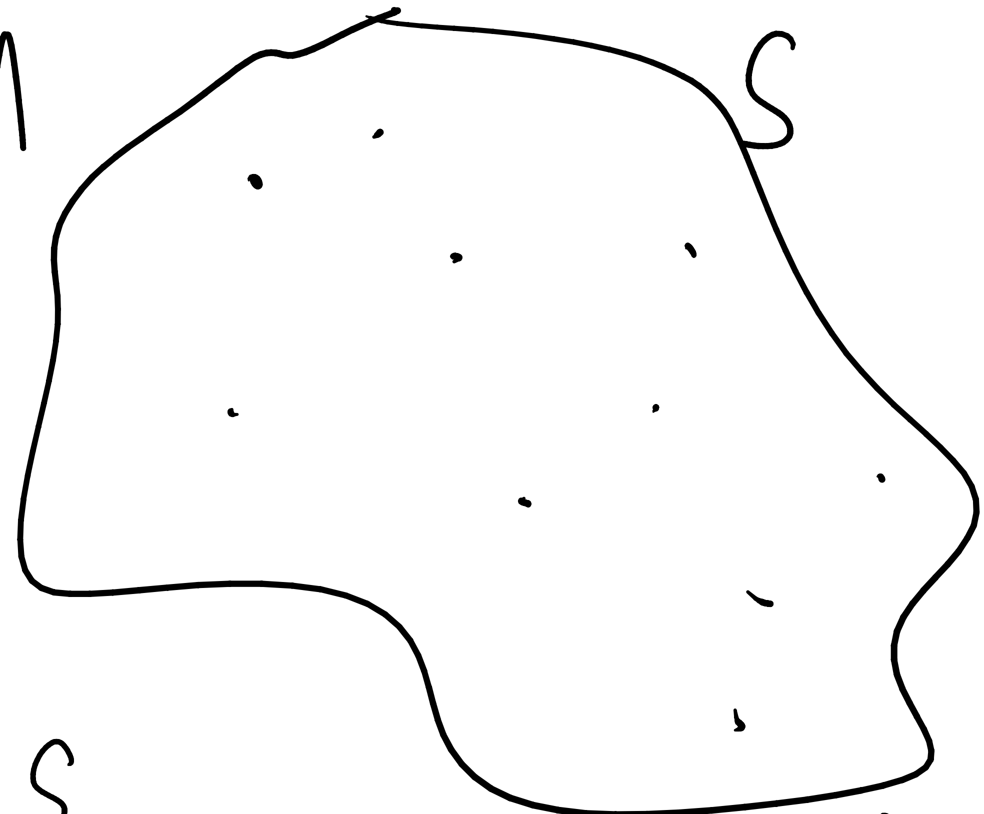
First order logic

Syntax, semantics, models, interpretations, decidability, proof systems, axiom systems, Godel's completeness theorem, strong completeness, compactness,
first-order theories, quantifier-free theories, decidable theories, Nelson-Oppen combination,
SMT, SMT solvers

Model Theory

M



S

$f_1, \ldots f_n$

$f_i : a(i)$

$f_i : S^{a(i)} \to S$

Relations : $R_1, \ldots R_m$ $\quad R_i : b(i)$

$R_i \subseteq S^{b(i)}$

Build formulas and Bool comb with quantifiers over S

$\exists \quad \forall$

Example $(\mathbb{N}, +, *, \cancel{n}, exp_2, =, <, even,$
$0, \quad prime \ldots)$

Sig: $(\{0, 1\}, \{+, *, exp\}, \{=, <, even, prime\})$

$\forall x \; \exists y \quad x < y$

$\forall x, z \; \exists y \quad x + z < y$

~~$\forall x, y \; (x < y \lor x = y \lor x > y)$~~

$\cancel{\forall} \; \exists x \quad x \neq 0$

$\neg \; \exists x \; \exists y \; \neg (x < y \lor x = y \lor \cancel{x > y} \; x + 1 < y)$

Syntax

$C = \{ c_0, c_1, \ldots \}$ Constant symbols

$F = \{ f_0, f_1, f_2, \ldots \}$ function symbols

$R = \{ R_0, R_1, R_2 \ldots \}$ relational symbols

$V = \{ v_0, v_1, v_2 \ldots \}$ variables

Terms $: t ::= c_i \mid f_i(\bar{t}) \mid v_i$

~~Functio~~

Formulas $\varphi ::= R_i(\bar{t}) \mid t_1 = t_2 \mid$
$\varphi \vee \varphi \mid \neg \varphi \mid \exists x . \varphi$

Examples:

$(\mathbb{N}, +, 0, 1)$ FOL Arithmetic with +

Presburger arithmetic

$\forall x \; \exists y \;\; x+1 < y$ Decidable

$(\mathbb{N}, +, 0, 1, *)$ FOL Arithmetic

Undecidable.

