Optimization

Here is lots of room for optimization since we only can preserve satisfiability anyway:

- size of the CNF exponential when done naively;
  but see the transformations we introduced for propositional logic
- want to preserve the original formula structure;
- want small arity of Skolem functions (follows)

3.6 Getting small Skolem Functions

- produce a negation normal form (NNF)
- apply miniscoping
- rename all variables
- skolemize

Negation Normal Form (NNF)

Apply the rewrite relation $\Rightarrow_{NNF}$, F is the overall formula:

$$
\begin{array}{rcl}
G \leftrightarrow H & \Rightarrow_{NNF} & (G \rightarrow H) \wedge (H \rightarrow G) \\
& & \text{if } F/p = G \leftrightarrow H \text{ and } F/p \text{ has positive polarity} \\
G \leftrightarrow H & \Rightarrow_{NNF} & (G \wedge H) \vee (\neg H \wedge \neg G) \\
& & \text{if } F/p = G \leftrightarrow H \text{ and } F/p \text{ has negative polarity} \\
\neg Qx\, G & \Rightarrow_{NNF} & \overline{Q}x \neg G \\
\neg(G \vee H) & \Rightarrow_{NNF} & \neg G \wedge \neg H \\
\neg(G \wedge H) & \Rightarrow_{NNF} & \neg G \vee \neg H \\
G \rightarrow H & \Rightarrow_{NNF} & \neg G \vee H \\
\neg\neg G & \Rightarrow_{NNF} & G
\end{array}
$$

Miniscoping

Apply the rewrite relation $\Rightarrow_{MS}$. For the below rules we assume that x occurs freely in G, H, but x does not occur freely in F:

$$
\begin{array}{rcl}
Qx\,(G \wedge F) & \Rightarrow_{MS} & Qx\, G \wedge F \\
Qx\,(G \vee F) & \Rightarrow_{MS} & Qx\, G \vee F \\
\forall x\,(G \wedge H) & \Rightarrow_{MS} & \forall x\, G \wedge \forall x\, H \\
\exists x\,(G \vee H) & \Rightarrow_{MS} & \exists x\, G \vee \exists x\, H
\end{array}
$$

Variable Renaming

Rename all variables in F such that there are no two different positions p, q with $F/p = Qx\, G$ and $F/q = Qx\, H$.

Standard Skolemization

Let F be the overall formula, then apply the rewrite rule:

$$\begin{array}{lll} \exists x\, H & \Rightarrow_{SK} & H[f(y_1, \dots, y_n)/x] \\ & \multicolumn{2}{l}{\text{if } F/p = \exists x\, H \text{ and } p \text{ has minimal length,}} \\ & \multicolumn{2}{l}{\{y_1, \dots, y_n\} \text{ are the free variables in } \exists x\, H,} \\ & \multicolumn{2}{l}{f \text{ is a new function symbol, } \mathsf{arity}(f) = n} \end{array}$$

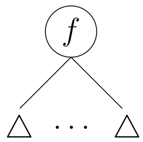
3.7 Herbrand Interpretations

From now an we shall consider PL without equality. Ω shall contains at least one constant symbol.

A *Herbrand interpretation* (over Σ) is a Σ-algebra $\mathcal{A}$ such that

- $U_{\mathcal{A}} = \mathrm{T}_{\Sigma}$ (= the set of ground terms over Σ)
- $f_{\mathcal{A}} : (s_1, \dots, s_n) \mapsto f(s_1, \dots, s_n),\ f \in \Omega, \mathsf{arity}(f) = n$

$f_{\mathcal{A}}(\triangle, \dots, \triangle) =$



In other words, *values are fixed* to be ground terms and *functions are fixed* to be the *term constructors*. Only predicate symbols $p \in \Pi$, $\mathsf{arity}(p) = m$ may be freely interpreted as relations $p_{\mathcal{A}} \subseteq \mathrm{T}_{\Sigma}^{m}$.

Proposition 3.12 *Every set of ground atoms I uniquely determines a Herbrand interpretation $\mathcal{A}$ via*

$$(s_1, \dots, s_n) \in p_{\mathcal{A}} \quad :\Leftrightarrow \quad p(s_1, \dots, s_n) \in I$$

Thus we shall identify Herbrand interpretations (over Σ) with sets of Σ-ground atoms.

