Combining satisfiability procedures by equality-sharing

- what is a model of an axiomatically def theory
→ satisfiability

E $=, \neq, f, g, \cdots$

R $=, \neq, +, -, \leq, 0, 1$

Try $f(f(x) - f(y)) \neq f(z)$

$x \leq y$

$y + z \leq x$

$z \geq 0$

- a formula from the combined theory
- we have sat procedure for each
  - E – Ackermann 1924
  - R – Fourier
- only in 1979 was a sat procedure for both created.
- let's separate the formula into $F_R \wedge F_E$ such that

F is sat iff $F_R \wedge F_E$ is sat

– simultaneous satisfiability is not equivalence

$x \leq y$ $\quad g_1 = f(x)$

$y + z \leq x$ $\quad g_2 = f(y)$

$z \geq 0$ $\quad f(g_3) \neq f(z)$

$g_3 = g_1 - g_2$

F_R $\quad F_E$

- here $F \Leftrightarrow F_R \wedge F_E$ clearly
- both F_R and F_E are independently sat. but $F_R \wedge F_E$ is unsat

Idea

- each sat procedure should announce equalities between variables that it discovers.

$F_R \xrightarrow{x=y}$

$g_1 = g_2$

$\xrightarrow{\quad} \times$

$g_3 = z$

- Does not work always

We will do the proof and point out the exceptions.

Counterexample ①

Th_1 $\exists ab\ \forall x\ \ x=a \vee x=b$

Th_2 $\exists abc\ \ a\neq b \wedge b\neq c \wedge a\neq c.$

- empty conjunction is unsat but does not use

Counterexample ②

$int(x)$
$1 \leq x$
$x \leq 2$
$a = 1$
$b = 2$

$f(x) \neq f(a)$
$f(x) \neq f(b)$

- no equalities, but not satisf.

$int(x)$ is an infinite disjunction
- this complicates matters significantly

When is a formula satisfiable in theory T

- pick a universe
- pick an interpretation Ψ of variables and of constants
  - such that Ψ satisfies all axioms of T

- if there is such an interpretation that furthermore satisfies F, we say that F is satisfiable.

We state formally that Nelson-Oppen strategy is sound and complete

Let F_1 in theory A_1 and F_2 in theory A_2 such that

- F_1, A_1 is satisfiable
- F_2, A_2 is satisfiable
- $\forall x,y \in Var \quad F_1, A_1 \vdash x = y$ iff $F_2, A_2 \vdash x = y$
  (all equalities have been broadcast)

then

$F_1 \wedge F_2 \; , A_1 \wedge A_2$ is satisfiable

- Actually, there are other conditions that must hold before the conclusion holds.
- These conditions limit somewhat the applicability of the strategy
- We will uncover these conditions while doing the proof.

Idea

- start with U_1 and the interpretation ψ_1
- extend ψ_1 to ψ such that

$$\psi(t) = \begin{cases} \psi_1(t) & t \in \text{Theory}_1 \\ \alpha(\psi_2(t)) & t \in \text{Theory}_2 \end{cases}$$

and α a bijection from $U_2 \longrightarrow U_1$

When is this possible?

a) **U_1 and U_2 must have the same cardinality**

(we assume that $U_1 = \text{Range}(\psi_1)$ and $U_2 = \text{Range}(\psi_2)$)

Counterexample

Th_1 $\quad \exists ab \; \forall x. \; x=a \vee x=b$ $\quad$ U_1 has at most 2 elements

Th_2 $\quad \exists abc \; a \neq b \wedge b \neq c \wedge a \neq b$ $\quad$ U_2 has at least 3 elements

the empty conjunction is sat in both theories but not in their combination

Nelson-Oppen does not work because U_1 is not isomorphic with U_2

b) variables belong to both theories.

Thus $\psi_1(x) = \alpha(\psi_2(x))$ for all variables x.

This is possible whenever

$$\psi_1(x) = \psi_1(y) \quad \text{iff} \quad \psi_2(x) = \psi_2(y)$$

A sufficient condition is.

$$\psi_1(x) = \psi_1(y) \quad \text{iff} \quad F_1, A_1 \vdash x = y$$

Definition

A theory is non-convex when there exists a formula F such that F entails a disjunction of equalities without entailing any singe equality.

Condition 2. | the theories must be convex |

Why?

Let A be a convex theory.

Separate variables in equivalence classes.

$$F, A \vdash x = y \quad \text{then} \quad x \equiv y$$

Theorem

Assume that F, A is satisfiable. Then there exists a satisfying interpretation ψ such that

$$\psi(x) = \psi(y) \quad \text{iff} \quad F, A \vdash x = y$$

Proof of theorem

if F, A is satisfiable, then $F_s \wedge \bigwedge_{i \neq j} x_i \neq x_j$, A is also satisfiable (where x_i are the representatives of equivalence classes)

For if $\neg F \wedge \bigwedge_{i \neq j} x_i \neq x_j$ is not satisfiable, then

$$F, A \vdash \bigvee_{i \neq j} x_i = x_j$$

But since A is convex $F, A \vdash x_i = x_j$ for some i and j $\neq$

but then $x_i \equiv x_j$ (contradiction)

□ (end of proof)

Thus there is always a satisfiability interpretation such that $\psi(x) = \psi(y) \iff F, A \vdash x = y$

Assume now that ψ_1 and ψ_2 are such interpretations.

Then

$$\psi_1(x) = \psi_1(y) \overset{\text{convexity } A_1}{\iff} F_1, A_1 \vdash x = y \overset{\text{hypotheses (all equalities have been shared)}}{\iff} F_2, A_2 \vdash x = y \overset{\text{convexity of } A_2}{\iff} \psi_2(x) = \psi_2(y)$$

Thus α is well-defined at least of $\psi_1(x)$ for all variables x

The final step is to define

$$\psi(f) = \lambda x_1 \ldots x_n . \alpha\left(\psi_2(f)\left(\alpha^{-1}(x_1), \ldots, \alpha^{-1}(x_n)\right)\right)$$

for all function symbols in $Theory_2$

$$\psi(f) = \psi_1(f) \quad \text{if} \quad f \in Theory_1$$

Condition 3 The two theories do not share function or predicate symbols.

Counterexample $\mathbb{Z}^+$ and $R^{+,\times}$ are decidable but $\mathbb{Z}^{\times,+}$ is undecidable

(the combination of $\mathbb{Z}^+$ and $R^{+,\times}$)

With these conditions we can indeed construct α such that

$$\psi(t) = \alpha(\psi_2(t)) \qquad t \in Theory_2$$

$$\psi(p) \text{ iff } \psi_2(p) \qquad p \in Theory_2 \text{ (a predicate)}$$

↖ we need an argument that

$\psi_2(t_1 = t_2)$ iff $\psi_2(t_1) = \psi_2(t_2)$

follows from convexity.

Thus ψ is a satisfying interpretation for $F_1 \wedge F_2, A_1 \wedge A_2$