SMT Solving: Combined Theories

Shaowei Cai

Institute of Software, Chinese Academy of Sciences

Constraint Solving (2022. Autumn)

Reminders: theories and signatures

- A first-order theory T is defined by the following components.

  1. Its signature Σ is a set of constant, function, and predicate symbols.

  2. Its set of axioms $\mathcal{A}$ is a set of closed FOL formulae in which only constant, function, and predicate symbols of Σ appear.

- A Σ-formula is constructed from constant, function, and predicate symbols of Σ, as well as variables, logical connectives, and quantifiers.

Reminders: T-satisfiability

- Given a FOL formula F and interpretation $I: (D_I, \alpha_I)$, we want to compute if F evaluates to true under interpretation I, I ⊨ F, or if F evaluates to false under interpretation I, I ⊭F.

- T – interpretation: an interpretation satisfying $I \models$ A for every A $\in \mathcal{A}$.

- A Σ-formula F is satisfiable in T , or T -satisfiable, if there is a T-interpretation I that satisfies F.

Combining Theories

- We know how to decide EUF and Linear Integer Arithmetic :

  EUF: $(x_1 = x_2) \lor \neg(f(x_2) = x_3) \land \cdots$

  LIA: $3x_1 + 5x_2 \geq 2x_3 \land x_2 \leq 4x_4 \ldots$

- What about a combined formula ?

$$(x_2 \geq x_1) \land (x_1 - x_3 \geq x_2) \land (x_3 \geq 0) \land f\big(f(x_1) - f(x_2)\big) \neq f(x_3)$$

The Theory-Combination problem

- Given theories T_1 and T_2 with signatures Σ_1 and Σ_2, the combined theory $T_1 \oplus T_2$
  - has signature $\Sigma_1 \cup \Sigma_2$ and
  - the union of their axioms.

- Let F be a $\Sigma_1 \cup \Sigma_2$-formula.
- The problem: Does $T_1 \oplus T_2 \models F$?

The Theory-Combination problem

- The Theory-Combination problem is undecidable (even when the individual theories are decidable).

- Under certain restrictions, it becomes decidable.

- We will assume the following restrictions:
  - T_1 and T_2 are decidable, quantifier-free first-order theories with equality;
  - Disjoint signatures (except =): $\Sigma_1 \cap \Sigma_2 = \{=\}$;
  - T_1 and T_2 are stably infinite (we will discuss this later).

The Theory-Combination problem

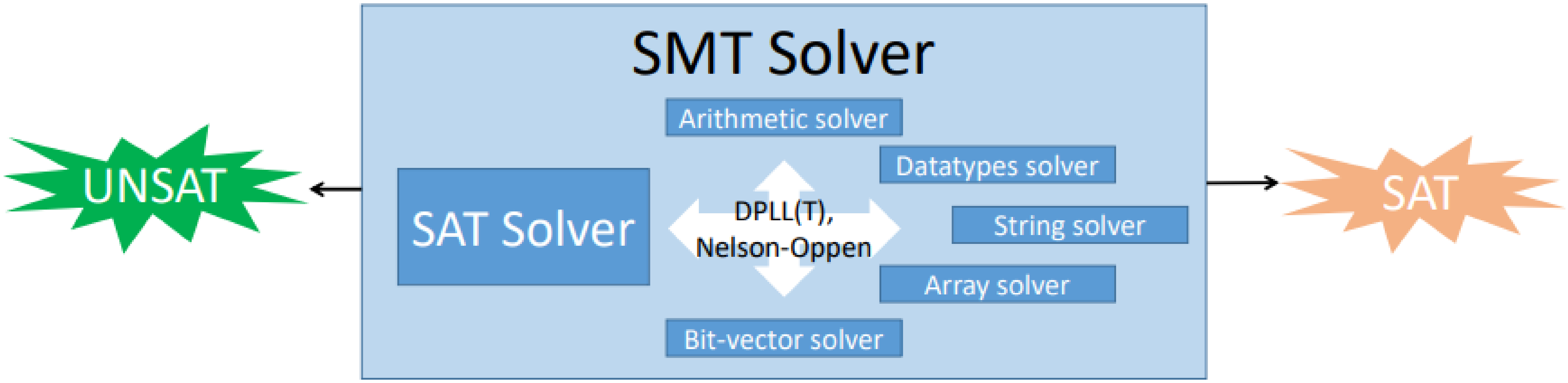
- We can reduce all theories to a common logic (e.g. Propositional Logic).

