Chapter 4

Integers

Decision Procedures
Last update of lecture notes: Tuesday, March 7, 2006
Last update of this chapter: Monday, February 27, 2006.

4.1 The modelclass

4.1.1 Definition
The signature of integers Σ_{int} contains the following symbols:

- The sort int for integer numbers.
- A constant symbol c_m of sort int, for all integer numbers $m \in \mathbb{Z}$.
- The binary infix predicate symbol $+$ (*addition*), of arity $\mathsf{real} \times \mathsf{real} \to \mathsf{real}$.
- The unary function symbol $-$ (*unary minus*), of arity $\mathsf{real} \to \mathsf{real}$.
- For each integer $k \in \mathbb{Z}$, a unary function symbol $k \times \bullet$ (*scalar multiplication*), of arity $\mathsf{real} \to \mathsf{real}$.
- For each positive integer $k \in \mathbb{Z}^+$, a unary predicate symbol $k \mid \bullet$ (*divisibility*), of arity real.
- The binary infix predicate symbol $<$ (*strict ordering*), of arity $\mathsf{real} \times \mathsf{real}$.

4.1.2 Definition
The standard int-structure is the unique Σ_{int}-structure $\mathcal{A}$ satisfying the following properties:

1. $A_{\mathsf{int}} = \mathbb{Z}$.
2. $c_m^{\mathcal{A}} = m$, for all integer numbers $m \in \mathbb{Z}$.
3. The symbols $+$, $-$, $\times$, $|$, and $<$ are interpreted according to their standard interpretation over $\mathbb{Z}$.

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

4.2 Cooper

4.2.1 Algorithm (ELIMINATE-VARIABLE-COOPER)
Input: A quantifier-free Σ_{int}-formula $F(x)$
Output: A quantifier-free Σ_{int}-formula $F^{-\infty}$ that is M_{int}-equivalent to $(\exists_{\mathsf{int}}\ x)F(x)$, and such that $vars(F^{-\infty}) = vars(F(x)) \setminus \{x\}$

function ELIMINATE-VARIABLE-COOPER($F(x)$)

Convert $F(x)$ in positive normal form.

Replace each literal in $F(x)$ of the form

$$s = t\,, \qquad \neg(s = t)\,, \qquad \neg(s < t)$$

with M_{int}-equivalent formulae involving only $<$. This can be done by means of the following rewrite rules

$$\begin{array}{lcl} s = t & \Longrightarrow & s < t+1 \ \wedge \ t < s+1\,, \\ \neg(s = t) & \Longrightarrow & s < t \ \vee \ t < s\,, \\ \neg(s < t) & \Longrightarrow & t < s+1\,. \end{array}$$

At the end of this instruction, all literals in $F(x)$ will be of the form

$$s < t\,, \qquad k \mid t\,, \qquad \neg(k \mid t)\,.$$

By opportunely collecting all terms involving x, rewrite $F(x)$ so that each literal in it either does not contain x, or is of the form

$$kx < t\,, \qquad t < kx\,, \qquad k \mid hx + t\,, \qquad \neg(k \mid hx + t)\,,$$

where t does not involve x.

Let δ' be the least common multiple of the coefficients of x in $F(x)$. Multiply all atoms in $F(x)$ by opportune constants, so that δ' becomes the coefficient of all occurrences of x. Finally, replace $(\exists_{\mathsf{int}}\ x)F(\delta' x)$ with $(\exists_{\mathsf{int}}\ x)(F(x) \wedge \delta' \mid x)$.
The result is a formula in positive normal form whose literals involving x are of the form

(A) $x < a_i$,

(B) $b_i < x$,

(C) $h_i \mid x + c_i$,

(D) $\neg(k_i \mid x + d_i)$

where the a_i, b_i, c_i, and d_i are terms not involving x.

6: Let δ be the least common multiple of all the h_i and k_i. Denote with $F_{-\infty}(x)$ the formula obtained from $F(x)$ by replacing all literals of the form (A) with `true`, and all literals of the form (B) with `false`. Return the formula

$$F^{-\infty}: \bigvee_{j=1}^{\delta} F_{-\infty}(j) \vee \bigvee_{j=1}^{\delta} \bigvee_{b_i} F(b_i + j)\,.$$

7: **end function**

4.2.2 Proposition

Let F be a quantifier-free formula in positive normal form, and let $\mathcal{A}, \mathcal{B}$ be interpretations such that $F^{\mathcal{A}} =$ true and $F^{\mathcal{B}} =$ false. Then there exists a literal ℓ in F such that $\ell^{\mathcal{A}} =$ true and $\ell^{\mathcal{B}} =$ false.

