Combining Theories

Emina Torlak
emina@cs.washington.edu
Today

Last lecture
• A survey of theory solvers and deciding $T_\leq$ with congruence closure

Today
• Deciding a combination of theories

Reminders
• HW1 is due by 11:00 pm
• HW2 is posted
  • Start early
  • Submit self-contained runnable code
Satisfiability Modulo Theories (SMT)

\[ x = g(y) \]
\[ 2x + y > 5 \]
\[ (b >> 2) = c \]
\[ \vdots \]
\[ a[i] = x \]

Theories

First-Order Logic

SMT solver

Core solver

DPLL(T)

Theory solver

\( \text{(un)satisfiable} \)
Combining theories with Nelson-Oppen

\[ \Sigma_1 \text{-theory } T_1 \text{ with axioms } A_1 \]

\[ \Sigma_2 \text{-theory } T_2 \text{ with axioms } A_2 \]

\[ \vdots \]

\[ \Sigma_n \text{-theory } T_n \text{ with axioms } A_n \]

Theory solver

\[ \Sigma_1 \cup \ldots \cup \Sigma_n \]

Combine solvers

Theory solver

Theory solver

\[ T_1 \cup \ldots \cup T_n \text{ with signatures } \Sigma_1 \cup \ldots \cup \Sigma_n \text{ and axioms } A_1 \cup \ldots \cup A_n \]
Combining theories with Nelson-Oppen

$\Sigma_1$-theory $T_1$ with axioms $A_1$

Theory solver

$\Sigma_2$-theory $T_2$ with axioms $A_2$

Theory solver

We’ll see how to combine two theories. Easy to generalize to $n$.  

Combination solver

Theory $T_1 \cup T_2$ with signature $\Sigma_1 \cup \Sigma_2$ and axioms $A_1 \cup A_2$
Combining theories with Nelson-Oppen

Theory $T_1 \cup T_2$ with signature $\Sigma_1 \cup \Sigma_2$ and axioms $A_1 \cup A_2$

We’ll see how to combine two theories. Easy to generalize to $n$.

The combination problem is undecidable for arbitrary (decidable) theories. It becomes decidable under Nelson-Oppen restrictions.
Nelson-Oppen restrictions

\( T_1 \) and \( T_2 \) can be combined when

- Both are decidable, quantifier-free conjunctive fragments
- Equality (=) is the only symbol in the intersection of their signatures: \( \Sigma_1 \cap \Sigma_2 = \{ = \} \)
- Both are stably infinite
Nelson-Oppen restrictions

$T_1$ and $T_2$ can be combined when

- Both are decidable, quantifier-free conjunctive fragments
- Equality (=) is the only symbol in the intersection of their signatures: $\Sigma_1 \cap \Sigma_2 = \{ = \}$
- Both are stably infinite

A theory $T$ is stably infinite if for every satisfiable $\Sigma_T$-formula $F$, there is a $T$-model that satisfies $F$ and that has a universe of infinite cardinality.
Examples of (non-)stably infinite theories

\( \Sigma_T: \{ a, b, = \} \)

\( A_T: \forall x. x = a \lor x = b \)
Examples of (non-)stably infinite theories

$\Sigma_T: \{ a, b, = \}$
$A_T: \forall x . x = a \lor x = b$
Examples of (non-)stably infinite theories

\[ \Sigma_T \colon \{ a, b, = \} \]
\[ \Lambda_T \colon \forall x \cdot x = a \lor x = b \]

Fixed width bit vectors \((T_{bv})\)
Examples of (non-)stably infinite theories

\[ \Sigma_T: \{ a, b, = \} \]
\[ \forall x . x = a \lor x = b \]

Fixed width bit vectors (\( T_{bv} \))
Examples of (non-)stably infinite theories

$\Sigma_T: \{ \text{a, b, =} \}$

$A_T: \forall x. x = a \lor x = b$

Equality and uninterpreted functions ($T_\equiv$)

Fixed width bit vectors ($T_{bv}$)
Examples of (non-)stably infinite theories

\[ \Sigma_T : \{ a, b, = \} \]
\[ A_T : \forall x . x = a \lor x = b \]

Fixed width bit vectors (T_{bv})

Equality and uninterpreted functions (T_=)