$(\mathbb{Z}, +, 0, 1)$ Decidable

$(\mathbb{Z}, +, *, 0, 1)$ Undecidable

$(\mathbb{Q}, +, 0, 1, \cancel{*})$ Decidable.

$(\mathbb{R}, +, 0, 1, *)$ Decidable

(Finite Strings or Σ, concat, rev, =, substr, even)

(Finite Arrays $\cup$ Integers, isint, isarray

Typed logic

Semantics

$$\exists x \forall y (x < y \wedge 3 * x + 4 * y > 9)$$

Universe

M : "meaning" of all functions and relations

$$3 < x$$

I: assign valuation to variables

$$M, I \models \alpha$$

Satisfiable : α is satisfiable if there is a model M s.t. $M \models \alpha$

Validity α is valid if in every model M, $M \models \alpha$.

α is satisfiable iff $\neg\alpha$ is not valid

α is ~~no~~ valid iff $\neg\alpha$ is not satisfiable.

$\exists x : R(x) \vee \neg R(x)$ Sat valid

$\exists x \; R(x)$ Sat Not valid

$\forall x, y \; (x = y \Rightarrow f(x) = f(y))$

All men are mortal

Socrates is a man.

Hence Socrates is mortal.

mortal( ) Relation

$\forall x \; \overset{\text{man}}{\cancel{\text{mortal}}}(x) \Rightarrow \text{mortal}(x)$

$\text{man}(\text{socrates})$

$\text{mortal}(\text{socrates})$

$$\Big(\Big[\forall x \, (\text{man}(x) \Rightarrow \text{mortal}(x)) \Big] \wedge \underset{\text{man}}{\cancel{\text{mortal}}}(\text{socrates}) \Big) \Rightarrow \text{mortal}(\text{socrates})$$

FOL (in general, function, relations have arbitrary meanings)

<u>Validity problem</u> : Undecidable

Satisfiability problem : Undecidable.

<u>Quantifier free fragment</u> $x = y \Rightarrow f(x) = f(y)$

Satisfiability : <u>decidable</u>

validity : decidable. Theory of "Uninterpreted functions"

Proof systems

Gödel's Completeness theorem.

There are axiom systems that are sound and complete for FOL

$$\models \alpha \quad \text{iff} \quad \vdash_{Ax} \alpha$$

Compactness theorem also holds

$$X \models \alpha \quad \text{iff} \quad \exists Y \subseteq_{fin} X \quad Y \models \alpha$$

Strong completeness

$\cancel{\emptyset}$ $\Gamma \models \alpha$ iff $\Gamma \vdash_{Ax} \alpha$

Validity : r.e

Satisfiability : <u>not</u> r.e.

Theories

A FO theory T

- Signature $\Sigma = (R, F, C)$
- Axioms A : closed FO formulae over Σ.

α is valid in theory T (is "T-valid")

if for every model M s.t.

for every $\beta \in A$, $M \models \beta$

then $M \models \alpha$

α is T-valid : $T \models \alpha$

T_E - Theory of equality

$\equiv$

$$\forall x \quad x \equiv x$$

$$\forall x, y \quad x \equiv y \Rightarrow y \equiv x$$

$$\forall x, y, z \; (x \equiv y \wedge y \equiv z) \Rightarrow (x \equiv z)$$

$$\forall \bar{x}, \bar{y} \left[\left(\bigwedge_{i=1}^{n} x_i \equiv y_i \right) \Rightarrow f(\bar{x}) \equiv f(\bar{y}) \right]$$

$$\forall \bar{x}, \bar{y} \left[\left(\bigwedge_{i=1}^{n} x_i \equiv y_i \right) \Rightarrow \left(r(\bar{x}) \Leftrightarrow r(\bar{y}) \right) \right]$$

T

Let $X_T = \{\alpha \mid T \vDash \alpha\}$

$= \{\alpha \mid T \vdash_{Ax} \alpha\}$

T has no model! X_T = all formulas!

