Lecture 8-9
Decidable and Undecidable Theories

Overview

- Decidability
- What do we learn from decidability ?
- The real and complex numbers
- The monadic second order theory of trees
- The complexity of decidable theories
- Undecidability

Model checking in infinite structures

We now look at infinite τ-structures $\mathfrak{A}$.

Given a sentence $\phi \in FOL(\tau)$
(or $\in SOL(\tau)$)
what do we need to know to check

$$\mathfrak{A} \models \phi?$$

- $\mathfrak{A}$ has universe $\mathbb{N}$ and each relation $R \in \tau$ is given by a Turing machine M_R.
- We know that $\mathfrak{A} \models \Sigma$ with $\Sigma \subseteq FOL(\tau)$.
- We know
  $$Th_{FOL(\tau)}(\mathfrak{A}) = \{\phi \subseteq FOL(\tau) : \mathfrak{A} \models \phi\}$$
  is computable.

Computable structure $\mathfrak{N}$

The classical example of a **computable structure** is

$$\mathfrak{N} = \langle \mathbb{N}, +, \cdot, <, 0, 1 \rangle$$

with $\tau_{arith} = \{F_+, F_\cdot, R_<, c_0, c_1\}$.

We can test for quantifierfree ϕ, and numbers $a_1, \ldots a_m$ whether

$$\mathfrak{N} \models \phi(\bar{a})$$

What about quantifiers?

Theorem 1 (Goedel 1931)
$Th_{FOL(\tau_{arith})}(\mathfrak{N})$ is not r.e.

Computable structure $\mathbb{Q}_<$

Here $\tau = \{R <\}$ and
we take the order of the rationals $\mathbb{Q}$.

Theorem 2 (Completeness of Th_{dense})
For $\phi \in FOL(\tau)$ the following are equivalent:

(1) $\mathbb{Q}_< \models \phi$
(2) $Th_{dense} \models \phi$
(3) $Th_{dense} \vdash \phi$

where Th_{dense} is the conjunction of sentences which say that we have a dense linear order with first nor last element.

Corollary 3
$Th_{FOL(\tau)}(\mathbb{Q}_<)$ is computable.

Use the completeness theorem

Proof of completeness of Th_{dense}, II

Lemma 4 (Cantor, ca. 1870)

Let $\mathfrak{A}$ and $\mathfrak{B}$ both satisfy Th_{dense}.
Then $\mathfrak{A} \simeq \mathfrak{B}$.

Proof: Construct isomorphism via Ehrenfeucht-Fraïssé games played infinitely long.

Details on the black board

Lemma 5 (Isomorphism lemma)
Let $\phi \in SOL(\tau)$ and $\mathfrak{A} \simeq \mathfrak{B}$ be two isomorphic τ-structures.

Then $\mathfrak{A} \models \phi$ iff $\mathfrak{B} \models \phi$.

Proof of completeness of Th_{dense}, II

1. $\Rightarrow$ 2.:
Assume $\mathbb{Q}_< \models \phi$ but $Th_{dense} \cup \{\neg\phi\}$ is satisfiable.
So $Th_{dense} \cup \{\neg\phi\}$ has a countable model $\mathfrak{A}$.

By the Cantor's lemma, $\mathfrak{A} \simeq \mathbb{Q}_<$.
By the isomorphims lemma,
$\mathfrak{A} \models \phi$ iff $\mathbb{Q}_< \models \phi$.

But $\mathfrak{A} \models \neg\phi$, a contradiction.

2. $\Rightarrow$ 3.:
This is the completeness theorem.

3. $\rightarrow$ 1.:
This is soundness of $\vdash$ and the fact that $\mathbb{Q}_< \models Th_{dense}$.

Q.E.D.

Quantifier elimination

Let $\tau' = \{R_<, c_0\}$ and $\mathbb{Q}_{<,0} = \langle \mathbb{Q}, <, 0 \rangle$.

Theorem 6 (Elimination of quantifiers)
For every formula $\phi(\bar{x})$ with possibly free variables, there exists a formula $\psi(\bar{x})$ such that

- *ψ is quantifierfree*
- *ψ has the same free variables as ϕ,*
- *$Th_{dense} \models \forall \bar{x}(\phi \leftrightarrow \psi)$*
- *ψ can be found in exponential time.*

In particular, every closed formula is either equivalent to $0 \approx 0$ or $\neg 0 \approx 0$.

