3.12.15 Theorem (Craig's Theorem)

Let ϕ and ψ be two propositional (first-order ground) formulas so that $\phi \models \psi$. Then there exists a formula χ (called the *interpolant* for $\phi \models \psi$), so that χ contains only propositional variables (first-order signature symbols) occurring both in ϕ and in ψ so that $\phi \models \chi$ and $\chi \models \psi$.

First-Order Logic Theories

3.17.1 Definition (First-Order Logic Theory)

Given a first-order many-sorted signature Σ, a *theory* $\mathcal{T}$ is a set of Σ-algebras.
For some first-order formula ϕ over Σ we say that ϕ is $\mathcal{T}$-*satisfiable* if there is some $\mathcal{A} \in \mathcal{T}$ such that $\mathcal{A}(\beta) \models \phi$ for some β. We say that ϕ is $\mathcal{T}$-*valid* ($\mathcal{T}$-*unsatisfiable*) if for all $\mathcal{A} \in \mathcal{T}$ and all β it holds $\mathcal{A}(\beta) \models \phi$ ($\mathcal{A}(\beta) \not\models \phi$). In case of validity I also write $\models_{\mathcal{T}} \phi$.

Alternatively, $\mathcal{T}$ may contain a set of satisfiable axioms which then stand for all algebras satisfying the axioms.

CDCL(T)

Consider a SAT problem where the propositional variables actually stand for ground atoms over some theory, ground equations or ground atoms of LRA, i.e., LRA atoms where all variables are existentially quantified. The basic idea is to apply CDCL, Section 2.9 in order to investigate the boolean structure of the problem. If CDCL derives unsatisfiable, then the problem clearly is. If CDCL derives satisfiable, then a ground decision procedure for the theory has to check whether the actual CDCL assignment constitutes also a model in the theory.

Let N be a finite set of clauses over some theory $\mathcal{T}$ over signature $\Sigma_{\mathcal{T}}$ such that there exists a decision procedure for satisfiability of a conjunction of literals: $\models_{\mathcal{T}} L_1 \wedge \ldots \wedge L_n$. Let $\mathtt{atr}$ be a bijection from the atoms over $\Sigma_{\mathcal{T}}$ into propositional variables Σ_{PROP} auch that $\mathtt{atr}^{-1}(\mathtt{atr}(A)) = A$. Furthermore, $\mathtt{atr}$ distributes over the propositional operators, e.g., $\mathtt{atr}(\neg A) = \neg\,\mathtt{atr}(A)$.

7.2.1 Lemma (Correctness of $\mathtt{atr}$)

Let N be a set of clauses over some theory $\mathcal{T}$. If $\mathtt{atr}(N) \models \bot$ then $N \models_{\mathcal{T}} \bot$.

A CDCL(T) problem state is a five-tuple $(M; N; U; k; C)$ where N is the propositional abstraction of some clause set N', $N = \mathtt{atr}(N')$, M a sequence of annotated propositional literals, U is a set of detived propositional clauses, $k \in \mathbb{N}$, and C is a propositional clause or $\top$ or $\bot$ or $\triangle$. In particular, the following states can be distinguished:

$(\epsilon; N; \emptyset; 0; \top)$	is the start state for some clause set N
$(M; N; U; k; \triangle)$	is a final state, where $\mathtt{atr}^{-1}(M) \models_{\mathcal{T}} N'$, $\mathtt{atr}^{-1}(M)$ satisfiable
$(M; N; U; k; \bot)$	is a final state, where N' has no model
$(M; N; U; k; \top)$	is a model search state if $k \neq 0$
$(M; N; U; k; D)$	is a backtracking state if $D \notin \{\top, \bot\}$

Propagate $(M; N; U; k; \top) \Rightarrow_{\text{CDCL}} (ML^{C \lor L}; N; U; k; \top)$
provided $C \lor L \in (N \cup U)$, $M \models \neg C$, and L is undefined in M

Decide $(M; N; U; k; \top) \Rightarrow_{\text{CDCL}} (ML^{k+1}; N; U; k+1; \top)$
provided L is undefined in M

Conflict $(M; N; U; k; \top) \Rightarrow_{\text{CDCL}} (M; N; U; k; D)$
provided $D \in (N \cup U)$ and $M \models \neg D$

Skip $(ML^{C\vee L}; N; U; k; D) \Rightarrow_{\text{CDCL}} (M; N; U; k; D)$

provided $D \notin \{\top, \bot\}$ and $\text{comp}(L)$ does not occur in D

Resolve $(ML^{C\vee L}; N; U; k; D \vee \text{comp}(L)) \Rightarrow_{\text{CDCL}}$
$(M; N; U; k; D \vee C)$

provided D is of level k

Backtrack $(M_1 K^{i+1} M_2; N; U; k; D \vee L) \Rightarrow_{\text{CDCL}}$
$(M_1 L^{D\vee L}; N; U \cup \{D \vee L\}; i; \top)$

provided L is of level k and D is of level i.

