LOGIC OF KNOWLEDGE AND TIME

Seminar Report
Mohsin Ahmed
Guide: Dr. G.Venkatesh

Department of Computer Science and Engineering
Indian Institute of Technology, Bombay
June 13, 2020

Abstract

This seminar report summarizes two possible research problems, one of which is to be taken up for further research.

The first problem involves combining a first order theory with first order temporal logic to increase expressive power without losing decidability. Though first order logic itself is undecidable, there are a number of useful first order theories which are decidable. Similarly first order temporal logic is undecidable and incomplete, but it may have decidable theories. Specifically, we believe first order temporal theories of Presburger arithmetic and real closed fields will be useful in reasoning about motion, and hence investigation of their decidability is of interest.

The second problem deals with the issue of evolving a logical system for knowledge representation which takes time and belief into account. The present modal system for reasoning about knowledge has serious drawbacks of monotonicity and logical omniscience. æ

Contents

Chapter 1

Introduction

Reasoning about time and knowledge can be automated only when it is properly formulated in a mathematical theory. We propose modal and temporal extensions of several first order theories as a basis for reasoning about knowledge and time. The logics so obtained must be expressive enough to model time and knowledge elegantly and they should be decidable. The theory of presburger arithmetic and real closed fields along with temporal logic can be used to reason about motion. Their expressive power and decision procedures will be discussed here.

In chapter two, we review several classical and non classical logics necessary to define the problems. We define the syntax, semantics and terminology of the following logics: propositonal logic, first order logic, modal logic, and temporal logic.

Chapter three presents several useful theories and their properties. The theories of interest are those of presburger arithmetic and real closed fields. It is well known that the theory of numbers with addition and multiplication, is very expressive, but it is undecidable and incomplete. However, Presburger has shown that presburger arithmetic (the theory of natural numbers with only addition) is decidable by the method of quantifier elimination [End 72]. The theory of real closed fields is the basis of axiomatic geometry, and its decidability can be shown by quantifier elimination. A non elementary decision procedure for real closed fields using quantifier elimination was given by Tarski [Tar 51]. Subsequently Collin's method of cylinderical algebraic decomposition decides theory of real closed fields in elementary time [Arn 88].

In general one could say that the issues of expressive power and decision complexity are complementary in nature, in the sense that increase in expressive power makes a theory harder to decide, leading to undecidability and finally to incompleteness.

Modal logic is useful in reasoning about knowledge. It has two modalities *box* $\Box$ and its dual *diamond* $\diamond$. The modal formula $\Box(\phi)$ has several meanings: ϕ is *necessary*, ϕ is *provable*, ϕ is *henceforth* true, ϕ is *known*, or ϕ is *true in all possible worlds* an agent knows about. The dual $\Diamond\phi$ would mean: ϕ is *possible*, ϕ is *consistent*, ϕ is *eventually* true, $\neg\phi$ is *not known*, or ϕ is *true in some possible worlds* an agent knows about.

Boolos [Boo 79] uses Lob's modal system $\mathcal{G}$ to reason about proofs and Gödel's second incompleteness theorem is reflected as a theorem of $\mathcal{G}$. In temporal logic Box ($\Box$) is stands for henceforth [Wol 83]. First order temporal logic is the combination of first order logic and temporal logic. First order temporal logic is expressive enough to finitely axiomatize the theory of natural numbers, and hence is incomplete and undecidable [Sza 87A, Sza 87B, Sza 88]. However restricting it suitably will result in useful logics.

Chapter four looks at first order temporal theory of presburger arithmetic and real closed fields, with applications in reasoning about motion. The tradeoff is between expressibility and ease in deciding. The factors to be considered are the model of the underlying geometry, the model of time, the language of predicates and functions, and the issues of completeness, axiomatization, finite axiomatization, and decidability. The theory should model facts about motion easily and there should be a practical decision procedure to decide a certain class of formulæ.

In chapter five, we consider the problem of knowledge representation from the theoretical point of view. In reasoning about knowledge [Hal 86], the present axiomatic modal system suffers from some serious drawbacks. First, the agent is assumed to be omniscient [Par 87]. That is, the agent (or knower) is assumed to know all the logical consequences of his knowledge. This is an unreasonable assumption about practical reasoners. Second, the agent can only reason monotonically [Sho 88]. Since he cannot revise his knowledge in face of contary evidence, he is expected to forsee all possible exceptions.

Third, the agent knows what it doesn't know [Leh 84] ! Fourth, common knowledge and self awareness is not properly handled. We will attempt to represent knowledge in a way that takes time and belief into account. æ

Chapter 2

Classical and Nonclassical Logics

In this chapter, we define the syntax and semantics of proposional, first order, modal, propositional temporal and first order temporal logics.

2.1 Terminology

The *Language* ($\mathcal{L}$) of a logic consists of logical and nonlogical constants together with a set of rules to generate a set of well formed formulæ ($wff(\mathcal{L})$). The logical constants have fixed meaning in a logic, while the nonlogical constants can have any interpretation.

$\mathcal{M}$ is called a *model* for a set Γ of formulæ ($\Gamma \subseteq wff(\mathcal{L})$) , if every $\phi \in \Gamma$ is interpreted as true in $\mathcal{M}$; written as $\models_{\mathcal{M}} \Gamma$. A set Γ *logically implies* ϕ (ϕ is a *logical consequence* of Γ), if ϕ is true in every model of Γ; written as $\Gamma \models \phi$. The set of logical consequences of Γ is denoted by $Cn(\Gamma) = \{\phi : \Gamma \models \phi\}$. A formula is *valid* if it is true in all models ($\models \phi$), and *unsatisfiable* if it has no models. It follows that ϕ is valid iff $\neg\phi$ is unsatisfiable.

A *theory* $\mathcal{T}$ is any set of sentences closed under logical consequences, that is $Cn(\mathcal{T}) = \mathcal{T}$. A *theory of a model* $\mathcal{M}$ is the set of sentences true in a model, denoted by $Th(\mathcal{M}) = \{\phi : \models_{\mathcal{M}} \phi\}$.