The consequence relation, I

Theorem 7 (Gödel 1931)
Given $\Sigma \subseteq FOL(\tau)$ and $\phi \in FOL(\tau)$.

Then $\Sigma \models \phi$ iff $\Sigma \vdash \phi$ and if Σ is r.e. then

$$\{\phi \in FOL(\tau) : \Sigma \vdash \phi\}$$

is r.e., but not computable.

Here we allow infinite structures

The consequence relation, II

Now we restrict ourselves to **finite structures**.

We denote by $\models_{fin}$ the consequence relation restricted to finite structures.

Theorem 8 (Trakhtenbrot 1941)
Given $\Sigma \subseteq FOL(\tau)$ and $\phi \in FOL(\tau)$.

Then the relation $\Sigma \models_{fin} \phi$ is co-r.e. but not .re.

In particular there is no r.e. provability notion $\vdash_{fin}$ such that $\Sigma \vdash_{fin} \phi$ iff $\Sigma \models_{fin} \phi$.

Definition 9 (Decidable Theories)

Let $\mathcal{L}$ be a regular logic (or just a class of formulas). For a class K of τ–structures, we say that

- K is *L–decidable*, if
  $Th_{\mathcal{L}}(K) = \{\theta \in \mathcal{L}(\tau) : \text{for every } \mathcal{A} \in K, \mathcal{A} \models \theta\}$
  is recursive.
- We say that K is *$\mathcal{L}$–elementarily–closed* if $\mathcal{A} \models Th_{\mathcal{L}}(K)$ iff $\mathcal{A} \in K$.
- We say that K is *$\mathcal{L}$–closed* if $K = Mod_{\mathcal{L}}(Th_{\mathcal{L}}(K))$.
- A theory T (a set of $\mathcal{L}$-formulas) is *decidable* if $Mod_{\mathcal{L}}(T)$ is decidable.

Examples 10
(Un-)decidable first oder theories

- For the empty vocabulary, the theory of all (infinite, finite) structures is decidable.
- For the vocabulary consisting of one binary relation symbol, the ($\forall\exists$) theory of all (infinite, finite) structures is undecidable.
- The theory of abelian groups (real closed, algebraically closed fields) is decidable.
- The theory of groups (fields, ordered fields) is undecidable.
- The universal theory of groups (= word problem for groups) is undecidable.

What do we learn from the decidability of a thery T ?

- Decidable = Computable
  (But not necessarily effectively computable)
- The decidability algorithm usually contains much more information:
  - We might get *(partial) elimination of quantifiers*.
  - We might get a better understanding of the definable sets in models of T.
  - We might get a *representation theorem* saying that every model of T is of a certain form.
- T (effectively) decidable = we understand T (very) well.

How do we prove (un)-decidability of T ?

- Direct proof, using the intricacies of T.
- Using *translation schemes* and a selected family of strong decidable or weak undecidable theories.
- Using model theoretic methods such as categoricity and Vaught's test.
- Using (partial) elimination of quantifiers.

Guide to the literature

Decidable theories:

Y. Eršov, I.A, Lavrov, A.D. Taimanov and M.A. Taitslin,
Elementary theories, Russian Mathematical Surveys 20 (1965) pp. 35-100 (English Translation)

M. Rabin, Decidable Theories, in:
Handbook of Mathematical Logic (J. Barwise ed.), Studies in Logic, North Holland 1977

Effectively decidable theories:

J. Ferrante and C. Rackoff, The computational complexity of logical theories, Lecture notes in Mathematics, vol. 718, Springer 1979.

K.J. Compton and C. W. Henson,
A uniform method for proving lower bounds on the computational complexity of logical theories, Annals of Pure and Applied Logic, 48 (1990) pp. 1-79

Guide to the literature (Contd)

Undecidable theories:

A. Tarski, A. Mostowski and R. Robinson, Undecdable theories, Studies in Logic, North Holland 1953

M. Davis, Unsolvable problems, in:
Handbook of Mathematical Logic (J. Barwise ed.), Studies in Logic, North Holland 1977

General references:

D. Monk, Mathematical Logic, Springer 1976

E. Börger, E. Grädel and Y. Gurevich, The classical decision problem, Perspectives in Mathematical Logic, Springer 1997

Proposition 11
(Decidability of complete theories)

A theory T is *L-complete* if for every $\mathfrak{A}, \mathfrak{B} \models T$ $Th_{\mathcal{L}}(\mathfrak{A}) = Th_{\mathcal{L}}(\mathfrak{B})$.