- But here, we focus on the Nelson-Oppen method
  - Combine decision procedures of the individual theories.

  - Greg Nelson and Derek Oppen, *simplification by cooperating decision procedures*, 1979

The Nelson-Oppen method

By utilizing DPLL(T), when deciding combined theories, we can focus on conjunctive fragments.



The Nelson-Oppen method

Step1: Purification: validity-preserving transformation of the formula after which predicates from different theories are not mixed.

Continue replacing a minimal "alien" expression e by a fresh variable a and add $a = e$ until no more "alien" expressions.

E.g. Transform $x_1 \leq f(x_1)$

..into $x_1 \leq a_1 \wedge a_1 = f(x_1)$

The Nelson-Oppen method

Step1: Purification: validity-preserving transformation of the formula after which predicates from different theories are not mixed.

$$x_2 \geq x_1 \wedge x_1 - x_3 \geq x_2 \wedge x_3 \geq 0 \wedge f\big(f(x_1) - f(x_2)\big) \neq f(x_3)$$

$$\Downarrow$$

$$x_2 \geq x_1 \wedge x_1 - x_3 \geq x_2 \wedge x_3 \geq 0 \wedge f(a) \neq f(x_3) \wedge \mathrm{a} = f(x_1) - f(x_2)$$

$$\Downarrow$$

$$x_2 \geq x_1 \wedge x_1 - x_3 \geq x_2 \wedge x_3 \geq 0 \wedge f(a) \neq f(x_3)$$
$$\wedge\, \mathrm{a} = a_1 - a_2 \wedge a_1 = f(x_1) \wedge a_2 = f(x_2)$$

The Nelson-Oppen method

- After purification we are left with several sets of pure expressions $F_1 \dots F_n$:
  - F_i belongs to some 'pure' theory which we can decide.
  - Shared variables are allowed.
  - ϕ is satisfiable $\leftrightarrow$ $F_1 \wedge \cdots \wedge F_n$ is satisfiable

$$x_2 \geq x_1 \wedge x_1 - x_3 \geq x_2 \wedge x_3 \geq 0 \wedge f(a) \neq f(x_3)$$
$$\wedge\, \mathrm{a} = a_1 - a_2 \wedge a_1 = f(x_1) \wedge a_2 = f(x_2)$$

$$\Downarrow$$

$$\phi_1: \quad x_2 \geq x_1 \wedge x_1 - x_3 \geq x_2 \wedge x_3 \geq 0 \wedge \mathrm{a} = a_1 - a_2$$
$$\wedge$$
$$\phi_2: \quad f(a) \neq f(x_3) \wedge a_1 = f(x_1) \wedge a_2 = f(x_2)$$

The Nelson-Oppen method: A Basic Algorithm

1. Purify ϕ into $F_1 \land \cdots \land F_n$
2. If ∃i, F_i is unsatisfiable, return `unsatisfiable' .
3. If ∃i, j. F_i implies an equality not implied by F_j , add it to F_j and goto step 2.
4. Return `satisfiable'.

The algorithm runs in polynomial time, if the conjunctive fragments of T_1 and T_2 can be decided in polynomial time.

Example

$$(x_2 \geq x_1) \ \wedge (x_1 - x_3 \geq x_2) \wedge (x_3 \geq 0) \wedge f\big(f(x_1) - f(x_2)\big) \neq f(x_3)$$

- Purification:

$$F_1: \quad x_2 \geq x_1 \wedge x_1 - x_3 \geq x_2 \wedge x_3 \geq 0 \wedge \mathrm{a} = a_1 - a_2$$

$$\wedge$$

$$F_2: \quad f(a) \neq f(x_3) \wedge a_1 = f(x_1) \wedge a_2 = f(x_2)$$

Example

Arithmetic	EUF
$x_2 \geq x_1$ $x_1 - x_3 \geq x_2$ $x_3 \geq 0$ $a_1 = a_2 - a_3$	$f(a_1) \neq f(x_3)$ $a_2 = f(x_1)$ $a_3 = f(x_2)$
$\boxed{x_3 = 0}$	$x_3 = 0$
$\boxed{x_1 = x_2}$	$x_1 = x_2$
$a_2 = a_3$	$\boxed{a_2 = a_3}$
$\boxed{a_1 = 0}$	$a_1 = 0$
	$\boxed{\text{False}}$

Wait, it’s not so simple…

- Consider: $\varphi: 1 \leq x \wedge x \leq 2 \wedge p(x) \wedge \neg p(1) \wedge \neg p(2)$

  $x \in \mathrm{Z}$

Arithmetic over Z	Uninterpreted predicates
$1 \leq x$ $x \leq 2$	$p(x)$ $\neg p(1)$ $p(2)$

- Neither theories imply an equality, and both are satisfiable.
- But ϕ is unsatisfiable!