A theory $\mathcal{T}$ is *inconsistent* if it contains all formulæ in $wff(\mathcal{L})$, otherwise it is *consistent*. An inconsistent theory is unsatisfiable. It is *complete* if for every $\phi \in L$, ϕ or $\neg\phi$ is in $\mathcal{T}$. Clearly for any model $\mathcal{M}$, $Th(\mathcal{M})$ is complete.

A *rule of inference* (ROI), is a rule to deduce true formulæ from formulæ already known to be true. A *proof* of ϕ from Γ is a finite deduction of ϕ from Γ using the ROI, and is denoted by $\Gamma \vdash \phi$. The set of formulæ provable from Γ is denoted by $Pr(\Gamma) = \{\phi : \Gamma \vdash \phi\}$.

Theory $\mathcal{T}$ is (finitely) *axiomatizable* if there is a (finite) recursive set of axioms Ax, such that $Cn(Ax) = \mathcal{T}$. A theory $\mathcal{T}$ with axioms Ax is *sound* if $Pr(Ax) \subseteq \mathcal{T}$. $\mathcal{T}$ is *partially decidable* (a recursively enumerable set), iff there is a recursive set of axioms $Ax : Cn(Ax) = \mathcal{T}$. It is *decidable* if $\mathcal{T}$ is a recursive set[1]. Clearly, a partially decidable complete theory is decidable.

A logic is *compact*, if whenever $\Gamma \models \phi$ then there is $\Gamma_{finite} \subseteq \Gamma : \Gamma_{finite} \models \phi$. A theory T has *finite model property* (fmp), when every sentence not in $\mathcal{T}$ can be falsified in a finite model. If a complete theory has finite model property, then we can decide if a sentence is not in it by enumerating finite models till we find a model falsifying the sentence. Thus a complete theory having fmp is decidable, and so a partially decidable theory having fmp.

2.2 Classical Logics

In this section we present [Bar 77, End 72, Rog 71] propositional logic (PL) and first order logic (FOL).

2.2.1 Proposition Logic

The language of PL (L_{PL}) has the following logical symbols: logical operators $\{\neg, \wedge, \vee, \rightarrow, \leftrightarrow\}$ standing for (not, and, or, implies, iff) respectively, and the truth constants $\top$ (true) and $\perp$ (false). The nonlogical symbols are a set $Prop = \{p_i\}$ of propositions, where the subscripts will denote any convenient enumeration. The set of formulae is the closure of $Prop$ and truth constants under the logical operations.

[1]We assume Church's thesis

A structure $\mathcal{M}$ is a function assigning truth values to $\phi \in wff(L_{PL})$, as given below.

$$\models_{\mathcal{M}} (\top) \tag{2.1}$$
$$\models_{\mathcal{M}} p_i \quad \text{iff} \quad \mathcal{M} : p_i \mapsto \top \tag{2.2}$$
$$\models_{\mathcal{M}} \neg\phi \quad \text{iff} \quad \not\models_{\mathcal{M}} \phi \tag{2.3}$$
$$\models_{\mathcal{M}} \phi \to \psi \quad \text{iff} \quad \not\models_{\mathcal{M}} \phi \text{ or } \models_{\mathcal{M}} \psi \tag{2.4}$$

Other operators and truth constants are defined as follows:

$$\bot \stackrel{\text{def}}{=} \neg\top \tag{2.5}$$
$$\phi \vee \psi \stackrel{\text{def}}{=} \neg\phi \to \psi \tag{2.6}$$
$$\phi \wedge \psi \stackrel{\text{def}}{=} \neg(\phi \to \neg\psi) \tag{2.7}$$
$$\phi \leftrightarrow \psi \stackrel{\text{def}}{=} (\phi \to \psi) \wedge (\psi \to \phi). \tag{2.8}$$

A PL formula is a *tautology* if it is true in every model. The ROI used is *detachment*: from ϕ and $\phi \to \psi$, derive ψ. PL is compact, finitely axiomatizable and decidable in polynomial space and exponential time.

2.2.2 First Order Logic

The language of FOL (L_{FOL}) has the following logical symbols: logical operators $\{\neg, \wedge, \vee, \to, \leftrightarrow\}$, quantifiers $\forall$ (for all) and $\exists$ (there exists), equality $=$, a set $X = \{x_i\}$ of variables, truth constants $\{\top, \bot\}$, The nonlogical symbols are sets $Const = \{c_i\}$ of constants, $Pred = \{p_i^n\}$ of predicates and $Func = \{f_i^n\}$ of functions, where the superscript will denote the arity. *Terms* are generated by closing $Const, X$ under $Func$. *Atomic formulæ* are $\top, \bot, p_i^n(t_1, \ldots, t_n), t_i = t_j$, where t_i is a term. The set of formulae is the closure of atomic formulæ under the logical operations and quantification by $\exists x_i$ or $\forall x_i$. A variable x occuring in ϕ is *bound*, if it is in the scope of a of $\exists x_i$ or $\forall x_i$ quantifier, otherwise it is called *free*. The set of free variables of ϕ is denoted by $FV(\phi)$. A *sentence* (or closed formula) is a formula without free variables.

A structure $\mathcal{M}$ consist of a non empty set $\mathcal{U}$ (called the *domain* of interpretation), where elements of $Const$, $Pred$ and $Func$ are interpreted as elements, relations and functions (of appropriate arity) on $\mathcal{U}$. The meaning of quantifiers is as follows:

$$\models_{\mathcal{M}} \forall x \phi(x) \quad \text{iff} \quad \forall b \in \mathcal{U}, \models_{\mathcal{M}} \phi(b) \tag{2.9}$$

$\models_{\mathcal{M}} (x = y)$ iff x and y represent the same element in $\mathcal{U}$. The dual of $\forall$ is $\exists$, $\exists x \phi(x)$ is defined as $\neg \forall x \neg \phi(x)$.

The rules of of inference used in FOL are modus ponens and generalization:

$$\text{MP} \quad \frac{\phi, \phi \rightarrow \psi}{\psi} \tag{2.10}$$

$$\text{Gen} \quad \frac{\phi(x)}{\forall x \phi(x)} \tag{2.11}$$

FOL is compact, finitely axiomatizable and undecidable.