If $\mathcal{L}$ be a regular logic with recursive sets of sentences $\mathcal{L}(\tau)$ for each finite τ and with recursive enumerable consequence relation then

K is decidable
iff
$Th_{\mathcal{L}}(K) = T$ for some
recursively enumerable
complete T.

Example 12 (Infinite sets)

Let K be the class of infinite sets.

Let T be $\{\exists^{>n} x(x = x) : n \in \mathbb{N}\}$.

Clearly (exercise !), $\mathfrak{A} \in K$ iff $\mathfrak{A} \models T$ and for any $\mathfrak{A}, \mathfrak{B} \in K$ we have

$$Th_{FOL}(\mathfrak{A}) = Th_{FOL}(\mathfrak{B})$$

Hence T is complete and therefore decidable.

[Löwenheim 1915] showed the decidability of the theory of equality of arbitrary sets, using the elimination of quantifiers.

Proposition 13 (Vaught's test)

A theory T is κ-categorical for some infinite cardinal κ, if any two models of T of cardinality κ are isomorphic.

If T is κ-categorical for some infinite κ and T has no finite models, then T is complete.

Proof:
Assume T is not complete. Let $\mathfrak{A} \models \phi$ and $\mathfrak{B} \models \neg\phi$ be two infinite models of T.

Let $\mathfrak{A}_1, \mathfrak{B}_1$ be of cardinality κ such that

$$Th_{FOL}(\mathfrak{A}) = Th_{FOL}(\mathfrak{A}_1)$$

and

$$Th_{FOL}(\mathfrak{B}) = Th_{FOL}(\mathfrak{B}_1)$$

(Löwenheim-Skolem Theorem).

But $\mathfrak{A}_1$ and $\mathfrak{B}_1$ are not isomorphic, as $\mathfrak{A}_1 \models \phi$ and and $\mathfrak{B}_1 \models \neg\phi$. *Q.E.D.*

Example 14 (Theory of infinite sets)
Let T_{inf} be $\{\exists^{>n} x(x = x) : n \in \mathbb{N}\}$.

T_{inf} has no finite models and is categorical in every infinite κ, hence it is complete.

Example 15 (Algebraically closed fields)
Let $\mathbf{ACF_0}$, the theory of algebraically closed fields of characteristic 0, *consisting of the field axioms, the set of axioms saying that every polynomial in one variable has a zero, and the set of axioms saying that no finite sum of 1's equals 0. Clearly,*

$$\mathfrak{C} = \langle \mathbb{C}, +, \cdot, 0, 1 \rangle \models \mathbf{ACF_0}$$

By a theorem due to Steinitz, any two models of cardinality κ with κ uncountable, are isomorphic. Hence, $\mathbf{ACF_0}$ is complete.

Theorem 16 (Preservation of Decidability)
(Mostowski, R. Robinson and Tarski; Rabin)

Let $\mathcal{L}$ be a logic with recursive enumerable consequence relation. Let K_1, K_2 be $\mathcal{L}$–closed classes of $\tau_1(\tau_2)$–structures and Φ be a translation scheme in $\mathcal{L}$.

1. If Φ^* is a weak reduction from K_1 to K_2 which is onto, K_1 is decidable, then K_2 is decidable. (Similar for K_1 decidable in TIME(f), SPACE(g) for suitable f and g, depending on the complexity of substitution in $\mathcal{L}$.)

2. If Φ^* is a transduction from K_1 to K_2 which is onto and K_1 is decidable and K_2 definable by a single $\mathcal{L}$–sentence, then K_2 is decidable.

Proof of theorem 16(i)

Proof:
Let $\theta \in \mathcal{L}(\tau_2)$.

We want to check whether $\theta \in Th(K_2)$.

We check whether $\Phi^{\#}(\theta) \in Th(K_1)$.
As $Th(K_1)$ is recursive, we get an answer.

If $\Phi^{\#}(\theta) \in Th(K_1)$, we have that $\theta \in Th(K_2)$, as Φ^* is a weak reduction.