✗

✓
Examples of (non-)stably infinite theories

$$\Sigma_T: \{ a, b, = \}$$

$$A_T: \forall x. x = a \lor x = b$$

Equality and uninterpreted functions ($T_=$) ✓

Fixed width bit vectors ($T_{bv}$) ✗

Linear real arithmetic ($T_R$) ✓

Arrays ($T_A$) ✓

Linear integer arithmetic ($T_{Ri}$) ✓
Overview of Nelson-Oppen

\[(\Sigma_1 \cup \Sigma_2)\text{-formula } F\]

Purification

\[\Sigma_1\text{-formula } F_1\]

Equality Propagation

\[\Sigma_2\text{-formula } F_2\]

\[T_1\text{ solver} \equiv T_2\text{ solver}\]
Overview of purification

Transforms a \((\Sigma_1 \cup \Sigma_2)\)-formula \(F\) into an equisatisfiable formula \(F_1 \land F_2\) with \(F_1\) in \(T_1\) and \(F_2\) in \(T_2\)
Overview of purification

Transforms a \((\Sigma_1 \cup \Sigma_2)\)-formula \(F\) into an equisatisfiable formula \(F_1 \land F_2\) with \(F_1\) in \(T_1\) and \(F_2\) in \(T_2\)

Repeat until fix point:

- If \(f\) is in \(T_i\) and \(t\) is not, and \(u\) is fresh:
  \[F[f(\ldots, t, \ldots)] \iff F[f(\ldots, u, \ldots)] \land u = t\]

- If \(p\) is in \(T_i\) and \(t\) is not, and \(v\) is fresh:
  \[F[p(\ldots, t, \ldots)] \iff F[p(\ldots, v, \ldots)] \land v = t\]
Overview of purification

Transforms a \((\Sigma_1 \cup \Sigma_2)\)-formula \(F\) into an equisatisfiable formula \(F_1 \land F_2\) with \(F_1\) in \(T_1\) and \(F_2\) in \(T_2\)

Repeat until fix point:

- If \(f\) is in \(T_i\) and \(t\) is not, and \(u\) is fresh:
  \(F[f(\ldots, t, \ldots)] \iff F[f(\ldots, u, \ldots)] \land u = t\)

- If \(p\) is in \(T_i\) and \(t\) is not, and \(v\) is fresh:
  \(F[p(\ldots, t, \ldots)] \iff F[p(\ldots, v, \ldots)] \land v = t\)
Overview of purification

Transforms a \((\Sigma_1 \cup \Sigma_2)\)-formula \(F\) into an equisatisfiable formula \(F_1 \land F_2\) with \(F_1\) in \(T_1\) and \(F_2\) in \(T_2\)

Repeat until fix point:

- If \(f\) is in \(T_i\) and \(t\) is not, and \(u\) is fresh:
  \(F[f(\ldots, t, \ldots)] \rightsquigarrow F[f(\ldots, u, \ldots)] \land u = t\)

- If \(p\) is in \(T_i\) and \(t\) is not, and \(v\) is fresh:
  \(F[p(\ldots, t, \ldots)] \rightsquigarrow F[p(\ldots, v, \ldots)] \land v = t\)
Another purification example

Transforms a \((\Sigma_1 \cup \Sigma_2)\)-formula \(F\) into an equisatisfiable formula \(F_1 \land F_2\) with \(F_1\) in \(T_1\) and \(F_2\) in \(T_2\)

Repeat until fix point:

- If \(f\) is in \(T_i\) and \(t\) is not, and \(u\) is fresh:
  \(F[f(\ldots, t, \ldots)] \rightsquigarrow F[f(\ldots, u, \ldots)] \land u = t\)

- If \(p\) is in \(T_i\) and \(t\) is not, and \(v\) is fresh:
  \(F[p(\ldots, t, \ldots)] \rightsquigarrow F[p(\ldots, v, \ldots)] \land v = t\)

\[f(x + g(y)) \leq g(a) + f(b)\]

\[\Sigma_R \quad \Sigma_e\]
Another purification example

Transforms a \((\Sigma_1 \cup \Sigma_2)\)-formula \(F\) into an equisatisfiable formula \(F_1 \land F_2\) with \(F_1\) in \(T_1\) and \(F_2\) in \(T_2\)

Repeat until fix point:

- If \(f\) is in \(T_i\) and \(t\) is not, and \(u\) is fresh:
  \[ F[f(\ldots, t, \ldots)] \leftrightarrow F[f(\ldots, u, \ldots)] \land u = t \]