Convexity of Theories

- Definition: A Σ-theory T is *convex* if for every conjunctive Σ-formula F,

$$\mathrm{F} \rightarrow \bigvee_{i=1..n} x_i = y_i\,, for\ some\ n > 1 \Rightarrow$$

$$\mathrm{F} \rightarrow x_i = y_i, for\ some\ i \in \{1..n\}$$

where x_i, y_i are some T variables.

- *Convex*: Linear Arithmetic over R, EUF
- *Non-convex*: Almost anything else…

Convexity of Theories: examples

Linear arithmetic over Z is not convex.

For example, while

$$x_1 = 1 \land x_2 = 2 \land 1 \leq x_3 \land x_3 \leq 2 \Rightarrow (x_3 = x_1 \lor x_3 = x_2)$$

holds, neither

$$x_1 = 1 \land x_2 = 2 \land 1 \leq x_3 \land x_3 \leq 2 \Rightarrow x_3 = x_1$$

nor

$$x_1 = 1 \land x_2 = 2 \land 1 \leq x_3 \land x_3 \leq 2 \Rightarrow x_3 = x_2$$

holds

LRA is Convex

Definition: A Σ-theory T is *convex* if for every conjunctive Σ-formula F,

$$F \to \bigvee_{i=1..n} x_i = y_i\,, for\ some\ n > 1 \Rightarrow F \to x_i = y_i, for\ some\ i \in \{1..n\}$$

Denote G: $\bigvee_{i=1..n} x_i = y_i$

Intuition: let us view an assignment of all variables as a point.

S(F): the set of points satisfying F; S(G) similarly.

F → G means, if a point is in S(F), then it is also in S(G) .

Intuition:

F cannot be covered by any disjunction of equalities, no matter how many, if no single equality covers F.

A polyhedron F cannot be covered by a finite disjunction of planes unless at least one of the planes is F itself.

LRA is Convex

Proof idea:

- F is a conjunction of linear rational equations/inequations. ⇒ F is convex.
- Suppose F →G, but for no $i \in \{1..n\}$ does F → $x_i = y_i$, we will prove that then F is not convex. This leads to a contradiction.

LRA is Convex

Proof:

- Each equality $x_i = y_i$ is convex: for an equality x=y, if two points $\vec{u}, \vec{v}$ satisfies the equality, then for any $\lambda \in (0,1), \lambda\vec{u} + (1-\lambda)\vec{v}$ also satisfies the equality.
- But the disjunction G is not convex (e.g. H: $x = y \vee x = z$, the points (0,0,1) and (1,0,1) are in the set of points satisfying H, denoted as S(H), but $\frac{1}{2}(0,0,1) + \frac{1}{2}(1,0,1)$=($\frac{1}{2}$,0,1) is not in S(H)).
- Indeed, S(G) consists of $S_{x_i=y_i}$ for each equation$x_i = y_i$.

LRA is Convex

- Suppose, then, that F →G : $\bigvee_{i=1..n} x_i = y_i$, but for no i ∊ $\{1..n\}$ does F → $x_i = y_i$.
- Then there must be two points $\vec{u}$ *and* $\vec{v}$ in S(F), they are in separate subsets of S(G).
  - otherwise, if all points are in the same subset, that means all points satisfy the same equality, F → $x_i = y_i$ for some i.
- By the arguments above, the points on the line segment between $\vec{u}$ *and* $\vec{v}$ are not in S(G) and thus not in S(F).

  ⇒ F is not convex.

This leads to a contradiction.

So why is convexity important ?

- Recall: $\varphi: 1 \leq x \wedge x \leq 2 \wedge p(x) \wedge \neg p(1) \wedge \neg p(2)$
  $x \in Z$

Arithmetic over Z	Uninterpreted predicates
$1 \leq x$ $x \leq 2$	$p(x)$ $\neg p(1)$ $p(2)$

- Neither theories imply an equality, and both are satisfiable.