If $\Phi^{\#}(\theta) \notin Th(K_1)$, there is $\mathcal{A} \in K_1$ with

$$\mathcal{A} \models \neg\Phi^{\#}(\theta)$$

But as Φ^* is onto

$$\Phi^*(\mathcal{A}) \models \neg\theta$$

As Φ^* is a weak reduction,

$$\Phi^*(\mathcal{A}) \in K_2$$

Hence $\theta \notin Th(K_2)$. $Q.E.D.$

Proof of theorem 16(ii)

Proof:
Assume that $K_2 = Mod(\alpha)$.

Now $\theta \in Th(K_2)$ iff $\alpha \to \theta$ is valid.

As $\mathcal{L}$ has an r.e. consequence relation, $Th(K_2)$ is r.e.

On the other hand:

$\theta \notin Th(K_2)$
iff
there is $\mathcal{B} \in K_2$ with $\mathcal{B} \models \neg\theta$
iff (here we use that Φ^* is onto)
there is $\mathcal{A} \in K_1$ with $\mathcal{A} \models \Phi^{\#}(\neg\theta)$
iff $\Phi^{\#}(\theta) \notin Th(K_1)$.

This shows that $Th(K_2)$ is co–r.e. $Q.E.D.$

The real and complex numbers revisited

Let $\mathfrak{R}$ be the structure

$$\mathfrak{R} = \langle \mathrm{IR}, +, \times \rangle$$

where the functions $+, \times$ are interpretations of ternary relation symbols A and M.
RCF is the set of first order sentences true in $\mathfrak{R}$.

Consider the *vectorized* translation scheme

$$\Phi_{Hamilton} = \langle (x = x \wedge y = y); \phi_A, \phi_M \rangle$$

with

$$\phi_A(x_1, x_2, y_1, y_2, z_1, z_2) = A(x_1, y_1, z_1) \wedge A(x_2, y_2, z_2)$$

and
$\phi_M(x_1, x_2, y_1, y_2, z_1, z_2)$ is the relational form of

$$(z_1 = x_1 \times x_2 - y_1 \times y_2) \wedge (z_2 = y_1 \times x_2 + x_1 \times y_2)$$

The real and complex numbers revisited (Contd)

$\Phi^{\star}_{Hamilton}(\mathfrak{R})$ is Hamilton's definition of the complex numbers, i.e. $\Phi^{\star}_{Hamilton}(\mathfrak{R}) \simeq \mathfrak{C}$.

Moreover, $\mathfrak{A}$ is a model of RCF iff $\Phi^{\star}_{Hamilton}(\mathfrak{A})$ is an algebraically closed field of characteristic 0.

Hence $\Phi^{\star}_{Hamilton}$ is a first order reduction from $Mod(RCF)$ to $Mod(ACF_0)$ which is onto.

Theorem 17 (Tarski, A. Robinson) *RCF is decidable. In fact it allows elimination of quantifiers.*

Corollary 18 *ACF_0 is decidable.*

It is enough to prove the decidability of RCF.

Is there also an inverse reduction from $Mod(ACF)$ to $Mod(RCF)$?

The answer is NO and uses *stability theory*.

The real and complex numbers revisited (Contd)

Definition 19 (Order property)
A first order theory T has the order property *if there is a formula $\phi(\bar{x}, \bar{y})$ which linearly orders an infinite set of k-tuples.*

RCF has the order property (trivially) but ACF does not have the order property (Morley).

Theorem 20
If Φ is a reduction from $Mod(T_1)$ to $Mod(T_2)$, T_1, T_2 are complete theories and T_2 has the order property, so has T_1.

Corollary 21
There is no first order reduction from $Mod(ACF)$ to $Mod(RCF)$.

The real and complex numbers revisited (Contd)

There are now several natural questions concerning $\mathfrak{R}$.

Let RCF_1 be the Monadic Second Order theory of $\mathfrak{R}$. Is RCF_1 still recursive ?

The answer is no, and the proof is an illustration of the method of direct interpretations.

Proposition 22 (Folklore) *There is a translation scheme Φ in Monadic Second Order Logic such that for every model $\mathfrak{A}$ of RCF $\Phi^\star(\mathfrak{A})$ is isomorphic to $\mathfrak{N}$.*

Hence, by theorem 16, RCF_1 is not recursively enumerable.