Proof. By structural induction on F.

4.2.3 Proposition

In Algorithm eliminate-variable-cooper*, let $F(x)$ be the formula obtained at the end of line 5. Let $\mathcal{A}$ be any M_{int}-interpretation. Then there exists an integer ν such that*

$$[F(x)]^{\mathcal{A}\circ\{x/n\}} = [F_{-\infty}(x)]^{\mathcal{A}\circ\{x/n\}}\,, \qquad \textit{for all } n < \nu\,.$$

Proof. We proceed by structural induction on $F(x)$.

For the base case, if $F(x)$ is a literal of the form $a_i < x$ then $F_{-\infty}(x)$ is `false`, and it suffices to take $\nu = s^{\mathcal{A}}$. If instead $F(x)$ is a literal of the form $x < b_i$ then $F_{-\infty}(x)$ is `true`, and it suffices to take $\nu = t^{\mathcal{A}}$. Finally, if $F(x)$ is a literal not containing x, or a literal of the form $h_i \mid x + c_i$ or $\neg(k_i \mid x + d_i)$, then $F(x)$ and $F_{-\infty}(x)$ are identical, and therefore they are M_{int}-equivalent.

For the inductive step, since $F(x)$ is in positive normal form, we need to consider only two cases, depending on whether the topmost connective of $F(x)$ is $\wedge$ or $\vee$. Thus, assume that $F(x)$ is of the form $G(x) \wedge H(x)$. By the inductive hypothesis, there exists integers ν_1 and ν_2 such that

$$[G(x)]^{\mathcal{A}\circ\{x/n\}} = [G_{-\infty}(x)]^{\mathcal{A}\circ\{x/n\}}\,, \qquad \text{for all } n < \nu_1\,.$$

and

$$[H(x)]^{\mathcal{A}\circ\{x/n\}} = [H_{-\infty}(x)]^{\mathcal{A}\circ\{x/n\}}\,, \qquad \text{for all } n < \nu_2\,.$$

But then, since $G_{-\infty}(x) \wedge H_{-\infty}(x)$ is identical to $F_{-\infty}(x)$, it suffices to take $\nu = \min(\nu_1, \nu_2)$.

The case in which $F(x)$ is of the form $G(x) \vee H(x)$ is similar to the one in which $F(x)$ is of the form $G(x) \wedge H(x)$.

4.2.4 Proposition

In Algorithm eliminate-variable-cooper*, let $F(x)$ be the formula obtained at the end of line 5. Let $\mathcal{A}$ be any M_{int}-interpretation, and let $n = x^{\mathcal{A}}$. Then*

$$[F_{-\infty}(x)]^{\mathcal{A}} = [F_{-\infty}(x)]^{\mathcal{A}\circ\{x/n+\lambda\delta\}}\,, \qquad \textit{for all } \lambda \in \mathbb{Z}\,.$$

PROOF. We proceed by structural induction on $F_{-\infty}(x)$.

For the base case, if $F_{-\infty}(x)$ is a literal then either it does not contain x, or it is of the form $h_i \mid x + c_i$ or $\neg(k_i \mid x + d_i)$. The case in which $F_{-\infty}(x)$ is a literal not containing x is trivial. If $F_{-\infty}(x)$ is a literal of the form $h_i \mid x + c_i$ or $\neg(k_i \mid x + d_i)$ then it suffices to note that $a \mid b$ if and only if $a \mid b + c$, for any integer a, b, c such that c is a multiple of a.

For the inductive step, if $F_{-\infty}(x)$ is of the form $G_{-\infty}(x) \wedge H_{-\infty}(x)$ then we have

$$[G_{-\infty}(x)]^{\mathcal{A}} = [G_{-\infty}(x)]^{\mathcal{A}\circ\{x/n+\lambda\delta\}}\,, \qquad \text{for all } \lambda \in \mathbb{Z}\,,$$

and

$$[H_{-\infty}(x)]^{\mathcal{A}} = [H_{-\infty}(x)]^{\mathcal{A}\circ\{x/n+\lambda\delta\}}\,, \qquad \text{for all } \lambda \in \mathbb{Z}\,.$$

Thus,

$$[G_{-\infty}(x) \wedge H_{-\infty}(x)]^{\mathcal{A}} = [G_{-\infty}(x) \wedge H_{-\infty}(x)]^{\mathcal{A}\circ\{x/n+\lambda\delta\}}\,, \quad \text{for all } \lambda \in \mathbb{Z}\,.$$

The case in which $F_{-\infty}(x)$ is of the form $G_{-\infty}(x) \vee H_{-\infty}(x)$ is similar to the one in which $F_{-\infty}(x)$ is of the form $G_{-\infty}(x) \wedge H_{-\infty}(x)$.

