Decision Procedures

An Algorithmic Point of View

Equalities and Uninterpreted Functions

D. Kroening O. Strichman

ETH/Technion

Version 1.0, 2007

Part III

Equalities and Uninterpreted Functions

Outline

- A Boolean combination of Equalities and Propositions

$$x_1 = x_2 \wedge (x_2 = x_3 \vee \neg((x_1 = x_3) \wedge b \wedge x_1 = 2))$$

- We always push negations inside (NNF):

$$x_1 = x_2 \wedge (x_2 = x_3 \vee ((x_1 \neq x_3) \wedge \neg b \wedge x_1 \neq 2))$$

$$
\begin{array}{lcl}
\mathit{formula} & : & \mathit{formula} \vee \mathit{formula} \\
 & | & \neg \mathit{formula} \\
 & | & \mathit{atom} \\
 & & \\
\mathit{atom} & : & \mathit{term\text{-}variable} = \mathit{term\text{-}variable} \\
 & | & \mathit{term\text{-}variable} = \mathit{constant} \\
 & | & \mathit{Boolean\text{-}variable}
\end{array}
$$

- The *term-variables* are defined over some (possible infinite) domain. The constants are from the same domain.
- The set of Boolean variables is always separate from the set of term variables

- Allows more natural description of systems, although technically it is as expressible as Propositional Logic.
- Obviously NP-hard.
- In fact, it is in NP, and hence NP-complete, for reasons we shall see later.

$$
\begin{array}{lcl}
\mathit{formula} & : & \mathit{formula} \lor \mathit{formula} \\
 & | & \neg \mathit{formula} \\
 & | & \mathit{atom} \\
 & & \\
\mathit{atom} & : & \mathit{term} = \mathit{term} \\
 & | & \mathit{Boolean\text{-}variable} \\
 & & \\
\mathit{term} & : & \mathit{term\text{-}variable} \\
 & | & \mathit{function}\,(\,\text{list of } \mathit{terms}\,)
\end{array}
$$

The *term-variables* are defined over some (possible infinite) domain.
Constants are functions with an empty list of terms.

- Every function is a mapping from a domain to a range.
- Example: the '$+$' function over the naturals $\mathbb{N}$ is a mapping from $\langle \mathbb{N} \times \mathbb{N} \rangle$ to $\mathbb{N}$.

- Suppose we replace '$+$' by an uninterpreted binary function $f(a, b)$
- Example:

$$x_1 + x_2 = x_3 + x_4 \quad \text{is replaced by} \quad f(x_1, x_2) = f(x_3, x_4)$$

- We lost the 'semantics' of '$+$', as f can represent any binary function.

- 'Loosing the semantics' means that f is not restricted by any axioms or rules of inference.
- But f is still a function!

- The most general axiom for any function is functional consistency.
- Example: if $x = y$, then $f(x) = f(y)$ for any function f.

- Functional consistency axiom schema:

$$x_1 = x_1' \wedge \ldots \wedge x_n = x_n' \quad \Longrightarrow \quad f(x_1, \ldots, x_n) = f(x_1', \ldots, x_n')$$

- Sometimes, functional consistency is all that is needed for a proof.