The real and complex numbers revisited (Contd)

Proof:
We define in $\mathfrak{A}$ the set of natural numbers as the smallest subset of the prime field containing 0 and which is closed under the operation $x + 1$. This is clearly expressible in Monadic Second Order Logic.

Addition and multiplication are simply the restrictions to this set. $Q.E.D.$

Exercise 23
Let $\mathfrak{R}_+$ ($\mathfrak{R}_<$) be the additive (ordered) structure of $\mathfrak{R}$, i.e.
$\mathfrak{R}_+ = \langle \mathrm{IR}, + \rangle$ *and* $\mathfrak{R}_< = \langle \mathrm{IR}, < \rangle$.
Clearly, the first order theories of $\mathfrak{R}_+$ and $\mathfrak{R}_<$ are decidable by Tarski's theorem.
What can you say about the monadic second order theory of $\mathfrak{R}_+$ and $\mathfrak{R}_<$?

The real and complex numbers revisited (Contd)

The next set of questions concerns the structures

$$\mathfrak{R}_{sin} = \langle \mathrm{IR}, +, \times, sin, 0, 1 \rangle$$

and

$$\mathfrak{R}_{exp} = \langle \mathrm{IR}, +, \times, exp, 0, 1 \rangle$$

where sin and exp are the usual unary real functions.
We denote by RCF_{sin} (RCF_{exp}) the corresponding first order theories.

Theorem 24 (Folklore)
There is a first order translation scheme Φ such that for every model $\mathfrak{A}$ of RCF_{sin} $\Phi^\star(\mathfrak{A})$ is a model of true arithmetic TA.

Hence, by theorem 16, RCF_{sin} is not recursively enumerable.

The real and complex numbers revisited (Contd)

Proof:
A number is positive iff it is a square. Hence the linear ordering is definable.

The number π is definable as the least positive zero of sin. With this we can define integer multiples of π, and hence the natural numbers. $Q.E.D.$

Exercise 25
What can we say about the complex exponential function in

$$\mathfrak{C}_{exp}\langle \mathbb{C}, +, \times, exp, 0, 1\rangle$$

Hint*: Look at* $e^x = 1$.

The real and complex numbers revisited (Contd)

In contrast to RCF_{sin}, Tarski conjectured that RCF_{exp} is decidable.

In the last 40 years this conjecture has challenged many model theorists. Their joint effort has culminated in

Theorem 26 (Wilkie 1993)
RCF_{exp} *allows elimination of quantifiers up to existential formulas (is model complete).*

Theorem 27 (MacIntyre and Wilkie 1995)
Assuming Shanuel's conjecture, RCF_{exp} *is decidable.*

Related results hold for a wide class of real valued functions called *Pfaffian functions*, but this goes beyond these lectures.

D. Marker, Model Theory and Exponentiation, Notices of the AMS, vol. 43.7, July 1996, pp. 753-759.

Conjecture 28 (Shanuel's concecture)

Let $a_1, \ldots, a_n \in \mathbb{R}$ be linearly independent over the rationals. Let F be the subfield of $\mathfrak{R}$ generated by

$$\{a_1, \ldots, a_n, e^{a_1}, \ldots, e^{a_n}\}$$

Then the transcendence degree of F over $\mathfrak{Q}$ is at least n.

The **conjecture implies:**
- the Lindemann-Weierstrass theorem,
- the Gelf'and-Schneider-Baker theorem and
- the algebraic independence of π and e.

The last statement is still an **open problem**.

A. Baker, Transcendental Number Theory, Cambridge University Press 1975

The Undecidability of Arithmetic

Let us denote by $\mathfrak{N}$ the τ_{arith}–structure

$$\mathfrak{N} = \langle \mathbb{N}, succ, +, \times, 0, 1\rangle$$

and by TA (True Arithmetic) the set of first order sentences true in $\mathfrak{N}$.

Theorem 29 (Gödel) TA *is not recursively enumerable. More precisely,* TA *is* Π^1_1*–complete.*

TA was the first theory proven undecidable, although the notion of recursiveness was not yet established. Gödel proved that TA is not primitive recursive.

A language is Π^1_1 if it can be defined by an universal sentence of Second Order Logic.

The notion of Π^1_1–completeness involves recursive Turing reducibility of formal languages.

