Chapter 3

Reals

DECISION PROCEDURES
LAST UPDATE OF LECTURE NOTES: TUESDAY, MARCH 7, 2006
LAST UPDATE OF THIS CHAPTER: WEDNESDAY, FEBRUARY 1, 2006

3.1 The modelclass

3.1.1 Definition
The SIGNATURE OF REALS Σ_{real} contains the following symbols:

- The sort real for real numbers.
- A constant symbol c_r of sort real, for all rational numbers $r \in \mathbb{Q}$.
- The binary infix predicate symbol $+$ (*addition*), of arity $\mathsf{real} \times \mathsf{real} \to \mathsf{real}$.
- The unary function symbol $-$ (*unary minus*), of arity $\mathsf{real} \to \mathsf{real}$.
- The binary function symbol $\times$ (*multiplication*), of arity $\mathsf{real} \times \mathsf{real} \to \mathsf{real}$.
- The binary infix predicate symbol $<$ (*strict ordering*), of arity $\mathsf{real} \times \mathsf{real}$.
- The binary infix predicate symbol $\leq$ (*weak ordering*), of arity $\mathsf{real} \times \mathsf{real}$.

3.1.2 Definition
The STANDARD real-STRUCTURE is the unique Σ_{real}-structure $\mathcal{A}$ satisfying the following properties:

1. $A_{\mathsf{real}} = \mathbb{R}$.
2. $c_r^{\mathcal{A}} = r$, for all rational numbers $r \in \mathbb{Q}$.
3. The symbols $+$, $-$, $\times$, $<$, and $\leq$ are interpreted according to their standard interpretation over $\mathbb{R}$.

3.1.3 Definition
The MODELCLASS OF REALS is the pair $M_{\mathsf{real}} = (\Sigma_{\mathsf{real}}, \mathbf{A})$, where $\mathbf{A}$ is the class of all Σ_{real}-structures that are isomorphic to the standard real-structure.

3.1.4 Notation
When writing Σ_{real}-terms, we follow the following conventions:

- For every rational number $r \in \mathbb{Q}$, the constant c_r is written directly as r.
- The term $s - t$ is a shorthand for $s + (-t)$.
- The term st is a shorthand for $s \times t$.
- Since the addition and multiplication of real numbers are associative, we drop the parenthesis when writing Σ_{real}-terms like $s + t + u$ or stu.

3.1.5 Definition
The set of LINEAR Σ_{real}-terms is the smallest set of Σ_{real}-terms satisfying the following properties.

1. Every variable or constant symbol of sort real is a linear Σ_{real}-term.
2. If s and t are linear Σ_{real}-terms then $s + t$ is a linear Σ_{real}-term.
3. If c is a constant symbol of sort real and t is a linear Σ_{real}-term then ct and tc are linear Σ_{real}-terms.

3.1.6 Definition
A quantifier-free Σ_{real}-formula is LINEAR if all terms occurring in it are linear.

3.1.7 Proposition
For every conjunction Γ of linear Σ_{real}-literals, and for every disjunction of the form $\bigvee_{i=1}^{n} s_i \approx t_i$, where the s_i, t_i are linear Σ_{real}-terms, we have

$$\Gamma \rightarrow \bigvee_{i=1}^{n} s_i \approx t_i \text{ is } M_{\mathsf{real}}\text{-valid} \quad \Longleftrightarrow \quad \Gamma \rightarrow s_j \approx t_j \text{ is } M_{\mathsf{real}}\text{-valid, for some } j\,.$$

3.2 Gaussian elimination

3.2.1 Algorithm (IS-SATISFIABLE-GAUSS)
Input: A finite set Γ of linear Σ_{real}-literals of the form $s \approx t$ and $s \not\approx t$
Output: `satisfiable` if Γ is satisfiable; `unsatisfiable` otherwise

function IS-SATISFIABLE-GAUSS(Γ)
  while *true* **do**
    Simplify Γ, so that all literals in it become of the form

$$a_1x_1 + \cdots + a_nx_n + b \approx 0\,, \qquad a_1x_1 + \cdots + a_nx_n + b \not\approx 0\,,$$

    where $n \geq 0$, the a_i are nonzero constant symbols, the x_i are variables, and b is a constant symbol