- If \(p\) is in \(T_i\) and \(t\) is not, and \(v\) is fresh:
  \[ F[p(\ldots, t, \ldots)] \leftrightarrow F[p(\ldots, v, \ldots)] \land v = t \]

\[ f(x + g(y)) \leq g(a) + f(b) \]
Another purification example

Transforms a $(\Sigma_1 \cup \Sigma_2)$-formula $F$ into an equisatisfiable formula $F_1 \land F_2$ with $F_1$ in $T_1$ and $F_2$ in $T_2$

Repeat until fix point:

• If $f$ is in $T_i$ and $t$ is not, and $u$ is fresh:
  $F[f(\ldots, t, \ldots)] \iff F[f(\ldots, u, \ldots)] \land u = t$

• If $p$ is in $T_i$ and $t$ is not, and $v$ is fresh:
  $F[p(\ldots, t, \ldots)] \iff F[p(\ldots, v, \ldots)] \land v = t$

\[f(x + u_1) \leq u_2 + u_3\]

\[u_1 = g(y)\]
\[u_2 = g(a)\]
\[u_3 = f(b)\]
Another purification example

Transforms a \((\Sigma_1 \cup \Sigma_2)\)-formula \(F\) into an equisatisfiable formula \(F_1 \land F_2\) with \(F_1\) in \(T_1\) and \(F_2\) in \(T_2\)

Repeat until fix point:

- If \(f\) is in \(T_i\) and \(t\) is not, and \(u\) is fresh:
  \(F[f(\ldots, t, \ldots)] \implies F[f(\ldots, u, \ldots)] \land u = t\)

- If \(p\) is in \(T_i\) and \(t\) is not, and \(v\) is fresh:
  \(F[p(\ldots, t, \ldots)] \implies F[p(\ldots, v, \ldots)] \land v = t\)

\[f(x + u_1) \leq u_2 + u_3\]

\(u_1 = g(y)\)
\(u_2 = g(a)\)
\(u_3 = f(b)\)
Another purification example

Transforms a \((\Sigma_1 \cup \Sigma_2)\)-formula \(F\) into an equisatisfiable formula \(F_1 \land F_2\) with \(F_1\) in \(T_1\) and \(F_2\) in \(T_2\)

Repeat until fix point:

- If \(f\) is in \(T_i\) and \(t\) is not, and \(u\) is fresh:
  \[ F[f(\ldots, t, \ldots)] \rightsquigarrow F[f(\ldots, u, \ldots)] \land u = t \]

- If \(p\) is in \(T_i\) and \(t\) is not, and \(v\) is fresh:
  \[ F[p(\ldots, t, \ldots)] \rightsquigarrow F[p(\ldots, v, \ldots)] \land v = t \]
Another purification example

Transforms a $(\Sigma_1 \cup \Sigma_2)$-formula $F$ into an equisatisfiable formula $F_1 \land F_2$ with $F_1$ in $T_1$ and $F_2$ in $T_2$

Repeat until fix point:

- If $f$ is in $T_i$ and $t$ is not, and $u$ is fresh:
  \[ F[f(\ldots, t, \ldots)] \iff F[f(\ldots, u, \ldots)] \land u = t \]

- If $p$ is in $T_i$ and $t$ is not, and $v$ is fresh:
  \[ F[p(\ldots, t, \ldots)] \iff F[p(\ldots, v, \ldots)] \land v = t \]

\[ f(u_4) \leq u_2 + u_3 \]

\[ u_4 = x + u_1 \]

\[ u_1 = g(y) \]
\[ u_2 = g(a) \]
\[ u_3 = f(b) \]
Another purification example

Transforms a $(\Sigma_1 \cup \Sigma_2)$-formula $F$ into an equisatisfiable formula $F_1 \land F_2$ with $F_1$ in $T_1$ and $F_2$ in $T_2$

Repeat until fix point:

- If $f$ is in $T_i$ and $t$ is not, and $u$ is fresh:
  $$F[f(\ldots, t, \ldots)] \rightsquigarrow F[f(\ldots, u, \ldots)] \land u = t$$