Robinson Arithmetic

Robinson Arithmetic Q consists of the logical consequences of the the following axioms in $FOL(\tau_{arith})$:

$$\forall v_0 \forall v_1 (suc(v_0) = suc(v_1) \to v_0 = v_1)$$
$$\forall v_0 \neg (suc(v_0) = 0)$$
$$\forall v_0 [(\neg v_0 = 0) \to \exists v_1 (suc(v_1) = v_0)]$$
$$\forall v_0 (v_0 + 0 = v_0)$$
$$\forall v_0 \forall v_1 [v_0 + suc(v_1) = suc(v_0 + v_1)]$$
$$\forall v_0 (v_0 \cdot 0 = 0)$$
$$\forall v_0 \forall v_1 (v_0 \cdot suc(v_1) = v_0 \cdot v_1 + v_0)$$

Theorem 30 (R.A. Robinson)
Q is not recursive. Moreover, if T is a consistent extension of Q, then T is inseparable.

A theory Σ is *inseparable* if $\{\theta : \Sigma \models \theta\}$ and $\{\theta : \Sigma \models \neg\theta\}$ are efectively inseparable.

Minimal Set Theory

Let τ_{bin} be the vocabulary consisting of one binary relation symbol R (with the intuitive meaning of membership of sets).

S is the set of logical consequences of the following three axioms:

(Empty set) $\exists y \forall x \neg R(x, y)$

(Extensionality)
$\forall y_1, y_2 (\forall x (R(x, y_1) \leftrightarrow R(x, y_2)) \leftrightarrow y_1 = y_2)$

(Pairs)
$\forall x_1, x_2 \exists y \forall z (R(z, y) \leftrightarrow (z = x_1 \vee z = x_2))$

Theorem 31 (Folklore, in Monk's book)
There is a first order translation scheme Φ_1 such that $\Phi_1^\star$ is a weak reduction and onto from $Mod(S)$ to $Mod(Q)$.

(Undirected) Graphs

T_{graph} is the set of logical consequences of the following two axioms:

(Irreflexivity:) $\forall v_0 \neg R(v_0, v_0)$

(Symmetry:) $\forall v_0 \forall v_1 (R(v_0, v_1) \leftrightarrow R(v_1, v_0))$

Theorem 32 (Rabin 1965) *There is a first order translation scheme Φ_2 such that $\Phi_2^\star$ is a weak reduction and onto from $Mod(T_{graph})$ to $Mod(S)$.*

One binary relation

Let T_{bin} be the set formulas true in all structures with one binary relation.

Theorem 33 (Rabin 1965) *There is a first order translation scheme Φ_3 such $\Phi_3^\star$ is a weak reduction and onto from $Mod(T_{bin})$ to $Mod(T_{graph})$. In fact, $\Phi_3^\star$ is also a weak reduction and onto from $Mod_{fin}(T_{bin})$ to $Mod_{fin}(T_{graph})$.*

Corollary 34 (Classical Undecidability)

(Folklore, Monk)
S is essentially undecidable.

(Kalmar, 1936)
The theory of a binary relation is undecidable (in fact finitely inseparable).

(Church and Quine, 1952)
The theory of a irreflexivie, symmetric binary relation is undecidable (in fact finitely inseparable).

Decidability of Successor Functions

We look at the structure $\mathcal{N}_{suc} = \langle \mathbb{N}, suc, 0 \rangle$ where suc is the unary successor function. We denote by $S1S$ the Monadic Second Order theory of $\mathcal{N}_{suc}$.

Theorem 35 (Büchi 1959) *$S1S$ is recursive.*

Let $\mathbf{T}_n$ the full n–ary tree and $\mathcal{T}_n$ the structure $\mathcal{T}_n \langle \mathbf{T}_n, suc_1, \ldots, suc_n \rangle$, where suc_i is the unary function mapping a node into its i–th successor. We denote by SnS the Monadic Second Order theory of $\mathcal{T}_n$.

Theorem 36 (Rabin 1965) *SnS is recursive.*

Rabin's theorem is proven via Automata Theory and is probably the most powerful decidability theorem proven sofar.

Caveat complexitatem

An *elementary recursive function (on strings or integers)* is one which can be computed by some Turing machine within time bounded above by a fixed composition of exponential functions of the length of the input.