2.3 Nonclassical Logics

In this section we present propositional modal logic (PML) [Che 80], propositional temporal logic (PTL) [Wol 83] and first order temporal logic (FOTL) [Sza 87A].

2.3.1 Propositional Modal Logic

PML is an extension of PL by the modalities $\{\Box, \Diamond\}$. The $\Box\phi$ (*box*) can read as ϕ is necessarily true, and its dual $\Diamond$ (*diamond*) for possibily true.

We will consider *normal* modal logics only, these logics satisfy the Kripke's axiom K : $\Box(\phi \rightarrow \psi) \rightarrow \Box\phi \rightarrow \Box\psi$. A *kripke structure* $\mathcal{M}$ consists of a set of worlds $\mathcal{W} = \{w_i\}$ and a binary accessibily relation R on the worlds. The worlds accessible from w are called the *possible worlds* for w. Each world w is a PL structure with truth as defined for PL, $\Box\phi$ is true at w in $\mathcal{M}$ iff ϕ is true in all possible worlds of w. Its dual, $\Diamond\phi$ is defined as $\neg\Box\neg\phi$.

2.3.2 Propositional Temporal Logic

PTL is an extension of PL by the following logical operation symbols $\{\Box, \Diamond, \bigcirc, \sqcup, Atnext\}$ called henceforth, eventually, next, until, atnext operations respectively. A model for PTL is an infinite linear sequence of worlds $< s_0, s_1, \ldots >$, where each world is a PL structure. The new logical operators are interpreted as follows:

$$\models_{s_i} \Box\phi \quad \text{iff} \quad \forall k \geq i : \models_{s_k} \phi \tag{2.12}$$

$$\models_{s_i} \bigcirc\phi \quad \text{iff} \quad \models_{s_{i+1}} \phi \tag{2.13}$$

$$\begin{aligned} \models_{s_i} \phi \sqcup \psi \quad \text{iff} \quad & \exists k \geq i : \forall m \in \{i, \ldots, k-1\} \models_{s_m} \phi \\ & \text{and } \models_{s_k} \psi \end{aligned} \tag{2.14}$$

$$\begin{aligned} \models_{s_i} \phi \, Atnext \, \psi \quad \text{iff} \quad & \exists k \geq i : \forall m \in \{i, \ldots, k-1\} \models_{s_m} \neg\phi \\ & \text{and } \models_{s_k} (\phi \wedge \psi) \end{aligned} \tag{2.15}$$

$$(\bigcirc z) = t \quad \stackrel{\text{def}}{=} \quad \forall x (t = x \to \bigcirc(z = x)) \tag{2.16}$$

We can use terms of the form $(\bigcirc z)$, because of the last definition.

2.3.3 First Order Temporal Logic

FOTL is the first order version of PTL. The language includes constants, functions, variables, equality, predicates, PL operators, FO quantifiers, operators and modalities of PTL. There are two types of variables: global variables $X = \{x_i\}$ which can be quantified, and state variables $Z = \{z_i\}$ which cannot be quantified.

A model for FOTL is an infinite linear sequence of states: $< s_0, s_1, \ldots >$, where each state is a FO structure. The domain of interpretation ($\mathcal{U}$) of the FO structure, is the same in each state. The constants, functions and predicates have the same interpretation in each state. Every state can independently assign values to the state variables from the domain. The meaning of logical constants are those from PL, PTL and FOL, (except that of the quantifiers). The meaning quantifiers depend on the temporal context:

$$\models_{\mathcal{M}, < s_0, \ldots >} \Box\exists x \phi(x) \quad \text{iff} \quad \forall i \geq 0, \exists b_i \in \mathcal{U}, \models_{\mathcal{M}, < s_i, \ldots >} \phi(b_i) \tag{2.17}$$

$$\models_{\mathcal{M}, < s_0, \ldots >} \exists x \Box\phi(x) \quad \text{iff} \quad \exists b \in \mathcal{U}, \forall i \geq 0, \models_{\mathcal{M}, < s_i, \ldots >} \phi(b) \tag{2.18}$$

The looping problem of a turing machine can be expressed as a formula in FOTL, this formula is valid iff the turing machine loops. Hence FOTL is undecidable [Sza 88]. FOTL with addition and multiplication is strongly incomplete, since the theory of numbers is finitely axiomatizable in it [Sza 87B].
æ

Chapter 3

Some Theories

A theory is useful in that various facts can be represented and reasoned about in it. The more expressive a theory is, the more difficult it is to reason in. The expressive power of a theory will be judged by the sets and relations that can be represented in it.

We look at some first order theories of natural numbers ($\mathcal{N}$) and of real numbers ($\mathcal{R}$).

3.1 Theory of Numbers

In this section we present presburger arithmetic (PrAr, $Th(\mathcal{N}, +)$) and skolem arithmetic ($Th(\mathcal{N}, +, *)$). PrAr is shown to be decidable by quantifiers elimination (QE), while skolem arithmetic is undecidable and not axiomatizable.

3.1.1 Presburger Arithmetic

PrAr is the first order theory of addition on natural numbers ($\mathcal{N}$). It can represent (any given) finite set, ultimately periodic set, and some relations, as show below [End 72].

$$\{0\} \stackrel{\text{def}}{=} \{x : x + x = x\} \tag{3.1}$$
$$n \leq m \stackrel{\text{def}}{=} \exists p\,(n + p = m) \tag{3.2}$$
$$\{1\} \stackrel{\text{def}}{=} \{n : \forall m(m \neq 0 \to n \leq m)\} \tag{3.3}$$
$$S(n) \stackrel{\text{def}}{=} n + 1 \tag{3.4}$$
$$n \stackrel{\text{def}}{=} \underbrace{1 + 1 + \cdots + 1}_{n\,times} \tag{3.5}$$
$$\{n : k|n\} \stackrel{\text{def}}{=} \{n : \exists y\,(\underbrace{y + y + \cdots + y}_{k\,times} = n)\} \tag{3.6}$$
$$\{n_1, \ldots, n_m\} \stackrel{\text{def}}{=} \{x : x = n_1 \vee \cdots \vee x = n_m\} \tag{3.7}$$

3.1.2 Quantifier Elimination

If the truth of any formula in a theory can be decided mechanically in finite number of steps, the theory is called decidable [End 72, Kri 67, Tar 53]. Quantifier Elimination decides the truth of a given closed formula of PrAr by eliminating quantifiers in the formula, then usual finite arithmetic is used to evaluate terms, finally equality, comparision and PL is used to decide its truth value. First the given formula is put in a standard form, then the quantifiers are eliminated one at a time, starting with the innermost.