Example: $\Sigma_{Pres} = (\{0/0, s/1, +/2\},\ \{</2, \leq/2\})$

$\mathbb{N}$ as Herbrand interpretation over Σ_{Pres}:

$$
\begin{array}{ll}
I = \{ & 0 \leq 0,\ 0 \leq s(0),\ 0 \leq s(s(0)),\ \ldots, \\
 & 0 + 0 \leq 0,\ 0 + 0 \leq s(0),\ \ldots, \\
 & \ldots,\ (s(0) + 0) + s(0) \leq s(0) + (s(0) + s(0)) \\
 & \ldots \\
 & s(0) + 0 < s(0) + 0 + 0 + s(0) \\
 & \ldots\}
\end{array}
$$

Existence of Herbrand Models

A Herbrand interpretation I is called a *Herbrand model* of F, if $I \models F$.

Theorem 3.13 (Herbrand) *Let N be a set of Σ-clauses.*

$$
\begin{array}{lll}
N \textit{ satisfiable} & \Leftrightarrow & N \textit{ has a Herbrand model (over } \Sigma) \\
 & \Leftrightarrow & G_\Sigma(N) \textit{ has a Herbrand model (over } \Sigma)
\end{array}
$$

where $G_\Sigma(N) = \{C\sigma \text{ ground clause} \mid C \in N,\ \sigma : X \to \mathrm{T}_\Sigma\}$ *is the set of* ground instances *of N.*

[The proof will be given below in the context of the completeness proof for resolution.]

Example of a G_Σ

For Σ_{Pres} one obtains for

$$C = (x < y) \vee (y \leq s(x))$$

the following ground instances:

$(0 < 0) \vee (0 \leq s(0))$
$(s(0) < 0) \vee (0 \leq s(s(0)))$
$\ldots$
$(s(0) + s(0) < s(0) + 0) \vee (s(0) + 0 \leq s(s(0) + s(0)))$
$\ldots$

3.8 Inference Systems and Proofs

Inference systems Γ (proof calculi) are sets of tuples

$$(F_1, \dots, F_n, F_{n+1}),\ n \geq 0,$$

called *inferences* or *inference rules*, and written

$$\frac{\overbrace{F_1\ \dots\ F_n}^{\text{premises}}}{\underbrace{F_{n+1}}_{\text{conclusion}}}\ .$$

Clausal inference system: premises and conclusions are clauses. One also considers inference systems over other data structures (cf. below).

Proofs

A *proof* in Γ of a formula F from a a set of formulas N (called *assumptions*) is a sequence $F_1, \dots, F_k$ of formulas where

(i) $F_k = F$,

(ii) for all $1 \leq i \leq k$: $F_i \in N$, or else there exists an inference

$$\frac{F_{i_1}\ \dots\ F_{i_{n_i}}}{F_i}$$

in Γ, such that $0 \leq i_j < i$, for $1 \leq j \leq n_i$.

Soundness and Completeness

Provability $\vdash_\Gamma$ of F from N in Γ: $N \vdash_\Gamma F$ $:\Leftrightarrow$ there exists a proof Γ of F from N.

Γ is called *sound* $:\Leftrightarrow$

$$\frac{F_1\ \dots\ F_n}{F} \in \Gamma \quad \Rightarrow \quad F_1, \dots, F_n \models F$$

Γ is called *complete* $:\Leftrightarrow$

$$N \models F \quad \Rightarrow \quad N \vdash_\Gamma F$$

Γ is called *refutationally complete* $:\Leftrightarrow$

$$N \models \bot \quad \Rightarrow \quad N \vdash_\Gamma \bot$$

Proposition 3.14

(i) Let Γ *be sound. Then* $N \vdash_\Gamma F \Rightarrow N \models F$

(ii) $N \vdash_\Gamma F \Rightarrow$ *there exist* $F_1, \ldots, F_n \in N$ *s.t.* $F_1, \ldots, F_n \vdash_\Gamma F$ *(resembles compactness).*

Proofs as Trees

markings	$\widehat{=}$	formulas			
leaves	$\widehat{=}$	assumptions and axioms			
other nodes	$\widehat{=}$	inferences:	conclusion	$\widehat{=}$	ancestor
			premises	$\widehat{=}$	direct descendants

$$\dfrac{P(f(c)) \qquad \dfrac{\dfrac{\dfrac{P(f(c)) \vee Q(b) \qquad \dfrac{\dfrac{P(f(c)) \vee Q(b) \quad \neg P(f(c)) \vee \neg P(f(c)) \vee Q(b)}{\neg P(f(c)) \vee Q(b) \vee Q(b)}}{\neg P(f(c)) \vee Q(b)}}{Q(b) \vee Q(b)}}{Q(b)} \qquad \neg P(f(c)) \vee \neg Q(b)}{\neg P(f(c))}}{\bot}$$

3.9 Propositional Resolution

We observe that propositional clauses and ground clauses are the same concept.

In this section we only deal with ground clauses.