Guideline

- Polynomial time is feasible and practical.
- Simple exponential time is still *almost* feasible but not practical.
- Double exponential time is *not feasible*.
- Finitely iterated exponetial time $2^{2^{\cdot^{\cdot^{\cdot^{2^n}}}}}$ ...

Non elementarily recursive theories

Theorem 37 (Mayer 1975)
SnS (already $S1S$) is not elementary recursive.

Let $MonFOrd$ be the FOL theory of finite linear orders $\langle A, <^A, P^A \rangle$ with a distinguished unary predicate.

Let $LinOrd$ be the FOL theory of linear orders $\langle A, <^A \rangle$.

Theorem 38 (Stockmayer 1974)
$MonOrd$ is not elementary recursive.

Theorem 39 (Compton-Henson 1990)
$LinOrd$ is not elementary recursive.

Note that there is a $MSOL$-translation scheme Φ which interprets $S1S$ in $LinOrd$ ($MonFOrd$).

Using Rabin's theorem

Rabin showed how to derive most decidability results from the decidability of SnS.

He used $MSOL$ translation schemes with unary second order variables X, Y as free variables.

We illustrate this with an easy example:
Let $K_{powerset}$ be the class of Boolean (set) algebras whose universe consists of the full power set of some set A.

Clearly there is a $MSOL$ translation scheme Φ such that $\Phi^\star$ is a transduction from structures over the empty vocabulary K_{set} to $K_{powerset}$.

$$\Phi = \langle \forall v (X(v) \leftrightarrow X(v)), \\ \forall v \left((X(v) \wedge Y(v)) \leftrightarrow Z(v) \right), \ldots \rangle$$

We can now conclude that the FOL theory of $K_{powerset}$ is decidable [Skolem 1917], but not that the $MSOL$ theory is decidable.

Using Rabin's theorem (Contd)

Theorem 40 (Rabin 1965)
There is a $MSOL$-transduction $\Phi^\star$ from models of $S2S$ to Boolean Algebras (with distinguished ideals).

Corollary 41 (Tarski 1949)
The FOL theory of Boolean Algebras (with distinguihsed ideals) is decidable.

[Kozen 1980] and [Compton-Henson 1990] showed a lower bound of $ATIME(2^{\frac{2n}{logn}}, cn)$ (double exponential deterministic space).

Using Rabin's theorem (Contd)

Theorem 42 (Rabin 1965)
There is a $MSOL$-transduction $\Phi^\star$ from models of $S2S$ to models of Presburger Arithmetic $Th(\langle \mathbb{N}, +, 0, 1 \rangle)$.

Corollary 43 (Pressburger 1929)
(First order) Pressburger Arithmetic is decidable.

[Fisher and Rabin 1974, Berman 1980] showed that it is decidable in double exponential deterministic space but not in double exponential nondeterministic time, with a lower bound of $ATIME(2^{2^{cn}}, dn)$.

Using Rabin's theorem (Contd)

Theorem 44 (Rabin 1965)
There is a $MSOL$-transduction $\Phi^\star$ from models of $S2S$ to Abelian Groups.

Corollary 45 (Szmielev 1954)
The FOL theory of Abelian Groups is decidable.

[L. Lo 1984 and Compton and Henson 1990] have shown matching upper and lower bounds of the form $ATIME(2^{2^{cn}}, dn)$.

The original proof of W. Szmielev (1954) used some kind of quantifier elimination. It was later simplified using the Feferman-Vaught Theorem on theories of generalized products and the representation theorem of finitely generated Abelian groups as sums of cyclic groups.

Using Rabin's theorem (Contd)

Theorem 46 (Folklore)
There is a $MSOL$-transduction $\Phi^\star$ from models of $S2S$ to Kripke models of Temporal Logic (i.e. linear orders).

Corollary 47 (Folklore)
Temporal Logic is decidable.

Temporal Logic is the three-variable FOL-fragment of the theory of linear order with a distinguished constant.

Using Rabin's theorem (Contd) Open Problems

Problem 48 (Rabin)
Is there a $MSOL$-transduction $\Phi^\star$ from models of SnS to models of Real Closed Fields RCF?

In other words, can one get the first order decidability of RCF via $MSOL$-transductions from the monadic second order decidability of SnS ?