In order to eliminate quantifiers use the rules of first order logic to convert the given Φ into prenex normal form:

$$Qx_1 \cdots Qx_n \bigvee_i \bigwedge_j \phi_{i,j}(x_1 \cdots x_n) \tag{3.8}$$

where Q denotes a quantifier. Write $\forall$ as $\neg\exists\neg$. Using the fact

$$\models \exists x(\phi(x) \vee \psi(x)) \leftrightarrow (\exists x\phi(x) \vee \exists x\psi(x)), \tag{3.9}$$

we need to consider only formulæ of type $\exists x \bigwedge_j \phi_j(x)$ for QE. The details of quantifier elimination for PrAr are given in appendix I.

3.1.3 Skolem arithmetic

The $Th(\mathcal{N}, +, *)$ is very rich in expressive power but is undecidable and not axiomatizable [Rog 71]. It is complete because it is defined as a theory of a model.

It is stronger than PrAr, since we can define the nonperiodic set of primes. All recursive sets can be defined here, including the syntax of $Th(\mathcal{N}, +, *)$.

$$\text{set of primes} \stackrel{\text{def}}{=} \{p : m * n = p \rightarrow (m = 1 \vee n = 1)\} \tag{3.10}$$

$$\lceil \phi \rceil \stackrel{\text{def}}{=} \text{GödelNumber}(\phi) \tag{3.11}$$

$$\models_{\mathcal{N}} Bew(\lceil \phi \rceil) \stackrel{\text{def}}{=} \vdash_{\mathcal{N}} \phi \tag{3.12}$$

3.2 Real Closed Fields

The $Th(RCF)$ plays an important role in the axiomatization of euclidean geometry [Tar 69]. Most of elementary geometry is expressible in RCF. Tarski has shown this theory to be complete and decidable by the method of quantifier elimination [Kri 67, Tar 51].

Quantifier elimination has nonelementary time complexity (w.r.t. size of formula), as elimination of each quantifier increases the length of the formula exponentially. However the recent method of Cylinderical Algebraic Decomposition (CAD) by Collins decides RCF in $2^{2^{|\phi|}}$ time [Arn 88].

The L_{RCF} is $(\mathcal{R}, 0, 1, +, <, -, *)$, where $\mathcal{R}$ is the set of real numbers. Note that $\{1, 0, <, -\}$ are all definable in $\mathcal{R}$ using $\{+, *\}$. The predicate $integer(x)$ is not definable in RCF, otherwise $Th(\mathcal{N}, +, *)$ would be interpretable in RCF, making skolem arithmetic decidable.

A term t in RCF is a multinomial in some variables $(x_1, \ldots, x_m)$, written as

$$t(x_1, \ldots, x_m) = \sum_i (c_i \prod_j x_{i,j}) \tag{3.13}$$

Atomic formulæ can be written as $term = 0$ or $term > 0$. To apply QE, we need to consider only formulæ of type:

$$\exists x((\bigwedge_i p_i(x) = 0) \wedge (\bigwedge_j q_j(x) > 0)) \tag{3.14}$$

RCF can be axiomatized as follows:

1. Axioms for ordered commutative field.
2. Axioms for existence of square roots and roots of polynomials of odd degree:

$$\forall x \exists y(x = y^2 \vee x = -y^2) \tag{3.15}$$
$$\forall x_0 \dots x_{2n} \exists y(x_0 + x_1 y + \cdots + x_{2n} y^{2n} + y^{2n+1} = 0) \tag{3.16}$$

Since all positive numbers have square roots in RCF, we can define $(y = \sqrt{x})$ as $(x \geq 0 \to y^2 = x)$. æ

Chapter 4

Reasoning about Motion

This chapter looks at ways to represent geometrical and temporal concepts.

4.1 Elementary Geometry

To model plane geometry, we should be able to talk about points, lines, curves, distances, angles, polygons and areas. Coordinate geometry is easily modelled in the first order theory of real numbers. Though only plane geometry is discussed here, generalization to higher dimensions is possible.

A point is the basic undefined unit. The set of points in space (here $\mathcal{R} \times \mathcal{R}$) is considered to be the domain of the model. A point p will be represented by it rectangular coordinates (p_x, p_y).

Let p, q, r, s be points in $\mathcal{R}^2$, we define the following:

$$
\begin{array}{rcll}
\text{distance} & |\overline{p\,q}| & \sqrt{(p_x - q_x)^2 + (p_y - q_y)^2} & (4.1) \\
\text{equidistant} & \delta(p, q, r, s) & \overline{p\,q} = \overline{r\,s} & (4.2) \\
\text{between} & \beta(p, q, r) & ((p_x \le q_x \le r_x) \vee (r_x \le q_x \le p_x)) \wedge & \\
 & & ((p_y \le q_y \le r_y) \vee (r_y \le q_y \le p_y)) & (4.3) \\
\text{line} & l(p) & ap_x + bp_y + c = 0 & (4.4) \\
\text{curve} & c(p) & \text{polynomial}(p_y, p_x) = 0 & (4.5)
\end{array}
$$

$$\text{region} \qquad r(p) \qquad \text{polynomial}(p_y, p_x) \leq 0 \tag{4.6}$$

Tarski [Tar 69] has given a complete axiom system using the predicates δ and β, this system is given in appendix III.

This theory is axiomatizable, complete and decidable; though not finitely axiomatizable. This is because an infinite number of axioms are required to capture the completeness[1] of real numbers.

Arbitrary polygons cannot be expressed in this theory because we need to talk about sets of points. That is possible if we introduce existential monadic predicates[2] to represent arbitary finite sets of points. However this theory can interpret arithmetic, and hence is essentially undecidable.

4.2 Motion

To reason about motion, the motion of points in space has to be represented. Taking the temporal approach, we divide time in discrete states, and use the temporal operators to talk about any particular time point. Let us see how motion can be represented in the first order temporal theory presburger arithmetic (FOTT of PrAr).