- If $p$ is in $T_i$ and $t$ is not, and $v$ is fresh:
  $$F[p(\ldots, t, \ldots)] \rightsquigarrow F[p(\ldots, v, \ldots)] \land v = t$$

\[
\begin{align*}
\Sigma_R & \\
& u_4 = x + u_1 \\
& u_5 \leq u_2 + u_3 \\
\Sigma_\Sigma & \\
& u_1 = g(y) \\
& u_2 = g(a) \\
& u_3 = f(b) \\
& u_5 = f(u_4)
\end{align*}
\]
Shared and local constants

A constant is *shared* if it occurs in both $F_1$ and $F_2$, and it is *local* otherwise.

\[ u_4 = x + u_1 \]
\[ u_5 \leq u_2 + u_3 \]

Purification

\[ \Sigma_R \]
\[ u_1 = g(y) \]
\[ u_2 = g(a) \]
\[ u_3 = f(b) \]
\[ u_5 = f(u_4) \]

\[ \Sigma_L \]
Shared and local constants

A constant is *shared* if it occurs in both $F_1$ and $F_2$, and it is *local* otherwise.

Shared: \{u_1, u_2, u_3, u_4, u_5\}
Local: \{x, y, a, b\}

\[
\begin{align*}
\Sigma_R &
\quad u_4 = x + u_1 \\
\quad u_5 \leq u_2 + u_3 \\
\Sigma_\ast &
\quad u_1 = g(y) \\
\quad u_2 = g(a) \\
\quad u_3 = f(b) \\
\quad u_5 = f(u_4)
\end{align*}
\]
Overview of Nelson-Oppen

\[(\Sigma_1 \cup \Sigma_2)\text{-formula } F\]

\[\Sigma_1\text{-formula } F_1\]

\[\Sigma_2\text{-formula } F_2\]

Equality Propagation

\[T_1 \text{ solver} \Leftrightarrow T_2 \text{ solver}\]
Overview of Nelson-Oppen

\[(\Sigma_1 \cup \Sigma_2)\text{-formula } F\]

\[
\begin{align*}
\Sigma_1\text{-formula } F_1 & \quad \text{Equality Propagation} \quad \Sigma_2\text{-formula } F_2 \\
\text{Purification} & \\
\end{align*}
\]

- Convex theories
- Non-convex theories
Convex theories

A theory $T$ is *convex* if for every conjunctive formula $F$, the following holds:

If $F \rightarrow x_1 = y_1 \lor \ldots \lor x_n = y_n$ for a finite $n > 1$, then $F \rightarrow x_i = y_i$ for some $i \in \{1, \ldots, n\}$. 
Convex theories

A theory $T$ is convex if for every conjunctive formula $F$, the following holds:

If $F \Rightarrow x_1 = y_1 \lor \ldots \lor x_n = y_n$ for a finite $n > 1$,
then $F \Rightarrow x_i = y_i$ for some $i \in \{1, \ldots, n\}$.

If $F$ implies a disjunction of equalities, then it also implies at least one of the equalities.
Examples of (non-)convex theories

Linear arithmetic over integers ($T_Z$)
Examples of (non-)convex theories

Linear arithmetic over integers ($T_\mathbb{Z}$)

$1 \leq x \land x \leq 2 \Rightarrow x = 1 \lor x = 2$ but not $1 \leq x \land x \leq 2 \Rightarrow x = 1$
not $1 \leq x \land x \leq 2 \Rightarrow x = 2$
Examples of (non-)convex theories

- Linear arithmetic over integers ($T\mathbb{Z}$)
  - $1 \leq x \land x \leq 2 \Rightarrow x = 1 \lor x = 2$ but
  - not $1 \leq x \land x \leq 2 \Rightarrow x = 1$
  - not $1 \leq x \land x \leq 2 \Rightarrow x = 2$
  - **✗**

- Equality and uninterpreted functions ($T\equal$)
  - **✓**

- Linear real arithmetic ($T\mathbb{R}$)
  - **✓**
Nelson-Oppen for convex theories

\[\text{NELSON-OPPEN-CONVEX}(F)\]
Nelson-Oppen for convex theories

\textsc{Nelson-Oppen-Convex}(F)

1. Purify F into $F_1 \land F_2$
Nelson-Oppen for convex theories

**NELSON-OPPEN-CONVEX**(F)

1. Purify F into $F_1 \land F_2$

2. Run $T_1$-solver on $F_1$ and $T_2$-solver on $F_2$ and return UNSAT if either is unsatisfiable
Nelson-Oppen for convex theories

Nelson-Oppen-Convex(F)