Definition 49
Let $\mathbf{C}$ be some complexity class. We say that a $\mathcal{L}$-theory Σ is $\mathbf{C}$-interpretation-complete if Σ is $\mathbf{C}$-decidable and every $\mathbf{C}$-decidable theory is $\mathcal{L}$-interpretable in Σ.
Similarly we can define $\mathcal{L}$-reduction-completeness.

Problem 50
Is the $MSOL$ theory of SnS complete for elementary recursively decidable theories ?

Arithmetic without multiplication

We look now at

$\mathcal{N}_{+,S} = \langle \mathbb{N}, +, S, 0, 1 \rangle$ and $\mathcal{N}_{suc,S} = \langle \mathbb{N}, suc, S, 0, 1 \rangle$ where S is any n–ary relation over $\mathbb{N}$.

We are interested in decidability questions for $\mathcal{N}_{+,S}$ and $\mathcal{N}_{suc,S}$ for various S both in First Order and Monadic Second Order Logic.

Of particular interest are the relations:

- SQ: binary, the squaring function $y = x^2$
- SQ_1: unary, the set of squares.
- D: binary, the divisibility relation x divides y
- P: unary, the set of primes.

Arithmetic without multiplication (Contd)

Proposition 51
In $\mathcal{N}_{+,SQ}$ multiplication is First Order definable.

Proof:
$x \cdot y = z$ is defined by $\exists u(z+z = u \vee u + sq(x) + sq(x) = sq(x+y))$. $Q.E.D.$

Arithmetic without multiplication (Contd)

Proposition 52
In $\mathcal{N}_{+,D}$ squaring is First Order definable.

Proof:
We first note that the linear order $x \leq y$ is definable by $\exists z(x + z = y)$. Next, we observe that the least common multiple $lcm(x, y)$ and the greatest common divisor $gcd(x, y)$ are definable using divisibility and order. Now, for x, y with $gcd(x, y) = 1$ $x \cdot y = z$ iff $z = lcm(x, y)$. Using the fact that $gcd(x, x + 1) = 1$ we can write $sq(x) = z$ iff $z+x = lcm(x, x+1)$. $Q.E.D.$

Arithmetic without multiplication (Contd)

Proposition 53
In $\mathcal{N}_{+}$ divisibility is Second Order definable.

Proof:
$div(x, y)$ iff y is a multiple of x iff y is in the smallest set which contains x and is closed under the addition of x. $Q.E.D.$
From this we get that

Theorem 54
The following theories are undecidable:

- *The First Order theories of $\mathcal{N}_{+,SQ}$ and $\mathcal{N}_{+,D}$.*
- *The Monadic Second Order theory of Presburger arithmetic.*

Arithmetic without multiplication (Contd)

Corollary 55
In $\mathcal{N}_{suc}$ addition is not Monadic Second Order definable.

Proof:
$S1S$ is decidable. If addition were definable in $S1S$, so would the Monadic Second Order theory of Presburger arithmetic, which contradicts the above theorem. $Q.E.D.$

Dickson's conjecture on primes

The situation with the prime predicate is more delicate. The only known answers are under the assumption of the linear case of Schinzel's Hypothesis (LSH) due to Dickson.

Conjecture 56 (Dickson 1904) *For $i \leq n$ let $f_i(x) = b_i x + a_i$ be integer polynomials ($b_i \geq 1$) such that no integer $m > 1$ divides the product $\prod_i f_i(k)$ for every k.*
Then there are exists infinitely many m such that all the numbers $f_i(m)$ are primes.

This is a generalization of both Dirichlet's theorem and the Twin Prime conjecture.

For a detailed discussion of Schinzel's Hypothesis, cf.

P. Ribenboim, The Book of Prime Number Records, Springer 1988.

Theorem 57
(Bateman, Jockusch and Woods 1993)

- Assume LSH. Then multiplication is First Order definable in $\mathcal{N}_{+,P}$, and hence its First Order theory is undecidable.

Surprisingly, we have the following

- Assume LSH. Then the Monadic Second Order theory of $\mathcal{N}_{suc,P}$ is decidable. Hence, addition is not Monadic Second Order definable in $\mathcal{N}_{suc,P}$.

A survey of history and recent results is:

P. Cegielski, Definability, decidability, complexity, Annals of Mathematics and Artificial Intelligence, 16 (1996), pp. 311-341.