4.2.5 Proposition

In Algorithm ELIMINATE-VARIABLE-COOPER*, let $F(x)$ be the formula obtained at the end of line 5. Then $(\exists_{\mathsf{int}}\ x)F(x)$ and $F^{-\infty}$ are M_{int}-equivalent.*

PROOF. Let $\mathcal{A}$ be an M_{int}-interpretation such that $[F^{-\infty}]^{\mathcal{A}} = \mathit{true}$. If

$$\left[\bigvee_{j=1}^{\delta} \bigvee_{b_i} F(b_i + j)\right]^{\mathcal{A}} = \mathit{true}$$

then clearly

$$[(\exists_{\mathsf{int}}\ x)F(x)]^{\mathcal{A}} = \mathit{true}\,.$$

Otherwise, $[F_{-\infty}(j)]^{\mathcal{A}} = \mathit{true}$, for some $j \in \{1, \ldots, \delta\}$. But then, by Propositions 4.2.3 and 4.2.4, we have $[(\exists_{\mathsf{int}}\ x)F(x)]^{\mathcal{A}} = \mathit{true}$.

Vice versa, let $\mathcal{A}$ be an interpretation such that $[(\exists_{\mathsf{int}}\ x)F(x)]^{\mathcal{A}} = \mathit{true}$, and let n be an integer such that $[F(x)]^{\mathcal{A}\circ\{x/n\}} = \mathit{true}$. Also assume, for a contradiction, that $[F^{-\infty}]^{\mathcal{A}} = \mathit{false}$.

We claim that

$$[F(x)]^{\mathcal{A}\circ\{x/n-\delta\}} = \mathit{true}\,.$$

To see this, let $\mathcal{B} = \mathcal{A} \circ \{x/n - \delta\}$, and note that if $[F(x)]^{\mathcal{B}} = \mathit{false}$ then, by Proposition 4.2.2, there exists a literal ℓ in $F(x)$ such that $\ell^{\mathcal{A}} = \mathit{true}$ and $\ell^{\mathcal{B}} = \mathit{false}$. However, if ℓ does not contain x, or it is of the form $x < a_i$, $h_i \mid x + c_i$ or $\neg(k_i \mid d_i)$ then it must be $\ell^{\mathcal{A}} = \ell^{\mathcal{B}}$. If instead ℓ is of the form $b_i < x$, then we have $t^{\mathcal{A}} < n$ and $n - \delta \leq t^{\mathcal{A}}$. It follows that $t^{\mathcal{A}} < n \leq t^{\mathcal{A}} + \delta$, and therefore there exists an integer $j \in \{1, \ldots, \delta\}$ such that $[F(t+j)]^{\mathcal{A}} = \mathit{true}$. But then $[F^{-\infty}]^{\mathcal{A}} = \mathit{true}$, a contradiction.

Thus, we conclude that $[F(x)]^{\mathcal{A} \circ \{x/n-\delta\}} = \mathit{true}$, and iterating the same reasoning we can also conclude that

$$[F(x)]^{\mathcal{A} \circ \{x/n-\lambda\delta\}} = \mathit{true}\,, \qquad \text{for all } \lambda > 0\,.$$

But then, by Proposition 4.2.3, we have that $[F_{-\infty}(x)]^{\mathcal{A} \circ \{x/m\}} = \mathit{true}$, for some integer m sufficiently small. But then, by Proposition 4.2.4, it follows that

$$\left[\bigvee_{j=1}^{\delta} F_{-\infty}(j) \right]^{\mathcal{A}} = \mathit{true}\,,$$

and therefore $[F^{-\infty}]^{\mathcal{A}} = \mathit{true}$.

4.2.6 Proposition

In Algorithm ELIMINATE-VARIABLE-COOPER, $(\exists_{\mathsf{int}}\ x)F(x)$ *and* $F^{-\infty}$ *are* M_{int}*-equivalent.*

PROOF. Instructions at lines 2 thru 5 clearly preserve equivalence. Line 6 preserves equivalence by Proposition 4.2.5.