The Language of first order temporal logic is extended by the addtion operation, and the domain of the underlying model is the set of natural numbers. Now, what formulæ can be written in this language and how would one interpret[3] them?

$$\Box(z > 0) \tag{4.7}$$

in every state, point z is greater than zero.

$$\Diamond(z_1 > z_2) \tag{4.8}$$

in some state, point z_1 is greater than point z_2.

[1]In the topological sense: every closed and bounded set of real numbers has a real least upper bound.

[2]Monadic second order logic.

[3]we consider motion on a one dimension number line

$$\Diamond\Box(z = 2) \tag{4.9}$$

finally z goes to two and remains there.

$$\Box\Diamond(z_1 = z_2) \tag{4.10}$$

infinitely often points z_1 and z_2 meet.

$$\forall x \Diamond(z = x) \tag{4.11}$$

z visits all points in the domain.

$$\Box\forall x(z = x \rightarrow \bigcirc(z = x + 1)) \tag{4.12}$$

z moves forward by one in every state.

$$(\bigcirc(z) = z + 1) \sqcup (z = z_1) \tag{4.13}$$

z moves right until it meets point z_1

$$(z = 0 \wedge \Box((\bigcirc z) = z + 1)) \rightarrow \forall x \Diamond(z = x) \tag{4.14}$$

if z starts at zero and moves right

then it eventually visits every point.

4.3 Conclusion

This theory is powerful enough to characterize the set of natural numbers[4], hence we must restrict it suitably before looking for a decision procedure. So we limit the interpretations to $(\mathcal{N}, +)$, and restrict the type of formulæ allowed by bounding the number of quantifiers.

A object cannot move from point p_1 to p_2 without passing through every point between p_1 and p_2. Consider the movement of point z on the real line from p_1 to p_2 in time t_1 to t_2, now as z moves through every point between p_1 and p_2, there must be distinct time points to refer to those positions. This is because we assume motion to be a continous function from time states to positions on the number line. Hence the above theory cannot express motion on the real line.

We hope to introduce motion into plane geometry also, and find ways to represent continous motion, velocity and collisions. æ

[4]compare equation 4.14 with the induction axiom.

Chapter 5

Reasoning about Knowledge

We wish to define the concept of knowledge and belief rigourously, so as to automate reasoning about knowledge. The system must model several agents[1] and reason about their knowledge, rules, time (cause and effect), learning, inference, belief and common knowledge. However, it is not yet possible to correctly model knowledge as a axiomatic mathematical theory. Though modal logic 'KW' has been successfully used to reason about proofs, the present modal knowledge system suffers from the following drawbacks:

Logical omniscience A agent is expected to know all the logical consequences of his knowledge. Suppose the agent knows the algorithm for factoring integers, then he is assumed to know factorizations of all numbers. On the other hand, one would hardly expect any agent to know the factors of a random five hundred digit integer.

Monotonocity Once the agent knows ϕ, then he can never revise his knowledge and know $\neg\phi$. Suppose he knows "Twitty is a bird", and he infers Twitty flies. Now if he is told "Twitty is a flightless kiwi bird", he will also know Twitty cannot fly. Hence he will become inconsistent and know everything[2].

Beliefs Agent may believe[3] something as plausible but not 'know' it. Sup-

[1]reasoners will be called agents.

[2]by definition of inconsistency.

[3]We differentiate between knowledge and belief: knowledge is necessarily true, but a

pose he knows "if it rains then the ground is wet", and he sees that the ground is wet then he believes that it rained. He knows well that it is only his belief, and may be revised in face of contrary evidence.

Common knowledge When two (or more) agents know ϕ, and each know that the other knows ϕ, also each knows that the other knows that he knows ... ad infinitum ϕ, then ϕ is said to be common knowledge between the agents. Suppose two agents want to coordinate a meeting through a faulty communication medium[4] and have the common knowledge that each will only come if and only if he is sure the other is coming, then it is impossible for them to coordinate the meeting. The last agent to acknowledge will never be sure if his acknowledgement[5] reached.

Causality In logic, if ϕ implies ψ then it does not mean that ϕ is the cause of ψ. ϕ and ψ may be unrelated.

Counterfactuals It is difficult to reason about counterfactuals in a logical theory. Consider the following statement: "Had block-1 been on top of block-2 then the robot would have lifted block-1 also".

Introspection Practical agents have limited self awareness. Depending on the type of reasoner, he may or maynot know what he knows or does not know. Self reference[Smu 86A] also leads to a paradox, as in the case of Gödel's incompleteness theorem.

5.1 Axioms for Knowledge

Several axiomatic formulations of knowledge [Hal 86] based on modal logic exists. The modality $K_i(\phi)$ is to read as *agent i knows* ϕ, the subscript will be omitted if there is only one agent . One such axiom system due to Hintikka is:

$$\text{Ax1} \qquad \text{PL tautologies} \tag{5.1}$$

belief may be false.

[4] by mail, for example

[5] about the other's acknowlegement, ... ad infinitum.

Ax2	$(K(\phi) \wedge K(\phi \rightarrow \psi)) \rightarrow K(\psi)$	logical omniscience.	(5.2)
Ax3	$K(\phi) \rightarrow \phi$	no belief.	(5.3)
Ax4	$K(\phi) \rightarrow K(K(\phi))$	positive introspection.	(5.4)
Ax5	$\neg K(\phi) \rightarrow K(\neg K(\phi))$	negative introspection.	(5.5)
ROI1	$\frac{\phi, \phi \rightarrow \psi}{\psi}$	modus ponens.	(5.6)
ROI2	$\frac{\phi}{K(\phi)}$	necessitation.	(5.7)