Propagate Disjunction for Non-Convex Theories

- But: $1 \leq x \wedge \mathrm{x} \leq 2$ imply the disjunction $x = 1 \vee \mathrm{x} = 2$

- Since the theory is non-convex we cannot propagate either $x = 1$ or $\mathrm{x} = 2$.

- We can only propagate the disjunction itself.

Propagate Disjunction for Non-Convex Theories

- Propagate the disjunction and perform case-splitting.

Arithmetic over Z	Uninterpreted predicates
$1 \le x$	$p(x)$
$x \le 2$	$\neg p(1) \land \neg p(2)$
$\boxed{x = 1 \lor x = 2}$	$x = 1 \lor x = 2$ *Split!*
	$\langle\cdot\rangle \land \mathrm{x} = 1 \quad\Big|\quad \langle\cdot\rangle \land \mathrm{x} = 2$
	False $\quad$ False

The Nelson-Oppen Method: the Full Algorithm

1. Purify ϕ into ϕ': $F_1 \wedge \cdots \wedge F_n$
2. If ∃i, F_i is unsatisfiable, return `unsatisfiable' .
3. If ∃i, $j. F_i$ implies an equality not implied by F_j , add it to F_j and goto step 2.
4. If ∃i, $F_i \rightarrow (x_1 = y_1 \vee \cdots \vee x_k = y_k)$but ∃$j$ $F_i \nrightarrow x_j = y_j$, apply recursively to φ'∧ $x_1 = y_1$, ... φ' ∧ $x_k = y_k$. If any of them is satisfiable, return 'satisfiable'. Otherwise return 'unsatisfiable'.
5. Return `satisfiable'.

The algorithm runs in exponential time, even if the conjunctive fragments of T_1 and T_2 can be decided in polynomial time.

Why the theories need to be Stably Infinite?

Example.

- T_1 : $\Sigma_1 = \{f, =\}$, axioms enforce solutions with at most two distinct values.
- T_2 : $\Sigma_1 = \{g, =\}$, axioms...

f and g are function symbols.

- The combined theory $T_1 \oplus T_2$ contains the union of the axioms, and thus, the solution to any formula $\phi \in T_1 \oplus T_2$ cannot have more than two distinct values.

Consider this formula: $f(\mathrm{x}_1) \neq f(x_2) \wedge g(x_1) \neq g(x_3) \wedge g(x_2) \neq g(x_3)$

No equalities are propagated, and the algorithm returns Satisfiable. Error!
In fact, the formula is unsatisfiable, because any assignment satisfying it must use three different values for x_1, x_2 and x_3.

F_1 (a Σ_1-formula)	F_2 (a Σ_2-formula)
$f(x_1) \neq f(x_2)$	$g(x_1) \neq g(x_3)$ $g(x_2) \neq g(x_3)$

Stably Infinite Theories

A Σ -theory is stably infinite if every satisfiable formula has a model with an infinite domain.

Examples of Stably infinite theories

- LIA and LRA: Linear integer arithmetic, Linear real arithmetic
- EUF: Equality logic with uninterpreted functions

Examples of non-stably infinite theories

- $\Sigma = \{a, b, =\}$ axiom: $\forall x.\ x = a \vee x = b$
- Theory of fixed width bit vectors: BV

There are extensions of Nelson-Oppen method that can handle non-stably infinite theories.
C. Tinelli and C. Zarba. Combining non-stably infinite theories.
Journal of Automated Reasoning, 34(3):209{238, 2005.

Nelson-Oppen Method: Nondeterministic Version

- In practice, Nelson-Oppen method is based on the deterministic method we just described.

- There is a nondeterministic version, which is easier to understand and to prove the correctness.
  - The purification phase is the same.
  - For the equality propagation phase, the nondeterministic version adopts a guess-and-check favor, instead of the construction favor in the deterministic version.

Nelson-Oppen Method: Nondeterministic Version

Purification phase separates $(\Sigma_1 \cup \Sigma_2)$-formula F into two formulas, Σ_1-formula F_1 and Σ_2-formula F_2.

F_1 and F_2 are linked by a set of shared variables.