1. Purify F into F₁ ∧ F₂
2. Run T₁-solver on F₁ and T₂-solver on F₂ and return UNSAT if either is unsatisfiable

Is F satisfiable if both F₁ and F₂ are satisfiable?
Nelson-Oppen for convex theories

\textbf{NELSON-OPPEN-CONVEX}(F)

1. Purify F into \( F_1 \land F_2 \)
2. Run \( T_1 \)-solver on \( F_1 \) and \( T_2 \)-solver on \( F_2 \) and return UNSAT if either is unsatisfiable

Is F satisfiable if both \( F_1 \) and \( F_2 \) are satisfiable? \textbf{No:}
\[ x = 1 \land 2 = x + y \land f(x) \neq f(y) \]
Nelson-Oppen for convex theories

\begin{align*}
\text{NELSON-OPPEN-CONVEX}(F) \\
1. \text{Purify } F \text{ into } F_1 \land F_2 \\
2. \text{Run } T_1\text{-solver on } F_1 \text{ and } T_2\text{-solver on } F_2 \text{ and return } \text{UNSAT} \text{ if either is unsatisfiable} \\
3. \text{If there are shared constants } x \text{ and } y \text{ such that } F_i \Rightarrow x = y \text{ but } F_j \text{ does not} \\
   \quad 1. F_j \leftarrow F_j \land x = y \\
   \quad 2. \text{Go to step 2.}
\end{align*}
Nelson-Oppen for convex theories

\textbf{NELSON-OPPEN-CONVEX}(F)

1. Purify \( F \) into \( F_1 \land F_2 \)

2. Run \( T_1 \)-solver on \( F_1 \) and \( T_2 \)-solver on \( F_2 \) and return \text{UNSAT} if either is unsatisfiable

3. If there are shared constants \( x \) and \( y \) such that \( F_i \Rightarrow x = y \) but \( F_j \) does not

   1. \( F_j \leftarrow F_j \land x = y \)
   2. Go to step 2.

4. Return \text{SAT}
Nelson-Oppen for convex theories: example

\textbf{NELSON-OPPEN-CONVEX}(F)

1. Purify F into $F_1 \land F_2$
2. Run $T_1$-solver on $F_1$ and $T_2$-solver on $F_2$ and return UNSAT if either is unsatisfiable
3. If there are shared constants $x$ and $y$ such that $F_i \Rightarrow x = y$ but $F_j$ does not
   1. $F_j \leftarrow F_j \land x = y$
   2. Go to step 2.
4. Return SAT

\[ f(f(x) - f(y)) \neq f(z) \land x \leq y \land y + z \leq x \land 0 \leq z \]
**Nelson-Oppen for convex theories: example**

**NELSON-OPPEN-CONVEX(F)**

1. Purify F into $F_1 \land F_2$
2. Run $T_1$-solver on $F_1$ and $T_2$-solver on $F_2$ and return UNSAT if either is unsatisfiable
3. If there are shared constants $x$ and $y$ such that $F_i \Rightarrow x = y$ but $F_j$ does not
   1. $F_j \leftarrow F_j \land x = y$
   2. Go to step 2.
4. Return SAT

\[
\begin{align*}
\text{if}(f(x) - f(y)) &\neq f(z) \land x \leq y \\
&\land y + z \leq x \land 0 \leq z
\end{align*}
\]

\[
\begin{array}{ll}
\text{x} \leq \text{y} \land & \text{f(w)} \neq \text{f(z)} \land \\
\text{y} + \text{z} \leq \text{x} \land & \text{u} = \text{f(x)} \land \\
\text{0} \leq \text{z} \land & \text{v} = \text{f(y)} \\
\text{w} = \text{u} - \text{v}
\end{array}
\]

\[
\Sigma_R \quad \Sigma =
\]
Nelson-Oppen for convex theories: example

**NELSON-OPPEN-CONVEX(F)**

1. Purify F into $F_1 \land F_2$
2. Run $T_1$-solver on $F_1$ and $T_2$-solver on $F_2$ and return UNSAT if either is unsatisfiable
3. If there are shared constants $x$ and $y$ such that $F_i \models x = y$ but $F_j$ does not
   1. $F_j \leftarrow F_j \land x = y$
   2. Go to step 2.
4. Return SAT

\[
\begin{align*}
\text{f(f(x) - f(y))} & \neq f(z) \land x \leq y \\
& \land y + z \leq x \land 0 \leq z
\end{align*}
\]

| $x \leq y \land$ | $f(w) \neq f(z) \land$
| $y + z \leq x \land$ | $u = f(x) \land$
| $0 \leq z \land$ | $v = f(y)$
| $w = u - v$ | 
| $x = y \land$ | $x = y \land$