The Resolution Calculus *Res*

Resolution inference rule:

$$\frac{D \vee A \qquad \neg A \vee C}{D \vee C}$$

Terminology: $D \vee C$: *resolvent*; A: *resolved atom*

(Positive) factorisation inference rule:

$$\frac{C \vee A \vee A}{C \vee A}$$

These are *schematic inference rules*; for each substitution of the *schematic variables* C, D, and A, respectively, by ground clauses and ground atoms we obtain an inference rule.

As "$\vee$" is considered associative and commutative, we assume that A and $\neg A$ can occur anywhere in their respective clauses.

Sample Refutation

1.	$\neg P(f(c)) \vee \neg P(f(c)) \vee Q(b)$	(given)
2.	$P(f(c)) \vee Q(b)$	(given)
3.	$\neg P(g(b,c)) \vee \neg Q(b)$	(given)
4.	$P(g(b,c))$	(given)
5.	$\neg P(f(c)) \vee Q(b) \vee Q(b)$	(Res. 2. into 1.)
6.	$\neg P(f(c)) \vee Q(b)$	(Fact. 5.)
7.	$Q(b) \vee Q(b)$	(Res. 2. into 6.)
8.	$Q(b)$	(Fact. 7.)
9.	$\neg P(g(b,c))$	(Res. 8. into 3.)
10.	$\bot$	(Res. 4. into 9.)

Resolution with Implicit Factorization RIF

$$\frac{D \vee A \vee \ldots \vee A \qquad \neg A \vee C}{D \vee C}$$

1.	$\neg P(f(c)) \vee \neg P(f(c)) \vee Q(b)$	(given)
2.	$P(f(c)) \vee Q(b)$	(given)
3.	$\neg P(g(b,c)) \vee \neg Q(b)$	(given)
4.	$P(g(b,c))$	(given)
5.	$\neg P(f(c)) \vee Q(b) \vee Q(b)$	(Res. 2. into 1.)
6.	$Q(b) \vee Q(b) \vee Q(b)$	(Res. 2. into 5.)
7.	$\neg P(g(b,c))$	(Res. 6. into 3.)
8.	$\bot$	(Res. 4. into 7.)

Soundness of Resolution

Theorem 3.15 *Propositional resolution is sound.*

Proof. Let $I \in \Sigma\text{-}\mathsf{Alg}$. To be shown:

(i) for resolution: $I \models D \vee A,\ I \models C \vee \neg A \;\Rightarrow\; I \models D \vee C$

(ii) for factorization: $I \models C \vee A \vee A \;\Rightarrow\; I \models C \vee A$

(i): Assume premises are valid in I. Two cases need to be considered:
If $I \models A$, then $I \models C$, hence $I \models D \vee C$.
Otherwise, $I \models \neg A$, then $I \models D$, and again $I \models D \vee C$.
(ii): even simpler. $\square$

Note: In propositional logic (ground clauses) we have:

1. $I \models L_1 \vee \ldots \vee L_n \;\Leftrightarrow\;$ there exists i: $I \models L_i$.
2. $I \models A$ or $I \models \neg A$.

This does not hold for formulas with variables!

3.10 Well-Founded Orderings

Literature: Franz Baader and Tobias Nipkow: *Term rewriting and all that*, Cambridge Univ. Press, 1998, Chapter 2.

To show the refutational completeness of resolution, we will make use of the concept of well-founded orderings.

Partial Orderings

A *(strict) partial ordering* $\succ$ on a set M is a transitive and irreflexive binary relation on M.

An $a \in M$ is called *minimal*, if there is no b in M such that $a \succ b$.

An $a \in M$ is called *smallest*, if $b \succ a$ for all $b \in M$ different from a.

Notation:
$\prec$ for the inverse relation $\succ^{-1}$
$\succeq$ for the reflexive closure $(\succ \cup =)$ of $\succ$

Well-Foundedness

A (strict) partial ordering $\succ$ is called *well-founded (Noetherian)*, if there is no infinite descending chain $a_0 \succ a_1 \succ a_2 \succ \dots$ with $a_i \in M$.

Well-Founded Orderings: Examples

Natural numbers. $(\mathbb{N}, >)$

Lexicographic orderings. Let $(M_1, \succ_1), (M_2, \succ_2)$ be well-founded orderings. Then let their *lexicographic combination*

$$\succ = (\succ_1, \succ_2)_{lex}$$

on $M_1 \times M_2$ be defined as

$$(a_1, a_2) \succ (b_1, b_2) \quad :\Leftrightarrow \quad a_1 \succ_1 b_1, \text{ or else } a_1 = b_1 \;\&\; a_2 \succ_2 b_2$$

(analogously for more than two orderings)

This again yields a well-founded ordering (proof below).