Suppose agent A tells agent B, "ϕ is true but you do not know ϕ":

$$K_B(\phi \wedge \neg K_B(\phi)) \tag{5.8}$$

$$\Rightarrow \quad K_B(\phi) \wedge K_B(\neg K_B(\phi)) \tag{5.9}$$

The statement was true when it was said, but immediately afterwards it is false. Thus, knowledge depends on time and must be modelled as such. To account for changes in knowledge with time [Leh 84], temporal logic can be used. Any exchange of information takes at least one time state:

$$\neg K_B(\phi) \wedge \bigcirc K_B(\phi) \tag{5.10}$$

5.2 Common Knowledge

Common knowledge is defined by introducing the modalities E and C for *everyone knows* and *common knowledge* respectively:

$$E(\phi) \stackrel{\text{def}}{=} \bigwedge_{\forall i} K_i(\phi) \tag{5.11}$$

$$E^1(\phi) \stackrel{\text{def}}{=} E(\phi) \tag{5.12}$$

$$E^n(\phi) \stackrel{\text{def}}{=} E^{n-1}(E(\phi)),\ if\ n > 1 \tag{5.13}$$

$$C(\phi) \stackrel{\text{def}}{=} \bigwedge_{\forall i \in \omega \geq 1} E^i(\phi) \tag{5.14}$$

Suppose agent B receives a letter from agent A to fix a meeting (ϕ), but A has received no acknowledgement from B, this is represented as:

$$K_A(\phi) \wedge K_B(\phi) \wedge K_B(K_A(\phi)) \wedge \neg K_A(K_B(\phi)) \ldots \tag{5.15}$$

$$\Rightarrow \quad E(\phi) \wedge K_B(E(\phi)) \wedge \neg K_A(E(\phi)) \ldots \tag{5.16}$$

On the other hand agent B receives a phone from agent A fixing a meeting (ψ), we write:

$$\begin{aligned} & E(\psi) \wedge E^2(\psi) \wedge \ldots \wedge E^i(\psi) \wedge \ldots & (5.17) \\ \Rightarrow \quad & C(\psi) & (5.18) \end{aligned}$$

5.3 Reasoning about Proofs

In reasoning about proofs [Boo 79], the modalities $\Box\phi$ and $\Diamond\psi$ have a precise mathematical meaning: ϕ is provable and ψ is consistent[6] respectively. The use of Bew[7] instead of $\Box$ will denote this special meaning.

The formula $Bew(\ulcorner\phi\urcorner)$ mentioned in connection with skolem arithmetic, obeys the laws of the normal modal logic 'KW'[8]:

$$\lceil\phi\rceil \stackrel{\text{def}}{=} \text{GödelNumber}(\phi) \tag{5.19}$$

$$\models_{\mathcal{N}} Bew(\lceil\phi\rceil) \stackrel{\text{def}}{=} \vdash_{\mathcal{N}} \phi \tag{5.20}$$

$$\phi \text{ is consistent} \stackrel{\text{def}}{=} \neg Bew(\lceil\neg\phi\rceil) \tag{5.21}$$

$$\phi \text{ is undecidable} \stackrel{\text{def}}{=} \neg Bew(\lceil\phi\rceil) \wedge \neg Bew(\lceil\neg\phi\rceil) \tag{5.22}$$

The system KW has the following axioms:

$$\text{AxK} \quad Bew(\lceil\phi \rightarrow \psi\rceil) \rightarrow Bew(\lceil\phi\rceil) \rightarrow Bew(\lceil\psi\rceil) \tag{5.23}$$

$$\text{AxW} \quad Bew(\lceil Bew(\lceil\phi\rceil) \rightarrow \phi\rceil) \rightarrow Bew(\lceil\phi\rceil) \tag{5.24}$$

$$\text{Th4} \quad \vdash_{KW} Bew(\lceil\phi\rceil) \rightarrow Bew(\lceil Bew(\lceil\phi\rceil)\rceil) \tag{5.25}$$

The modal logic KW is complete and decidable, and the following of its theorems give insight into arithmetic:

$$\vdash_{KW} \Box\Diamond\top \rightarrow \Box\bot \tag{5.26}$$

$$\Rightarrow \quad \vdash_{\mathcal{N}} Bew(\lceil\neg Bew(\lceil\bot\rceil)\rceil) \rightarrow Bew(\lceil\bot\rceil) \tag{5.27}$$

[6] that is: $\neg\psi$ is not provable.

[7] From beweisbar, means provable in Hebrew.

[8] Also known as Löb's system.

Equation 5.27 is Gödel's second incompleteness theorem, it says "if the consistency of arithmetic can be proved (in arithmetic), then arithmetic is inconsistent".

$$\begin{aligned} & \vdash_{KW} \Diamond\top \leftrightarrow \neg\Box\Diamond\top && (5.28)\\ \Rightarrow\ & \vdash_{\mathcal{N}} \neg Bew(\ulcorner\bot\urcorner) \leftrightarrow \neg Bew(\ulcorner\neg Bew(\ulcorner\bot\urcorner)\urcorner) && (5.29)\end{aligned}$$

This says "arithmetic is consistent iff its consistency is not provable (in arithmetic[9])"

$$\begin{aligned} & \vdash_{KW} \neg\Box\Box\bot \rightarrow (\neg\Box\Diamond\top \wedge \neg\Box\neg\Diamond\top) && (5.30)\\ \Rightarrow\ & \vdash_{\mathcal{N}} \neg Bew(\ulcorner Bew(\ulcorner\bot\urcorner)\urcorner) \rightarrow \\ & (\neg Bew(\ulcorner\neg Bew(\ulcorner\bot\urcorner)\urcorner) \wedge \neg Bew(\ulcorner Bew(\ulcorner\bot\urcorner)\urcorner)) && (5.31)\end{aligned}$$

It can be proved in arithmetic that "if the inconsistency of arithmetic is unprovable (in arithmetic) then its consistency is undecidable[10] (in arithmetic)".

5.4 Conclusion

We can start with the modalities K_i and B_i as the modalities for knowledge and belief respectively, box, diamond and circle will denote the usual temporal operations. If there is no evidence either way, the agent may believe the default, with the provision that beliefs may be wrong and can be revised in the future. With these objectives we define the following axioms:

$$K(\neg\phi) \rightarrow \neg K(\phi) \quad (5.32)$$
$$K(\phi) \rightarrow (\Box K(\phi) \wedge \bigcirc\Box B(\phi)) \quad (5.33)$$
$$K(\phi) \wedge K(\psi) \leftrightarrow K(\phi \wedge \psi) \quad (5.34)$$
$$B(\phi) \rightarrow \Diamond(K(\phi) \vee K(\neg\phi)) \quad (5.35)$$
$$(K(\phi) \wedge K(\phi \rightarrow \psi)) \rightarrow \bigcirc K(\psi) \quad (5.36)$$
$$K(\phi) \rightarrow \bigcirc K(K(\phi)) \quad (5.37)$$

[9] The consistency of arithmetic can be proved from outside.