$\Sigma_R$ $\Sigma =$
Nelson-Oppen for convex theories: example

**\textsc{Nelson-Oppen-Convex}(F)**

1. Purify F into $F_1 \land F_2$
2. Run $T_1$-solver on $F_1$ and $T_2$-solver on $F_2$ and return UNSAT if either is unsatisfiable
3. If there are shared constants $x$ and $y$ such that $F_i \Rightarrow x = y$ but $F_j$ does not
   1. $F_j \leftarrow F_j \land x = y$
   2. Go to step 2.
4. Return SAT

\[
\begin{align*}
\text{f}(\text{f}(x) - \text{f}(y)) \neq \text{f}(z) \land x \leq y \\
\land y + z \leq x \land 0 \leq z
\end{align*}
\]

\[
\begin{align*}
x \leq y \land & \quad \text{f}(w) \neq \text{f}(z) \land \\
\text{y} + z \leq x \land & \quad u = \text{f}(x) \land \\
0 \leq z \land & \quad v = \text{f}(y) \\
w = u - v
\end{align*}
\]

\[
\begin{align*}
x = y \land & \quad x = y \land \\
u = v \land & \quad u = v \land
\end{align*}
\]

\[
\Sigma_R \\
\Sigma =
\]
Nelson-Oppen for convex theories: example

**Nelson-Oppen-Convex(F)**

1. Purify F into $F_1 \land F_2$
2. Run $T_1$-solver on $F_1$ and $T_2$-solver on $F_2$ and return UNSAT if either is unsatisfiable
3. If there are shared constants x and y such that $F_i \Rightarrow x = y$ but $F_j$ does not
   1. $F_j \leftarrow F_j \land x = y$
   2. Go to step 2.
4. Return SAT

| $f(f(x) - f(y)) \neq f(z) \land x \leq y$
| $\land y + z \leq x \land 0 \leq z$
| $x \leq y \land$
| $f(w) \neq f(z) \land$
| $y + z \leq x \land$
| $u = f(x) \land$
| $0 \leq z \land$
| $v = f(y)$
| $w = u - v$ |
| $x = y \land$
| $x = y \land$
| $u = v \land$
| $u = v \land$
| $w = z \land$
| $w = z \land$
| $\Sigma_R$
| $\Sigma_=$
Nelson-Oppen for convex theories: example

NELSON-OPPEN-CONVEX(F)

1. Purify F into F₁ ∨ F₂
2. Run T₁-solver on F₁ and T₂-solver on F₂ and return UNSAT if either is unsatisfiable
3. If there are shared constants x and y such that Fᵢ ⇒ x = y but Fⱼ does not
   1. Fⱼ ← Fⱼ ∧ x = y
   2. Go to step 2.
4. Return SAT

\[
\begin{align*}
f(f(x) - f(y)) \neq f(z) & \land x \leq y \\
& \land y + z \leq x \land 0 \leq z
\end{align*}
\]

\[
\begin{array}{ll}
x \leq y \land & f(w) \neq f(z) \land \\
y + z \leq x \land & u = f(x) \land \\
0 \leq z \land & v = f(y) \\
w = u - v
\end{array}
\]

\[
\begin{align*}
x = y \land & x = y \land \\
u = v \land & u = v \land \\
w = z \land & w = z \land \\
UNSAT
\end{align*}
\]

\[\Sigma_R \Sigma =\]
This doesn’t work for non-convex theories ...

**NELSON-OPPEN-CONVEX(F)**
1. Purify F into $F_1 \land F_2$
2. Run $T_1$-solver on $F_1$ and $T_2$-solver on $F_2$ and return UNSAT if either is unsatisfiable
3. If there are shared constants $x$ and $y$ such that $F_i \Rightarrow x = y$ but $F_j$ does not
   1. $F_j \leftarrow F_j \land x = y$
   2. Go to step 2.
4. Return SAT

\[ 1 \leq x \land x \leq 2 \land f(x) \neq f(1) \land f(x) \neq f(2) \]
This doesn’t work for non-convex theories ...

