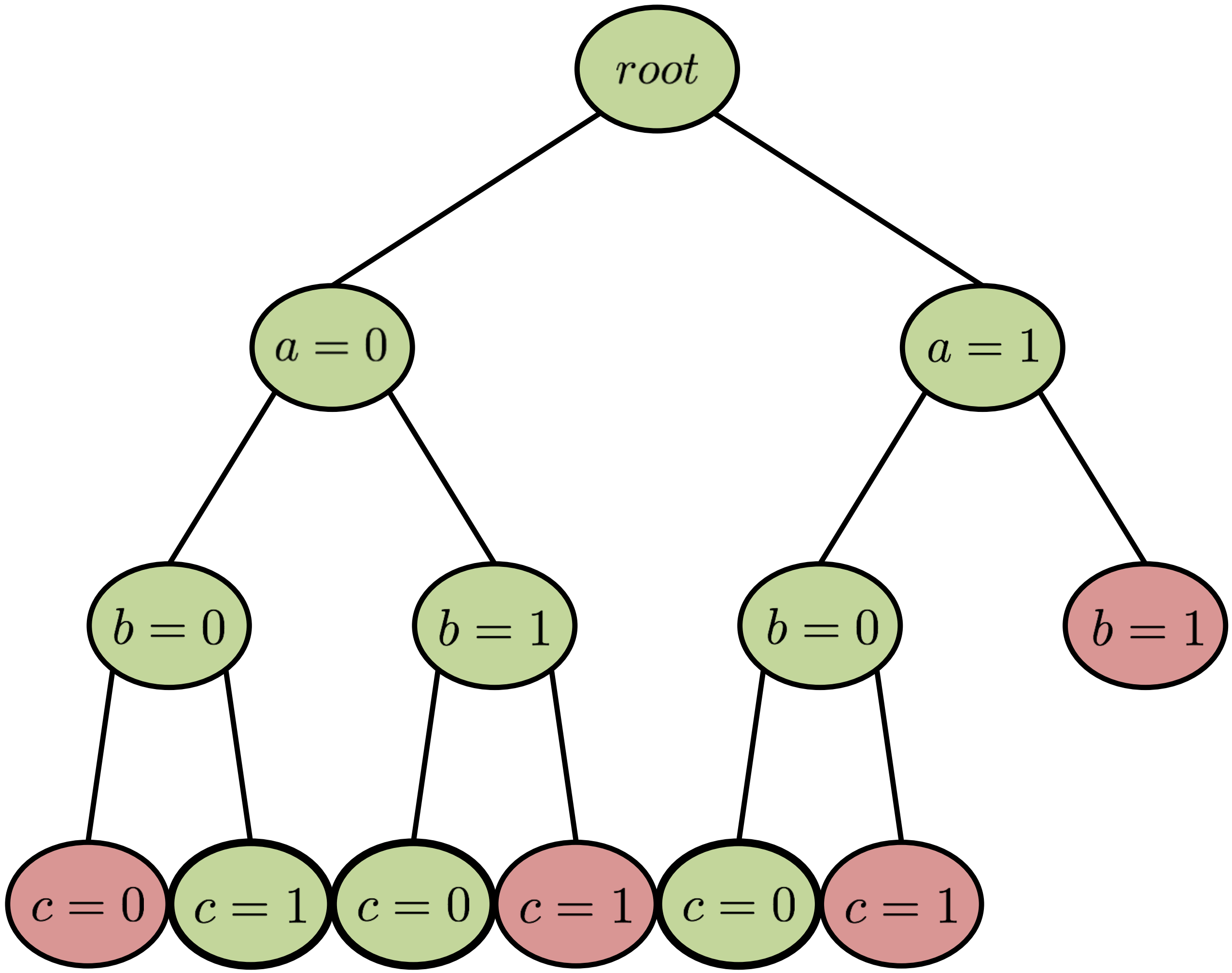
$$
\begin{aligned}
&(\underline{a} \vee \underline{b} \vee c)\\
\wedge&(\underline{\neg a} \vee \underline{\neg b})\\
\wedge&(\underline{\neg b} \vee \neg c)\\
\wedge&(\neg c \vee \underline{\neg a})
\end{aligned}
$$



Satisfiable

Systematic Search with Backtracking

$$(a \vee b \vee c)$$
$$\wedge(\neg a \vee \neg b)$$
$$\wedge(\neg b \vee \neg c)$$
$$\wedge(\neg c \vee \neg a)$$



Satisfiable
3 solutions total