$\beta, \neg\beta, \perp$ $p \wedge \neg p$

T is consistent if it has at least one model.

T could have more than one model

When T has more than zero models

- All models agree with each other

i.e. $\forall M, M'$ where M and M' sat all axioms of T

$\forall \alpha . \quad M \models \alpha$ iff $M' \models \alpha$.

$X_T = \{ \alpha \mid T \models \alpha \}$

X_T will never have β and $\neg\beta$.

For any α, either α or $\neg\alpha$ will be in X.

X_T is <u>complete</u>.

It could happen that T is incomplete
but consistent.

Some models of T satisfy α
and some don't.

$$T \not\models \alpha \qquad T \nvdash_{Ax} \alpha$$

$$T \not\models \neg\alpha \qquad T \nvdash_{Ax} \neg\alpha$$

Gödel's first incompleteness theorem.

Arithmetic with $(+, \times)$ (and in fact anything that includes arithmetic) does not have a consistent and complete (finitary) axiomatization.

Overview of various theories

From Calculus of Computation (switch to this text)

- Theory of equality ("uninterpreted functions")
- Peano arithmetic (natural numbers, 0, 1, +, *)
- Presburger arithmetic (natural numbers, 0, 1, +)
- Integers with above two sets of signatures
- Reals (reals, 0, 1, +, -, *, =, $\leq$)
- Rationals (rationals, 0, 1, +, -, =, $\leq$)
  [same as reals with this signature]
- Recursive data structures
  - Lists, cons, car, cdr, atom, =
  - RDS in general : constructors, projections, atom, =
- Arrays

Theory	Full FO logic	Quanti free frag
Equality (uninterpreted fns)	Undecidable	Decidable
Peano arithmetic (+, *)	Undecidable	Undecidable
Presburger arithmetic (+)	Dec	Dec
Linear integers (+)	Dec	Dec
Reals (+, *)	Dec (QE)	Dec
Rationals (only +)	Dec (QE)	Dec
Rec data str (incl lists)	Undec	Dec
Arrays (with or without extensionality)	Undec.	Dec

Nonlinear arithmetic

Complexity of decidable theories

Theory	Complexity
PL	NP-complete
$T_{\mathbb{N}}$, $T_{\mathbb{Z}}$	$\Omega\left(2^{2^{n}}\right)$, $O\left(2^{2^{2^{kn}}}\right)$
$T_{\mathbb{R}}$	$O\left(2^{2^{kn}}\right)$
$T_{\mathbb{Q}}$	$\Omega\left(2^{n}\right)$, $O\left(2^{2^{kn}}\right)$
T_{RDS}^{+}	not elementary recursive

Complexity of quantifier-free conjunctive fragments

Theory	Complexity	Theory	Complexity
PL	$\Theta(n)$	T_{E}	$O(n \log n)$
$T_{\mathbb{N}}$, $T_{\mathbb{Z}}$	NP-complete	$T_{\mathbb{R}}$	$O\left(2^{2^{kn}}\right)$
$T_{\mathbb{Q}}$	PTIME	T^{+}_{RDS}	$\Theta(n)$
T_{RDS}	$O(n \log n)$	T_{A}	NP-complete

Combination theories

$x = y+2 \wedge A[x] = 3 \wedge A[y] = 5$

$T_1 \quad : \quad \Sigma_1, \mathcal{A}_1 \qquad \Sigma_1 \cap \Sigma_2 \subseteq \{=\}$

$T_2 \quad : \quad \Sigma_2, \mathcal{A}_2$

$T_1 \cup T_2 \quad : \quad \Sigma_1 \cup \Sigma_2, \quad \mathcal{A}_1 \cup \mathcal{A}_2$