**Nelson-Oppen-Convex** *(F)*

1. Purify F into $F_1 \land F_2$
2. Run $T_1$-solver on $F_1$ and $T_2$-solver on $F_2$ and return UNSAT if either is unsatisfiable
3. If there are shared constants $x$ and $y$ such that $F_i \Rightarrow x = y$ but $F_j$ does not
   1. $F_j \leftarrow F_j \land x = y$
   2. Go to step 2.
4. Return SAT

<table>
<thead>
<tr>
<th>$1 \leq x \land x \leq 2 \land f(x) \neq f(1) \land f(x) \neq f(2)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$1 \leq x$ \land $f(x) \neq f(z_1) \land z_1 = 1 \land z_2 = 2$</td>
</tr>
</tbody>
</table>

$\Sigma_Z$ $\Sigma_=$
This doesn’t work for non-convex theories ...

\text{NELSON-OPPEN-CONVEX}(F)

1. Purify \( F \) into \( F_1 \land F_2 \)

2. Run \( T_1 \)-solver on \( F_1 \) and \( T_2 \)-solver on \( F_2 \) and return UNSAT if either is unsatisfiable

3. If there are shared constants \( x \) and \( y \) such that \( F_i \Rightarrow x = y \) but \( F_j \) does not
   1. \( F_j \leftarrow F_j \land x = y \)
   2. Go to step 2.

4. Return SAT

\[
\begin{array}{c|c|c}

\quad & 1 \leq x \land x \leq 2 \land & f(x) \neq f(1) \land f(x) \neq f(2) \\
\hline
1 \leq x \land & f(x) \neq f(z_1) \land & f(x) \neq f(z_2) \\
x \leq 2 \land & z_1 = 1 \land & f(x) \neq f(z_2) \\
z_2 = 2 & & \\
\end{array}
\]

\[\Sigma Z \quad \Sigma Z\]
This doesn’t work for non-convex theories ...

\textbf{NELSON-OPPEN-CONVEX}(F)

1. Purify F into $F_1 \land F_2$

2. Run $T_1$-solver on $F_1$ and $T_2$-solver on $F_2$ and return UNSAT if either is unsatisfiable

3. If there are shared constants $x$ and $y$ such that $F_i \Rightarrow x = y$ but $F_j$ does not
   1. $F_j \leftarrow F_j \land x = y$
   2. Go to step 2.

4. Return SAT

If $T$ is non-convex, it may imply a disjunction of equalities without implying any single equality.

We have to propagate disjunctions as well as individual equalities. Which disjunctions? How do we propagate disjunctions to theory solvers which reason only about conjunctions?
Nelson-Oppen for non-convex theories

NELSON-OPPEN(F)
1. Purify F into F₁ ∧ F₂
2. Run T₁-solver on F₁ and T₂-solver on F₂ and return UNSAT if either is unsatisfiable
3. If there are shared constants x and y such that Fᵢ ⇒ x = y but Fⱼ does not
   1. Fⱼ ← Fⱼ ∧ x = y
   2. Go to step 2.
4. If Fᵢ ⇒ x₁ = y₁ ∨... ∨ xₙ = yₙ but Fⱼ does not, then if NELSON-OPPEN(Fᵢ ∧ Fⱼ ∧ xₖ = yₖ) outputs SAT for any k, return SAT. Otherwise, return UNSAT.
5. Return SAT
Nelson-Oppen for non-convex theories

\text{NELSON-OPPEN}(F)
1. Purify F into $F_1 \land F_2$
2. Run $T_1$-solver on $F_1$ and $T_2$-solver on $F_2$ and return UNSAT if either is unsatisfiable
3. If there are shared constants $x$ and $y$ such that $F_i \Rightarrow x = y$ but $F_j$ does not
   1. $F_j \leftarrow F_j \land x = y$
   2. Go to step 2.
4. If $F_i \Rightarrow x_1 = y_1 \lor \ldots \lor x_n = y_n$ but $F_j$ does not, then
   if \text{NELSON-OPPEN}(F_i \land F_j \land x_k = y_k) outputs SAT for any $k$, return SAT. Otherwise, return UNSAT.
5. Return SAT
Nelson-Oppen for non-convex theories: example

\[ 1 \leq x \land x \leq 2 \land f(x) \neq f(1) \land f(x) \neq f(2) \]
Nelson-Oppen for non-convex theories: example

\[
\begin{align*}
1 \leq x & \land x \leq 2 \land \\
f(x) & \neq f(1) \land f(x) \neq f(2)
\end{align*}
\]