4: **while** Γ contains a ground literal ℓ **do**
5: **if** $(\ell \equiv b \approx 0$ and $b \neq 0)$ or $(\ell \equiv b \not\approx 0$ and $b = 0)$ **then**
6: **return** `unsatisfiable`
7: **else**
8: $\Gamma \leftarrow \Gamma \setminus \{\ell\}$
9: **end if**
10: **end while**
11: **if** all literals in Γ are of the form $a_1x_1 + \cdots + a_nx_n + b \not\approx 0$ **then**
12: **return** `satisfiable`
13: **end if**
14: Let $\Gamma = \Delta \cup \{a_1x_1 + \ldots + a_nx_n \approx 0\}$, and construct the substitution

$$\sigma = \left\{ x_1 / - \frac{a_2}{a_1}x_2 - \ldots - \frac{a_n}{a_1}x_n - \frac{b}{a_1} \right\}$$

15: $\Gamma \leftarrow \Delta\sigma$
16: **end while**
17: **end function**

3.2.2 Proposition
Algorithm IS-SATISFIABLE-GAUSS *is terminating.*

PROOF. Notice that, for every iteration of the **while** loop at line 2, either the algorithm ends at line 6 or 12, or the value of $|vars(\Gamma)|$ strictly decreases because the assignment at line 15 removes the variable x_1. It follows that the number of iterations of the **while** loop at line 2 is finite, which implies termination of the algorithm.

3.2.3 Proposition
In Algorithm IS-SATISFIABLE-GAUSS*, every modification of* Γ *preserves* M_{real}*-satisfiability.*

PROOF. Γ is modified at lines 3, 8, and 15. The modification at line 3 clearly preserves M_{real}-equivalence, and therefore it also preserves M_{real}-satisfiability.

Concerning the modification at line 8, we have that the literal ℓ is M_{real}-equivalent to *true*, implying that this modification also preserves M_{real}-equivalence, and therefore it also preserves M_{real}-satisfiability.

Concerning the modification at line 16, let

$$\Gamma = \Delta \cup \{a_1x_1 + \cdots a_nx_n + b \approx 0\},$$

and let

$$\Gamma' = \Delta\sigma$$

where

$$\sigma = \left\{ x_1 / - \frac{a_2}{a_1}x_2 - \ldots - \frac{a_n}{a_1}x_n - \frac{b}{a_1} \right\}$$

We want to show that Γ and Γ' are M_{real}-equisatisfiable.

Clearly, if Γ is M_{real}-satisfiable then Γ' is M_{real}-satisfiable. Viceversa, assume that Γ' is M_{real}-satisfiable, and let $\mathcal{A}$ be a M_{real}-interpretation over $vars(\Gamma')$ such that $\mathcal{A} \models \Gamma'$. Let $\mathcal{B}$ be the M_{real}-interpreation over $vars(\Gamma) = vars(\Gamma') \cup \{x_1\}$ that is defined as being exactly as $\mathcal{A}$, except that

$$x_1^{\mathcal{B}} = \left[-\frac{a_2}{a_1}x_2 - \ldots - \frac{a_n}{a_1}x_n - \frac{b}{a_1}\right]^{\mathcal{A}} .$$

By construction, $\mathcal{B} \models \Gamma$.

3.2.4 Proposition
Algorithm IS-SATISFIABLE-GAUSS *is partially correct.*

PROOF. Let Γ_0 be the value of Γ at the beginning of the algorithm, and let Γ_1 be the value of Γ at the end of the algorithm.

Assume that the algorithm ends at line 6 returning `unsatisfiable`. Then, Γ_1 contains a literal ℓ that is M_{real}-unsatisfiable. Thus, Γ_1 is unsatisfiable. By Proposition 3.2.3, Γ_0 is unsatisfiable.

If instead the algorithm ends at line 12, returning `satisfiable`, then Γ_1 is a finite set of literals of the form

$$a_1x_1 + \cdots a_nx_n + b \not\approx 0 ,$$

where $n > 0$. Since all these literals are M_{real}-satisfiable, by Proposition 3.1.7, it follows that Γ_1 is M_{real}-satisfiable. Therefore, by Proposition 3.2.3, Γ_0 is satisfiable.

3.2.5 Proposition
Algorithm IS-SATISFIABLE-GAUSS *is correct.*

PROOF. By Propositions 3.2.2 and 3.2.4.