Restart $(M; N; U; k; \top) \Rightarrow_{\text{CDCL}} (\epsilon; N; U; 0; \top)$

provided $M \not\models N$

Forget $(M; N; U \uplus \{C\}; k; \top) \Rightarrow_{\text{CDCL}} (M; N; U; k; \top)$

provided $M \not\models N$

Note that these rules are exactly the rules of CDCL from Section 2.9. The only difference that any normal form $(M; N; U; k; \top)$ was a final state in CDCL, but not in CDCL(T). On the other hand, if CDCL derives the empty clause, i.e., $\bot$, then this is also a final state for CDCL(T), see Lemma 7.2.1. The $\mathcal{T}$ rules are missing that in particular check whether the propoistional model is in fact also a theory model.

$\mathcal{T}$-Success $(V; M; N; U; k; \top) \Rightarrow_{\text{CDCL(T)}} (V; M; N; U; k; \triangle)$
provided $M \models (N \cup U)$ and $\mathrm{atr}^{-}1(M)$ is $\mathcal{T}$-satisfiable.

$\mathcal{T}$-Propagate $(V; M; N; U; k; \top)$
$\Rightarrow_{\text{CDCL(T)}} (V; M_1 L^{C \vee L}; N; U \cup \{C \vee L\}; j; \top)$
provided $\models_{\mathcal{T}} \mathrm{atr}^{-}1(C \vee L)$, L is undefined in M, $\mathrm{atom}(L) \in V$, $C \vee L \notin (N \cup U)$, $M = M_1 M_2$, $M_1 \models \neg C$, $M_1 = \epsilon$ or $M_1 = M_3 K$ and $M_3 \not\models \neg C$, and j is the decision level of $M_1 L^{C \vee L}$.

$\mathcal{T}$-Atom $(V; M; N; U; k; \top)$

$\Rightarrow_{\text{CDCL(T)}} \quad (V \cup \{A\}; M; N; U; k; \top)$

provided $A \notin V$ and $\text{atr}^-1(A)$ is a meaningful $\mathcal{T}$-atom.

$\mathcal{T}$-Learn $(V; M; N; U; k; \top)$

$\Rightarrow_{\text{CDCL(T)}} \quad (V; M_1; N; U \cup \{C\}; j; \top)$

provided $\text{atom}(C) \subseteq V$, $\models_{\mathcal{T}} \text{atr}^-1(C)$, $C \notin (N \cup U)$ and $M \not\models \neg C$. If $|\text{atom}(C) \cap \text{atom}(M)| < |C| - 1$ or $M \models C$ then $M_1 = M$, else if $|\text{atom}(C) \cap \text{atom}(M)| = |C| - 1$ and $\text{atom}(L) \in \text{atom}(C)$ is the rightmost atom of C in M then $M = M_2\, \text{comp}(L) M_3$ and $M_1 = M_2\, \text{comp}(L)$. In all cases, j is the decision level of M_1.

$\mathcal{T}$-Conflict $(V; M; N; U; k; \top)$

$\Rightarrow_{\mathrm{CDCL(T)}}$ $(V; M_1; N; U \cup \{C \vee L\}; j; \top)$

provided $\models_{\mathcal{T}} \mathrm{atr}^-1(C \vee L)$, $M \models \neg(C \vee L)$, $M = M_1 M_2\, \mathrm{comp}(L) M_3$, $M_1 \models \neg C$, $M_1 = \epsilon$ or $M_1 = M_4 K$ and $M_4 \not\models \neg C$, and j is the decision level of M_1.

7.2.4 Definition (Reasonable CDCL(T) Strategy)

A CDCL(T) strategy is *reasonable* if the rules Conflict and Propagate are always preferred over all other rules.

7.2.5 Definition (Sound State)

A CDCL(T) state $(V; M; N; U; k; D)$ is called sound if

1. $\text{atr}^{-}1(N) \models_{\mathcal{T}} \text{atr}^{-}1(U)$,
2. if $D \neq \triangle$, then $N \cup U \models D$,
3. if $D \notin \{\top, \triangle\}$, then $M \models \neg D$,
4. if $D \notin \{\top, \triangle\}$, then D is of level k,
5. if $M = M_1 L^{C \vee L} M_2$, then $C \vee L \in (N \cup U)$, $M_1 \models \neg C$ and C is of the same level as L,
6. if $M = M_1 K^j M_2$, then there is no clause $C \vee L \in (N \cup U)$ such that $M_1 \models \neg C$ and L is undefined in M_1,
7. and if $M = M_1 L M_2$ then there is no $C \in (N \cup U)$ such that $M_1 \models \neg C$.