<table>
<thead>
<tr>
<th>(1 \leq x \land x \leq 2)</th>
<th>(f(x) \neq f(1) \land f(x) \neq f(2))</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1 \leq x \land)</td>
<td>(f(x) \neq f(z_1) \land)</td>
</tr>
<tr>
<td>(x \leq 2 \land)</td>
<td>(f(x) \neq f(z_2))</td>
</tr>
<tr>
<td>(z_1 = 1 \land)</td>
<td>()</td>
</tr>
<tr>
<td>(z_2 = 2)</td>
<td>()</td>
</tr>
</tbody>
</table>

\[
\Sigma_Z \quad \Sigma =
\]
### Nelson-Oppen for non-convex theories: example

\[\begin{align*}
1 \leq x & \land x \leq 2 \land \\
\text{f(x) \neq f(1)} & \land \text{f(x) \neq f(2)} \\
\hline
1 \leq x & \land f(x) \neq f(z_1) \land \\
x \leq 2 & \land f(x) \neq f(z_2) \\
z_1 = 1 & \land \\
z_2 = 2 & \\
(x = z_1 \lor x = z_2) & \\
\Sigma_Z & = \\
\Sigma & =
\end{align*}\]
Nelson-Oppen for non-convex theories: example

\[
\begin{array}{l}
1 \leq x \land x \leq 2 \land \\
f(x) \neq f(1) \land f(x) \neq f(2)
\end{array}
\]

| \(1 \leq x \land \) | \(f(x) \neq f(z_1) \land \) |
| \(x \leq 2 \land \) | \(f(x) \neq f(z_2) \land \) |
| \(z_1 = 1 \land \)  | \(x = z_1 \land \) |
| \(z_2 = 2 \)    |  "UNSAT" |

\[
\Sigma_Z = (x=z_1 \lor x=z_2) \land \Sigma =
\]
### Nelson-Oppen for non-convex theories: example

<table>
<thead>
<tr>
<th>Condition</th>
<th>Left</th>
<th>Right</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1 \leq x ) (\land) (x \leq 2) (\land) (f(x) \neq f(1)) (\land) (f(x) \neq f(2))</td>
<td>(1 \leq x ) (\land) (f(x) \neq f(z_1)) (\land) (f(x) \neq f(z_2))</td>
<td>(x = z_1) (\land) (x = z_2)</td>
</tr>
<tr>
<td>(x = z_1) (\land) (x = z_2) (\lor) (x = z_1) (\land) (x = z_2)</td>
<td>(\Sigma_Z) (\Sigma =)</td>
<td></td>
</tr>
</tbody>
</table>

\[1 \leq x \land x \leq 2 \land f(x) \neq f(1) \land f(x) \neq f(2)\]

\[f(x) \neq f(z_1) \land f(x) \neq f(z_2)\]

\[x = z_1 \land x = z_2\]

\[\Sigma =\] UNSAT

---

\[1 \leq x \land x \leq 2 \land z_1 = 1 \land z_2 = 2\]

\[f(x) \neq f(z_1) \land f(x) \neq f(z_2)\]

\[x = z_1\]

\[\Sigma =\] UNSAT

---

\[1 \leq x \land x \leq 2 \land z_1 = 1 \land z_2 = 2\]

\[f(x) \neq f(z_1) \land f(x) \neq f(z_2)\]

\[x = z_2\]

\[\Sigma =\] UNSAT

---
Soundness and completeness of Nelson-Oppen

If the theories $T_1$ and $T_2$ satisfy Nelson-Open restrictions, then the combination procedure returns UNSAT for a formula $F$ in $T_1 \cup T_2$ iff $F$ is unsatisfiable modulo $T_1 \cup T_2$. 
Complexity of Nelson-Oppen

If decision procedures for convex theories $T_1$ and $T_2$ have polynomial time complexity, so does their Nelson-Oppen combination.

If decision procedures for non-convex theories $T_1$ and $T_2$ have NP time complexity, so does their Nelson-Oppen combination.
Summary

Today

• Sound and complete procedure for a combination of restricted theories

• Stably infinite, conjunctive, quantifier-free with signatures that are disjoint except for =

Next lecture

• Deciding satisfiability of arbitrary boolean combinations of quantifier-free first-order formulas