[10] If a theory contains an undecidable sentence then it is incomplete.

All knowledge is consistent, and belief must agree with knowledge. Only what can eventually be known can be believed. Inference and self-awareness proceed in steps, the steps may be large or small depending on the context. It is hoped to expand this system into a useful one. æ

Appendix A

Bibliography

Bibliography

[Arn 88] Arnon, D.S., Geometric reasoning with logic and algebra, *Artificial Intelligence* **37** (1988) 37-60.

[Bar 77] Barwise, J., Introduction to first order logic, in: J. Barwise (Ed.),*Handbook of Mathematical Logic*, (North Holland, Amsterdam, 1977) 5-46.

[Boo 79] Boolos, G., *The Unprovability of Consistency*, (Cambridge University Press, 1979).

[Che 80] Chellas, B., *Introduction to Modal Logic*, (Cambridge University Press, 1980).

[End 72] Enderton, H., *A Mathematical Introduction to Logic*, (Academic press 1972).

[Hal 86] Halpern, J., Reasoning about knowledge: an overview, in: J. Halpern (ed.), *Reasoning about Knowledge*, (Morgan Kaufman 1986) 1-17.

[Kap 88] Kapur, D. and Mundy J.L., (Eds.), *Special Volume on Geometric Reasoning*, *Artificial Intelligence* **37** journal, (North Holland, Amsterdam, 1988).

[Kri 67] Kriesel, G. and Kirvine, J.L., *Introduction to Mathematical Logic*, (North Holland, Amsterdam, 1967) 60-64.

[Lad 86] Ladner, R. and Reif, J., The logic of distributed protocols, preliminary report, in: J. Halpern (ed.), *Reasoning about Knowledge*, (Morgan Kaufman 1986) 207-222.

[Leh 84] Lehman, D., Knowledge, common knowledge and related puzzles, *Proceedings of Third ACM Conference on Principles of Distributed Computing*, 1984, 62-67.

[Par 87] Parikh, R., Knowledge and problem of logical omniscience, *ISMIS-87*, North Holland, 432-439.

[Rac 79] Rackoff, J. and Ferrante C.W., *The computational complexity of logical theories*, Lecture Notes in Mathematics **718**, (Springer Verlag, 1979).

[Rog 71] Rogers, R., *Mathematical Logic and Formalized Theories*, (North Holland, 1971).

[Sho 88] Shoham, Y., *Reasoning about Change*, (MIT Press, 1988).

[Smu 86A] Smullyan, R., *Forever Undecided*, Oxford University Press 1986.

[Smu 86B] Smullyan, R., Logicians who reason about themselves, in: J. Halpern (ed.), *Reasoning about Knowledge*, (Morgan Kaufman 1986) 341-352.

[Sza 87A] Szalas, A., A complete axiomatic characterization of first order temporal logic of linear time, *Theoretical Computer Science* **54**, 1987.

[Sza 87B] Szalas, A., Arithmetical axiomatization of first order temporal logic, *Information Processing Letters*, **26**, 1987.

[Sza 88] Szalas, A. and Holenderski, L., Incompleteness of first order temporal logic with until, *Theoretical Computer Science* **57**, 1988.

[Tar 51] Tarski, A., *A Decision Method for Elementary Algebra and Geometry* (University of California Press, Berkeley, CA, 2nd ed., 1951).

[Tar 53] Tarski, A., *Undecidable Theories*, (North Holland, Amsterdam, 1953).

[Tar 69] Tarski, A., What is elementary geometry ?, in J. Hintikka (Ed.), *The Philosophy of Mathematics*, (Oxford University Press, 1969) 164 - 177.

[Tar 86] Tarski, A., Truth and proof, in: S.R. Givant and R.N. Mckenzie (Eds.), *Tarski: Collected Papers*, Volume **4**, (Birkauser, Basel, 1986).

[Wol 83] Wolper, P., Temporal logic can be more expressive, *Information and Control* **56**, 1983.

Appendix B

Quantifier Elimination for Presburger Arithmetic

To eliminate x from $\exists x \bigwedge_j \phi_j(x)$, where each $\phi_j(x)$ is an atomic formula or its negation.

1. Add to the language L_{PrAr}, the modulo operators: $\{\equiv_i : i \geq 2\}$

2. Remove negation from atomic formulæ:

$$\begin{aligned}
\neg(t_1 = t_2) &\Rightarrow (t_1 < t_2) \vee (t_2 < t_1) \\
\neg(t_1 < t_2) &\Rightarrow (t_2 < t_1) \vee (t_2 = t_1) \\
\neg(t_1 \equiv_m t_2) &\Rightarrow \bigvee_{i=1}^{m-1} (t_1 = t_2 + i)
\end{aligned}$$

3. Bring x on LHS of $<$ or $=$ (Use $-$ and $>$ for convenience)

$$\begin{aligned}
nx + t = u &\Rightarrow nx = u - t \\
nx + t \equiv_m u &\Rightarrow nx \equiv_m u - t \\
nx + t < u &\Rightarrow nx < u - t \\
u < nx + t &\Rightarrow nx > u - t
\end{aligned}$$

4. Uniformize the coefficients of x, using LCM of coefficients, be sure to multiply the modulii appropriately. In ϕ replace px by a new variable x', and include $x' \equiv_p 0$.

$$\exists x \phi(px) \Rightarrow \exists x'(\phi'(x') \wedge x' \equiv_p 0)$$

5. If equality is present, substitute the value of x.

$$\exists x(\phi(x) \wedge x = u) \quad \Rightarrow \quad (\phi(u) \wedge 0 \leq u)$$

6. The formula is now in the form:

$$\exists x \left((\bigwedge_i \overbrace{r_i - s_i}^{lb_i} < x) \wedge \underbrace{(\bigwedge_j x \equiv_{m_j} \overbrace{v_j - w_j}^{md_j})}_{B} \wedge (\bigwedge_k x < \overbrace{r_i - s_i}^{ub_k}) \right)$$

We must find x such that it satisfies the lower bounds (lb_i), moduli (md_j) and upper bounds (ub_k) simultaneously.