- Let V = shared(F_1, F_2) = free(F_1) $\cap$ free(F_2)
- Let E be an equivalence relation over shared (F_1, F_2).
- The arrangement $\alpha(V, E)$ of V induced by E is the formula:

$$\alpha(V, E) : \bigwedge_{u,v \,\in\, V.\ uEv} u = v \ \wedge \bigwedge_{u,v \,\in\, V.\ \neg(uEv)} u \neq v$$

F is $T_1 \oplus T_2$ -satisfiable iff there exists an equivalence relation E of V such that $F_1 \wedge \alpha(V, E)$ is T_1–satisfiable, and $F_2 \wedge \alpha(V, E)$ is T_2–satisfiable.

Nelson-Oppen Method: Nondeterministic Version

We can check the equivalence relation over V, one by one

- Once an equivalence relation E makes $F_1 \wedge \alpha(V, E)$ be T_1−satisfiable and $F_2 \wedge \alpha(V, E)$ be T_2−satisfiable, then we show that F is satisfiable

- If all the equivalence relations over V have been checked and failed, then F is unsatisfiable.

Example

Example

$$F: 1 \le x \wedge x \le 2 \wedge f(x) \neq f(1) \wedge f(x) \neq f(2)$$

The purification phase separates it into a $\Sigma_{\mathbb{Z}}$-formula F_1 and a Σ_{EUF}-formula F_2.

$$F_1: 1 \le x \wedge x \le 2 \wedge w_1 = 1 \wedge w_2 = 2$$

$$\wedge$$

$$F_2: \quad f(x) \neq f(w_1) \wedge f(x) \neq f(w_2)$$

Then, V = shared(F_1, F_2)= $\{x, w_1, w_2\}$

Example

- There are 5 equivalence relations to consider:

1. $\{\{x, w_1, w_2\}\}$, *i.e.*, $x = w_1 = w_2$: $F_{\mathsf{E}} \wedge \alpha(V, E)$ is T_{E}-unsatisfiable because it cannot be the case that both $x = w_1$ and $f(x) \neq f(w_1)$.
2. $\{\{x, w_1\}, \{w_2\}\}$, *i.e.*, $x = w_1$, $x \neq w_2$: $F_{\mathsf{E}} \wedge \alpha(V, E)$ is T_{E}-unsatisfiable because it cannot be the case that both $x = w_1$ and $f(x) \neq f(w_1)$.
3. $\{\{x, w_2\}, \{w_1\}\}$, *i.e.*, $x = w_2$, $x \neq w_1$: $F_{\mathsf{E}} \wedge \alpha(V, E)$ is T_{E}-unsatisfiable because it cannot be the case that both $x = w_2$ and $f(x) \neq f(w_2)$.
4. $\{\{x\}, \{w_1, w_2\}\}$, *i.e.*, $x \neq w_1$, $w_1 = w_2$: $F_{\mathbb{Z}} \wedge \alpha(V, E)$ is $T_{\mathbb{Z}}$-unsatisfiable because it cannot be the case that both $w_1 = w_2$ and $w_1 = 1 \ \wedge \ w_2 = 2$.
5. $\{\{x\}, \{w_1\}, \{w_2\}\}$, *i.e.*, $x \neq w_1$, $x \neq w_2$, $w_1 \neq w_2$: $F_{\mathbb{Z}} \wedge \alpha(V, E)$ is $T_{\mathbb{Z}}$-unsatisfiable because it cannot be the case that both $x \neq w_1 \ \wedge \ x \neq w_2$ and $x = w_1 = 1 \vee x = w_2 = 2$ (since $1 \leq x \leq 2$ implies that $x = 1 \vee x = 2$ in $T_{\mathbb{Z}}$).

Hence, F is $(T_{\mathsf{E}} \cup T_{\mathbb{Z}})$-unsatisfiable. ■

Nelson-Oppen Method: Nondeterministic Version

- Phase 2 is formulated as “guess and check”: first, guess an equivalence relation E, then check the induced arrangement.
- Unfortunately, the number of equivalence relations is given by the sequence of Bell numbers, which grows super-exponentially.
  - For example, just 12 shared variables induce over four million equivalence relations.
- However, there is no need to guess the entire equivalence relation at once; instead, construct it incrementally.

Correctness of the Nelson-Oppen Method

- We reason at the level of arrangements, which is more suited to the nondeterministic version of the method.
- However, we have shown how to construct an arrangement in the deterministic version, so the proof can be extended to the deterministic version.
- We assume the purification phase is correct.