3.3 Fourier-Motzkin

3.3.1 Algorithm (IS-SATISFIABLE-FOURIER-MOTZKIN**)**
Input: A finite set Γ of linear Σ_{real}-literals of the form $s \leq t$ and $s < t$
Output: `satisfiable` if Γ is satisfiable; `unsatisfiable` otherwise

function IS-SATISFIABLE-FOURIER-MOTZKIN(Γ)
  while *true* **do**
    Simplify Γ, so that all literals in it become of the form

$$a_1x_1 + \cdots + a_nx_n + b \leq 0 , \qquad a_1x_1 + \cdots + a_nx_n + b < 0 ,$$

    where $n \geq 0$, the a_i are nonzero constant symbols, the x_i are variables, and b is a constant symbol
    while Γ contains a ground literal ℓ **do**
      if ($\ell \equiv b \leq 0$ and $b > 0$) or ($\ell \equiv b < 0$ and $b \geq 0$) **then**

6: **return** `unsatisfiable`
7: **else**
8: $\Gamma \leftarrow \Gamma \setminus \{\ell\}$
9: **end if**
10: **end while**
11: **if** $\Gamma = \varnothing$ **then**
12: **return** `satisfiable`
13: **end if**
14: Pick a variable $x \in vars(\Gamma)$, and rewrite Γ so that we have

$$\Gamma = \Delta \cup \{s_i \leq x\}_i \cup \{s'_j < x\}_j \cup \{x \leq t_k\}_k \cup \{x < t'_h\}_h$$

where Δ does not contain x.
15: $\Gamma \leftarrow \Delta \cup \{s_i \leq t_k\}_{i,k} \cup \{s_i < t'_h\}_{i,h} \cup \{s'_j < t_k\}_{j,k} \cup \{s'_j < t'_h\}_{j,h}$
16: **end while**
17: **end function**

3.3.2 Proposition
Algorithm is-satisfiable-fourier-motzkin *is terminating.*

Proof. Notice that, for every iteration of the **while** loop at line 2, either the algorithm ends at line 6 or 12, or the value of $|vars(\Gamma)|$ strictly decreases because the assignment at line 15 removes the variable x. It follows that the number of iterations of the **while** loop at line 2 is finite, which implies termination of the algorithm.

3.3.3 Proposition
In Algorithm is-satisfiable-fourier-motzkin*, every modification of* Γ *preserves* M_{real}*-satisfiability.*

Proof. Γ is modified at lines 3, 8, 14, and 15. The modifications at lines 3 and 14 clearly preserve M_{real}-equivalence, and therefore they also preserve M_{real}-satisfiability.

Concerning the modification at line 8, we have that the literal ℓ is M_{real}-equivalent to *true*, implying that this modification also preserves M_{real}-equivalence, and therefore it also preserves M_{real}-satisfiability.

Concerning the modification at line 15, let

$$\Gamma = \Delta \cup \{s_i \leq x\}_i \cup \{s'_j < x\}_j \cup \{x \leq t_k\}_k \cup \{x < t'_h\}_h\,,$$

and let

$$\Gamma' = \Delta \cup \{s_i \leq t_k\}_{i,k} \cup \{s_i < t'_h\}_{i,h} \cup \{s'_j < t_k\}_{j,k} \cup \{s'_j < t'_h\}_{j,h}\,.$$

We want to show that Γ and Γ' are M_{real}-equisatisfiable.

Clearly, if Γ is M_{real}-satisfiable then Γ' is M_{real}-satisfiable. Viceversa, assume that Γ' is M_{real}-satisfiable, and let $\mathcal{A}$ be a M_{real}-interpretation over $vars(\Gamma')$ such that $\mathcal{A} \models \Gamma'$. Let $\mathcal{B}$ be the M_{real}-interpretation over $vars(\Gamma) = vars(\Gamma') \cup \{x\}$ that is defined as being exactly as $\mathcal{A}$, except that

$$x^{\mathcal{B}} = \frac{\min\left(\left\{(t_k)^{\mathcal{A}}\right\}_k \cup \left\{(t'_h)^{\mathcal{A}}\right\}_h\right) - \max\left(\left\{(s_i)^{\mathcal{A}}\right\}_i \cup \left\{(s'_j)^{\mathcal{A}}\right\}_j\right)}{2}.$$

By construction, $\mathcal{B} \models \Gamma$.

3.3.4 Proposition
Algorithm IS-SATISFIABLE-FOURIER-MOTZKIN *is partially correct.*

PROOF. Let Γ_0 be the value of Γ at the beginning of the algorithm, and let Γ_1 be the value of Γ at the end of the algorithm.

Assume that the algorithm ends at line 6 returning `unsatisfiable`. Then, Γ_1 contains a literal ℓ that is M_{real}-unsatisfiable. Thus, Γ_1 is unsatisfiable. By Proposition 3.3.3, Γ_0 is unsatisfiable.

If instead the algorithm ends at line 15, returning `satisfiable`, then $\Gamma_1 = \varnothing$. Thus, Γ_1 is M_{real}-satisfiable. By Proposition 3.3.3, Γ_0 is M_{real}-satisfiable.

3.3.5 Proposition
Algorithm IS-SATISFIABLE-FOURIER-MOTZKIN *is correct.*

PROOF. By Propositions 3.3.2 and 3.3.4.