Slide 1

North American Summer School in Logic Language and Information, June 2003

Algorithmic Verification for Epistemic Logic

Ron van der Meyden

University of New South Wales/National ICT Australia

Slide 2

Model Checking Knowledge and Linear Time

Slide 3

References

Implementing Knowledge-based Programs, M.Y. Vardi, TARK 96

Model Checking Knowledge and Time in Systems with Perfect Recall, R. van der Meyden and N.V. Shilov, FST & TCS'99

Synthesis from Knowledge-Based Specifications. R. van der Meyden and M. Y. Vardi, CONCUR'98

Slide 4

Some results from temporal logic

Theorem: the following are PSPACE complete:

1. Given $\varphi \in \mathcal{L}_{\{\bigcirc, \mathcal{U}\}}$ determine if φ is satisfiable/valid.
2. Given $\varphi \in \mathcal{L}_{\{\bigcirc, \mathcal{U}\}}$ and a finite state environment E, determine if φ is realized in E.

Slide 5

Extend π_s by making p_s true just at s.

define

$$\varphi_E = \begin{array}{l} \bigwedge_{s \neq t} p_s \rightarrow \neg p_t \\ \wedge \bigwedge_s \Box(p_s \rightarrow \bigcirc \bigvee_{t \in T(s)} p_t) \\ \wedge \bigwedge_s \bigwedge_{p:\pi_e(s,p)=1} \Box(p_s \rightarrow p) \\ \wedge \bigwedge_s \bigwedge_{p:\pi_e(s,p)=0} \Box(p_s \rightarrow \neg p) \\ \wedge \bigvee_{s \in \alpha} \Box\Diamond p_s \end{array}$$

φ realized in E iff $\bigvee_{s \in I_e} p_s \wedge \varphi_E \wedge \neg\varphi$ is unsatisfiable

Slide 6

Realization (observational View)

The following can be obtained using techniques of [Vardi, TARK'96]:

Theorem: Realization of $\varphi \in \mathcal{L}_{\{K_1,\ldots,K_n,C,\bigcirc,\ \mathcal{U}\ \}}$ in a finite environment wrt the observational view is PSPACE complete.

Slide 7

Let $KF(\varphi)$ be the set of subformulas of φ of the form $K_i\psi$ or $C\varphi$

Let S' be the set of reachable states of E.

A *knowledge interpretation* is a function $\kappa : S' \rightarrow \mathcal{P}(KF(\varphi))$

Slide 8

An *execution* ε of an environment is a run, except it need not start at an initial state

Let κ be a knowledge interpretation

1. $E,\kappa,(\varepsilon,m) \models p$ if $\pi_e(\varepsilon(m),p) = 1$
2. $E,\kappa,(\varepsilon,m) \models \bigcirc\psi$ if $E,\kappa,(\varepsilon,m+1) \models \psi$
3. $E,\kappa,(\varepsilon,m) \models \psi_1\ \mathcal{U}\,\psi_2$ if there exists $m' > m$ such that $E,\kappa,(\varepsilon,m') \models \psi_2$ and $E,\kappa,(\varepsilon,k) \models \psi_1$ for $m \leq k < m'$.
4. $E,\kappa,(\varepsilon,m) \models K_i\psi$ iff $K_i\psi \in \kappa(\varepsilon(m))$
5. $E,\kappa,(\varepsilon,m) \models C\psi$ iff $C\psi \in \kappa(\varepsilon(m))$

Slide 9

κ is *consistent* if for all states s

1. for $K_i\psi \in KF(\varphi)$, $K_i\psi \in \kappa(s)$ iff for all states t such that $s\mathcal{K}_i t$, for all executions ε of E with $\varepsilon(0) = t$, we have $E, \kappa, (\varepsilon(0), 0) \models \psi$
2. for $C\psi \in KF(\varphi)$, $C\psi \in \kappa(s)$ iff for all states t such that $s\mathcal{K}_C t$, for all executions ε of E with $\varepsilon(0) = t$, we have $E, \kappa, (\varepsilon(0), 0) \models \psi$

Slide 10

Proposition: There exists a unique consistent knowledge interpretation κ and it can be computed in PSPACE

Proposition: φ is realized in E with respect to $\mathtt{obs}$ iff all runs ε of E satisfy $E, \kappa, (\varepsilon, 0) \models \varphi$, where κ is the unique consistent knowledge interpretation.

Slide 11

Realization (Synchronous Perfect Recall View)

Theorem: Realization of $\varphi \in \mathcal{L}_{\{K_1,\ldots,K_n,C,\bigcirc,\ \mathcal{U}\ \}}$ in a finite environment wrt the synchronous perfect recall view is undecidable.

Theorem: Realization of $\varphi \in \mathcal{L}_{\{K_1,\ldots,K_n,C,\bigcirc\}}$ in a finite environment wrt the synchronous perfect recall view is PSPACE complete.