Correctness of the Nelson-Oppen Method

Theorem (Sound & Complete of Nelson-Oppen).

Consider stably infinite theories T_1 and T_2 such that $\Sigma_1 \cap \Sigma_2 = \{=\}$.

For conjunctive quantifier-free Σ_1 -formula F_1 and conjunctive quantifier-free Σ_2 -formula F_2, $F_1 \wedge F_2$ is $(T_1 \oplus T_2)$-satisfiable iff

there exists an arrangement K = α(shared(F_1, F_2),E) such that $F_1 \wedge K$ is T_1 -satisfiable and $F_2 \wedge K$ is T_2 -satisfiable.

Proof of Soundness

Soundness if straightforward.

- Suppose that $F_1 \wedge F_2$ is $(T_1 \oplus T_2)$-satisfiable with a satisfying $(T_1 \oplus T_2)$-interpretation I.

- Extract from I the equivalence relation E such that the arrangement

  K = α(V = shared(F_1, F_2),E) is satisfied by I.

- Then $F_1 \wedge K$ and $F_2 \wedge K$ are both satisfied by I, which can be viewed as both a T_1 -interpretation and a T_2 -interpretation, so that they are T_1-satisfiable and T_2 -satisfiable, respectively.

- In other words, if the N.O. returns unsatisfiable, then $F_1 \wedge F_2$ is unsatisfiable.

Proof of Completeness

- Let K = α(V = shared(F_1, F_2),E) be an arrangement such that $F_1 \wedge K$ is T_1-satisfiable and $F_2 \wedge K$ is T_2-satisfiable. We want to prove that, $F_1 \wedge F_2$ is $(T_1 \oplus T_2)$-satisfiable.

Proof sketch:

- We suppose that $F_1 \wedge F_2$ is $(T_1 \oplus T_2)$-unsatisfiable, and derive a contradiction.
- $F_1 \wedge F_2$ is $(T_1 \oplus T_2)$-unsatisfiable $\Rightarrow$ $F_1 \rightarrow \neg F_2$
- Using Craig Interpolation Lemma, we show that

there is a quantifier-free formula H, such that $F_1 \rightarrow H$ over all infinite T_1-interpretations, and $H \rightarrow \neg F_2$, equally $F_2 \rightarrow \neg H$, over all infinite T_2-interpretations.

- We then show that K $\rightarrow H$, which means $F_2 \rightarrow \neg K$ over all infinite T2-interpretations.
- In other words, no infinite T2-interpretation satisfies $F_2 \wedge K$.
- But, if T_2 is stably infinite and $F_2 \wedge K$ is T_2-satisfiable as assumed, then $F_2 \wedge K$ is satisfied by some infinite T_2-interpretation, a contradiction.

Compactness Theorem. A countable set of first-order formulae S is simultaneously satisfiable iff the conjunction of every finite subset is satisfiable.

- Let S_1 be conjunction of a finite subset of axioms of T_1 and S_2 a conjunction of a finite subset of axioms of T_2. Choose S_1 and S_2 to include the axioms that imply reflexivity, symmetry, and transitivity of equality.

- Since $F_1 \wedge F_2$ is $(T_1 \oplus T_2)$-unsatisfiable, the Compactness Theorem tells us $S_1 \wedge F_1 \wedge S_2 \wedge F_2$ is unsatisfiable.

- Then, rearranging, we have $S_1 \wedge F_1 \Rightarrow \neg S_2 \vee \neg F_2 \qquad (a)$

Craig Interpolation Lemma

If $\phi_1 \to \phi_2$, then there exists a formula H such that $\phi_1 \to H$ and $H \to \phi_2$, and each free variable, function symbol, and predicate symbol of H appears in ϕ_1 and ϕ_2.

- Using Craig Interpolation Lemma, according to (a), there exists an interpolant H′ such that free(H′) = shared(F_1, F_2) and $S_1 \land F_1 \Rightarrow H'$ *and* $S_2 \land H' \Rightarrow \neg F_2$ (b)

  (The latter implication is derived by rearranging $\mathrm{H}' \Rightarrow \neg S_2 \lor \neg F_2$)
- Because = is the only predicate or function shared between $S_1 \land F_1$ and $S_2 \land F_2$,

  H′ is of a special form: its atoms are equalities between variables of shared(F_1, F_2) .