Nelson-Oppen

NO theorem

If $T_1 = \Sigma_1, A_1$ has a decidable quantifier free theory

and $T_2 = \Sigma_2, A_2$ has a decidable quantifier free theory

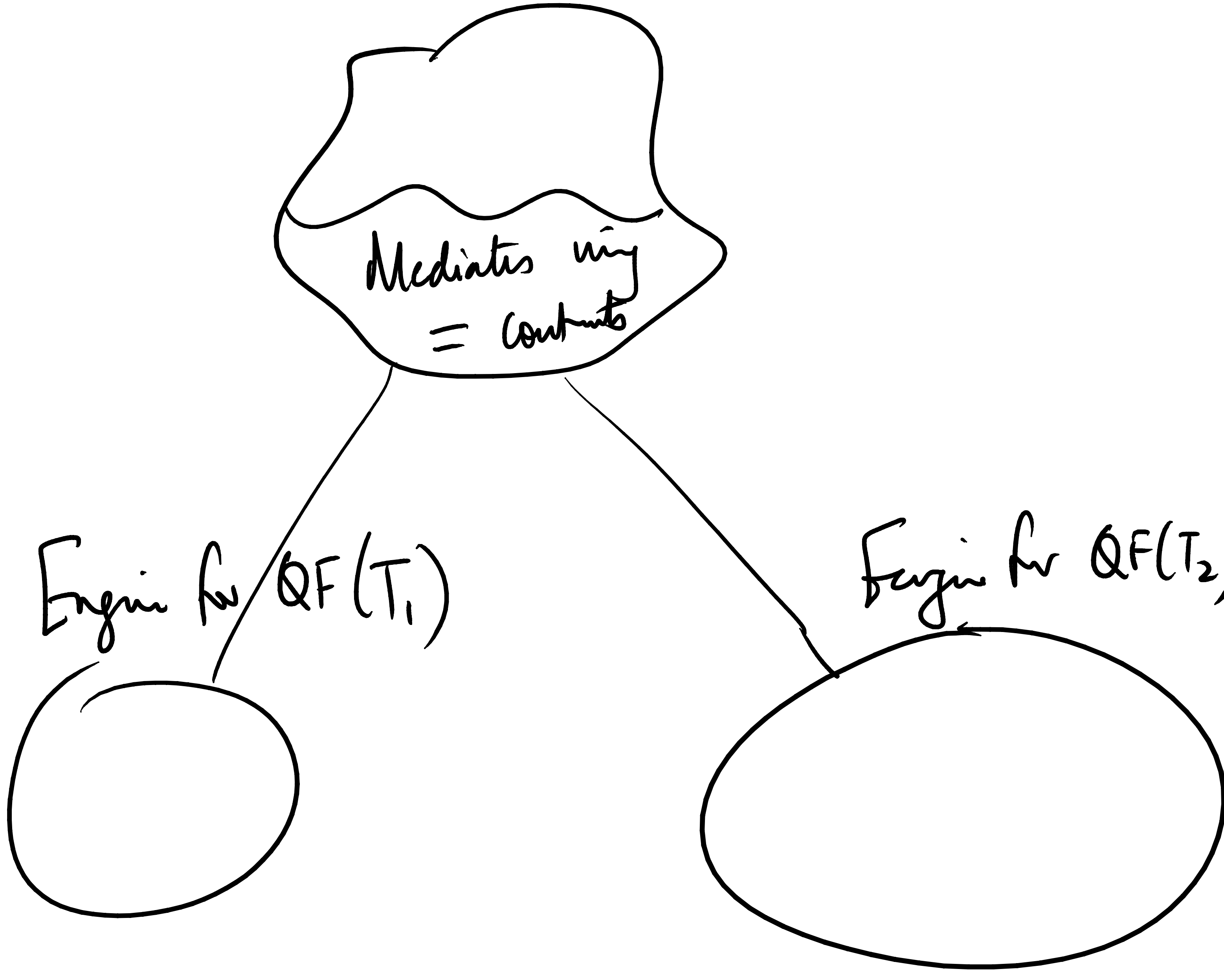
and $\Sigma_1 \cap \Sigma_2 = \{=\}$

and a technical condition

then the quant free theory of $T_1 \cup T_2$ is decidable.

~~Path~~ Technical condition: Stably infinite.

Any formula which is sat must be sat in a <u>infinite model</u>.