(a) If B is absent, x must lie in between $lb_i and ub_k$, so we write:

$$\begin{aligned} &\Rightarrow \quad (\exists x \textstyle\bigwedge_i \bigwedge_k (lb_i < x < ub_k)) \wedge \bigwedge_k (0 < ub_k) \\ &\Rightarrow \quad (\textstyle\bigwedge_i \bigwedge_k (lb_i < ub_k + 1)) \wedge \bigwedge_k (0 < ub_k) \end{aligned}$$

(b) Else if B is present, let $M = LCM(m_i : m_i \in B)$, and include an extra lower bound $= -1$ (in case all $lb_i < 0$). Now x must lie in the set

$$S = \bigcup_i \{lb_i + m : m \in \{0 \ldots M-1\}\}$$

The formula can now be written as:

$$\bigvee_{r \in S} \left(\bigwedge_i (lb_i < r) \wedge \bigwedge_j (r \equiv_{m_j} v_j - w_j) \wedge \bigwedge_k (r < ub_k) \right)$$

Hence the quantifier $\exists x$ has been eliminated. æ

Appendix C

Index of Symbols

$\mathcal{L}$	language of a logic
$\mathcal{M}$	model
$\mathcal{N}$	natural numbers
$\mathcal{R}$	real numbers
$\mathcal{T}$	theory
$\mathcal{W}$	set of possible worlds
$\mathcal{X}$	set of variables
$\mathcal{U}$	domain of a model
$\mathcal{Z}$	set of state variables
$Prop$	set of propositions
p_i	proposition
$const$	set of constants
c_i	constant
$func$	set of functions
f_i^n	n-ary function
$pred$	set of predicates
p_i^n	n-ary predicate
x_i	variable
z_i	state variable
w_i	possible world
PL	propositional logic
FO	first order
FOL	first order logic

FOT	first order theory
PML	propositional modal logic
TL	temporal logic
PTL	propositional temporal logic
FOTL	first order temporal logic
ROI	rule of inference
MP	modus ponens
fmp	finite model property
$wff(\mathcal{L})$	well formed formulæ in $\mathcal{L}$
$Th(..)$	theory of ..
const$(\mathcal{T})$	theory $\mathcal{T}$ is consistent
$\top$	true
$\bot$	false
$\neg$	negation, not
$\vee$	disjunction, or
$\wedge$	conjunction, and
$\rightarrow$	implies, only if
$\leftrightarrow$	equivalent, iff
$\forall$	for all
$\exists$	there exists
$\exists!$	there exists a unique
ϕ, ψ	formulæ in $wff(\mathcal{L})$
Γ, Δ	set of formulæ
$.. \models \phi$	ϕ is a consequence of ..
$.. \vdash \phi$	ϕ is provable from ..
$Cn(..)$	set of consequences of ..
$Pr(..)$	set of formulæ provable from ..
PrAr	presburger arithmetic
RCF	real closed fields
$\Box$	box, henceforth, necessary
$\Diamond$	diamond, eventually, possible
$\bigcirc$	next
$\sqcup$	until
$Atnext$	at the next state
$K_i(..)$	agent i knows ..
$E(..)$	every agent knows ..
$C(..)$	.. is common knowledge

p, q, r, s	points in space
$\|\overline{p\,q}\|$	distance between points p and q
$p = (p_x, p_y)$	coordinates of a point p
$\delta(p, q, r, s)$	distance pq = distance rs
$\beta(p, q, r)$	point q is between points p and r

æ

Appendix D

Axioms for Plane Geometry

Ax1	$\forall xy\,[\beta(xyx) \to (x = y)]$
Ax2	$\forall xyzu\,[(\beta(xyu) \wedge \beta(yzu)) \to \beta(xyz)]$
Ax3	$\forall xyzu\,[(\beta(xyz) \wedge \beta(xyu) \wedge (x \neq y)) \to (\beta(xzu) \vee \beta(xuz))]$
Ax4	$\forall xy\,[\delta(xyyx)]$
Ax5	$\forall xyz\,[\delta(xyzz) \to (x = y)]$
Ax6	$\forall xyzuvw\,[(\delta(xyzu) \wedge \delta(xyvw)) \to \delta(zuvw)]$
Ax7	$\forall txyzu\exists v\,[(\beta(xtu) \wedge \beta(yuz)) \to (\beta(xvy) \wedge \beta(ztv))]$
Ax8	$\forall txyzu\exists vw\,[(\beta(xut) \wedge \beta(yut) \wedge (x \neq u))$ $\to (\beta(xzv) \wedge \beta(xyw) \wedge \beta(vtw))]$
Ax9	$\forall xx'yy'zz'uu'\,[(\delta(xyx'y') \wedge \delta(yzy'z') \wedge \delta(xux'u') \wedge \delta(yuy'u') \wedge$ $\beta(xyz) \wedge \beta(x'y'z') \wedge (x \neq y)) \to \delta(zuz'u')]$
Ax10	$\forall xyuv\exists z\,[\beta(xyz) \wedge \delta(yzuv)]$
Ax11	$\forall xyz\,[\neg\beta(xyz) \wedge \neg\beta(yzx) \wedge \neg\beta(zxy)]$
Ax12	$\forall xyzuv\,[(\delta(xuxv) \wedge \delta(yuyv) \wedge \delta(zuzv) \wedge (u \neq v))$ $\to (\beta(xyz) \vee \beta(yzx) \vee \beta(zxy))]$
Ax13*	$\forall p,\ldots,q\,[\forall xy\exists z((\phi(x) \wedge \psi(y)) \to \beta(zxy))$ $\longrightarrow \exists u\forall xy((\phi(x) \wedge \psi(y)) \to \beta(xuy))]$

æ

Appendix E

Acknowledgement

I thank Dr. G. Venkatesh for his guidance and constant help in clearing my doubts. I also thank him for suggesting the problems, and his patience while I prepared this report.