- However, H′ may have quantifiers.
- We prove next that in fact a "weak" quantifier free interpolant H exists.

- What is “weakly equivalent”?

- We define $\Rightarrow*$ as a weaker form of implication: F $\Rightarrow*$ G iff G is true on every interpretation I that has an infinite domain and that satisfies F.
- Similarly, weaken $\Leftrightarrow$ to $\Leftrightarrow*$.

- If F $\Rightarrow*$ G, we say that F weakly implies G;
- if F $\Leftrightarrow*$ G, we say that F is weakly equivalent to G.

- Note: since we are considering only stably infinite theories, we need only consider interpretations with infinite domains. We can extend a T1- or T2-interpretation with a finite domain to a T1- or T2-interpretation with an infinite domain.

Lemma (Weak Quantifier Elimination for Pure Equality). Consider any stably infinite theory T with equality. For each pure equality formula F, there exists a quantifier-free pure equality formula F′ such that F is weakly T-equivalent to F′.

Proof. Consider pure equality formula $\exists x.\ G[x, \overline{y}]$, where G is quantifier-free with free variables x and $\overline{y}$. Define

$$G_0 :\ G\{x = x \mapsto \mathsf{true},\ x = y_1 \mapsto \mathsf{false},\ \ldots,\ x = y_n \mapsto \mathsf{false}\}$$

and, for $i \in \{1, \ldots, n\}$,

$$G_i :\ G\{x \mapsto y_i\}\ .$$

We claim that $\exists x.\ G$ is weakly T-equivalent to

$$G' :\ G_0\ \vee\ G_1\ \vee\ \cdots\ \vee\ G_n\ .$$

For G' asserts that x is either equal to some free variable y_i or not. Because we consider only interpretations with infinite domains, it is always possible for x not to equal any y_i.

It is weak because equivalence is only guaranteed to hold on infinite interpretations.

- By Lemma(Weak Quantifier Elimination for Pure Equality), according to (b), we claim that there exists a quantifier-free pure equality formula H over shared(F1, F2) such that

$$S_1 \land F_1 \Rightarrow * \ H \ and \ S_2 \land H \Rightarrow * \ \neg F_2$$

Next step:

- Recall from the beginning of the proof that $F_1 \wedge K$ is T_1-satisfiable and $F_2 \wedge K$ is T_2-satisfiable, where K = α(V = shared(F_1, F_2),E) is an arrangement.
- Thus, $S_1 \wedge F_1 \wedge K$ and $S_2 \wedge F_2 \wedge K$
- Moreover, as T_1 and T_2 are stably infinite, each of these formulae has an interpretation with an infinite domain.

Now, let's look at K.

- We know K is a conjunction of equalities and disequalities between pairs of variables of shared(F_1, F_2).

- Now, we construct the formula K' by conjoining additional equality literals:
  - for each pair of variables $\mathrm{u}, \mathrm{v} \in shared(F_1, F_2)$, conjoin either $\mathrm{u} = \mathrm{v}$ or $\mathrm{u} \neq \mathrm{v}$, depending on which maintains the satisfiability of K' in a theory with equality.

- Since $\mathrm{S}_1 \wedge F_1 \wedge K$ is satisfiable, then so is $\mathrm{S}_1 \wedge F_1 \wedge K'$, indeed by the same interpretations

We claim that the DNF representation of H must include K′ or a (conjunctive) subformula of K′ as a disjunct.

- Suppose not; then every disjunct of the DNF representation of H contradicts the satisfying interpretations of $S_1 \wedge F_1 \wedge K'$. But we know at least one interpretation satisfies $S_1 \wedge F_1 \wedge K'$.

- So, $K' \Rightarrow H$, and because K and K′ are equivalent in a theory with equality, thus

  $K \Rightarrow H$.

$S_2 \wedge H \Rightarrow * \neg F_2$

Rearranging,
$S_2 \wedge F_2 \Rightarrow * \neg \mathrm{H}$

From K⇒H, we have ¬H ⇒ $\neg K$, so
$S_2 \wedge F_2 \Rightarrow * \neg K$

- But this weak implication contradicts that $\mathrm{S}_2 \wedge F_2 \wedge K$ is satisfied by some infinite interpretation.

Proof finished □

- The Nelson-Oppen method is correct.

Thank you!