Mediates using = constants
Engine for QF(T1)
Engine for QF(T2)

SMT solvers

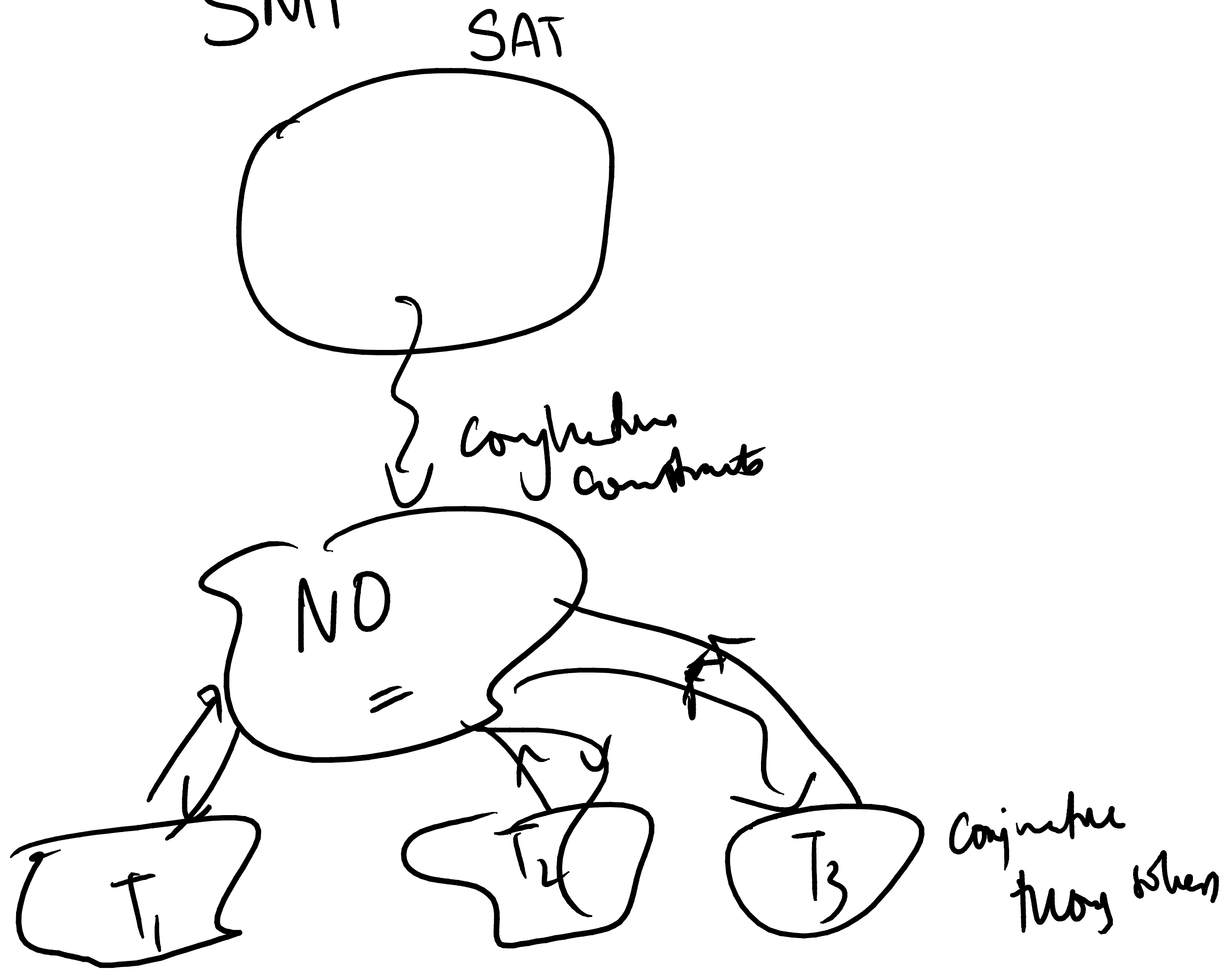
- Support decision procedures for quantifier free fragments of the theories we have seen

 (and a semi decision procedure for Peano arithmetic)

- Support Nelson-Oppen combination of qf fragments of these theories as well

~~Examples~~

SMT



SMT solver Z3

- Propositional logic
- Using various theories
- Using combination of theories
- See Z3 Tutorial