Slide 12

Theorem: Realization of a formula $\varphi \in \mathcal{L}_{\{K_1,\ldots,K_n,\bigcirc,\ \mathcal{U}\ \}}$ of knowledge depth k in a finite environment E wrt the synchronous perfect recall view is decidable in space polynomial in $C_k(E) \cdot |\varphi|$.

Slide 13

Let E be $\langle S_e, I_e, T, O, \pi_e, \alpha \rangle$ and $k \geq 0$.

Define $A_k(E) = \langle S_k, I_k, T_k, \alpha_k \rangle$ to be the Büchi automaton with

1. S_k equal to the set $\mathcal{T}_k$ of k-trees over E,
2. initial states I_k equal to the set of k-trees $F_k(s)$ where $s \in I$,
3. transition relation T_k defined by wT_kw' when there exists state $s \in S$ such that $root(w)Ts$ and $w' = G_k(w,s)$,
4. acceptance condition α_k defined by $\alpha_k = \{w \in S_k : root(w) \in \alpha\}$.

$A_k(E)$ accepts sequences of k-trees.

Slide 14

Given a run ε of E, define $Lift_k(\varepsilon)$ to be the sequence of k-trees $w_0w_1\ldots$ such that $w_0 = F_k(\varepsilon(0))$ and $w_{m+1} = G_k(w_m, \varepsilon(m+1))$ for all $m \geq 0$.

Proposition: $Lift_k$ is a bijection between the runs of E and the ω-language accepted by $A_k(E)$.

Slide 15

Let e be an infinite sequence of k-trees. Define

- $E,(e,m) \models_k p$, where $p \in Prop$, iff $\pi_e(root(e(m)), p) = 1$,
- $E,(e,m) \models_k \varphi_1 \wedge \varphi_2$, iff $E,(e,m) \models_k \varphi_1$ and $E,(e,m) \models_k \varphi_2$,
- $E,(e,m) \models_k \neg\varphi$, iff not $E,(e,m) \models_k \varphi$,
- $E,(e,m) \models_k \bigcirc\varphi$, iff $E,(e,m+1) \models_k \varphi$,
- $E,(e,m) \models_k \varphi_1 \mathcal{U} \varphi_2$, iff there exists $m'' \geq m$ such that $E,(e,m'') \models_k \varphi_2$ and $E,(e,m') \models_k \varphi_1$ for all m' with $m \leq m' < m''$.

Slide 16

Let $\varphi \in \mathcal{L}_{\{K_1,\ldots,K_n,\bigcirc,\mathcal{U}\}}$.

First define $\models_k$ on k-trees w by:

$E, w \models_k K_i\varphi$ if for all $k-1$-trees w' that are i-children of w, and for all fair executions e of $A_{k-1}(E)$ such that $e(0) = w'$, we have $E,(e,0) \models_{k-1} \varphi$.

Now define

$E,(e,m) \models_k K_i\varphi$ if $E, e(m) \models_k K_i\varphi$.

Slide 17

Proposition: For each natural number $k \geq 0$, each formula φ in $\mathcal{L}_{\{\bigcirc,\mathcal{U},K_1,\ldots K_n\}}$ of knowledge depth at most k, for each environment E, every run ε of E and $m \geq 0$ we have

$$I^{\mathtt{spr}}(E),(\varepsilon^{\mathtt{spr}},m) \models \varphi \quad \text{iff} \quad E,(Lift_k(\varepsilon),m) \models_k \varphi.$$

Slide 18

Key Observation:

If φ is a formula of temporal logic, determining $E,w \models_k K_i\varphi$, i.e,

> for all $k-1$-trees w' that are i-children of w, and for all fair executions e of $A_{k-1}(E)$ such that $e(0) = w'$, we have $E,(e,0) \models_{k-1} \varphi$.

reduces to the realization problem of temporal logic once we have computed $E,u \models_{k-1} K_j\psi$ for all proper subformulae $K_j\psi$ of φ.

Slide 19

Realizability

A formula φ is *realizable* in an environment E with respect to a view v if there exists a protocol $\mathbf{P}$ such that for all runs r of $I^v(E,\mathbf{P})$, we have

$$I^v(E,\mathbf{P}),(r,0) \models \varphi$$

Slide 20

Synthesis

Theorem: [van der Meyden and Vardi, CONCUR 98] Let E be an environment for a single agent. There is an algorithm that decides whether a formula $\psi \in \mathcal{L}_{\{K_1,\bigcirc,\mathcal{U}\}}$ is realizable in E with respect to the synchronous perfect recall view in time

$$2^{O(||E||)} \cdot 2^{2^{O(||\psi||)}}$$

The bound is tight, because

Theorem (Pnueli and Rosner 1989): Realizability of temporal logic

Slide 21

formulae with complete information is 2-EXPTIME hard.