up to now:
Given a set of equations $E$, two terms $s, t$ check whether $E \models s = t$ holds.

This means: is $s = t$ true in all models of $E$ (i.e., does $A \models E$ imply $A \models s = t$ for all algebras $A$)?

But: in prog. verification, we are not interested in all models, but only in certain specific models of $E$.

Ex. G3/1 plus-equations (slide)

We want to verify the following statement about our plus-equations $E$:

$$\text{plus}(X, \text{succ}(Y)) \equiv \text{succ}(\text{plus}(X, Y))$$

$S$ is a convergent TRS that is equivalent to $E$:

$$S \models t \iff S \downarrow_R = t \downarrow_R$$

Here: $S$ and $t$ are already in normal form

$\forall \ S \models_E t$.

Problem: "$S \models_E t$" requires that $S \models t$ is true in all models. But in prog. verif., we are only interested
in a model like \( A = (\mathbb{N}, \alpha) \) where

\[
\begin{align*}
\alpha_0 &= 0 \\
\alpha_{\text{succ}}(n) &= n+1 \\
\alpha_{\text{plus}}(n, m) &= n+m .
\end{align*}
\]

Here, we have \( A \models E \) and \( A \models s \leq t \). But \( E \) also has models \( B \) where \( B \models E \), \( B \not\models s \leq t \). Such models typically contain elements in their domain that do not correspond to any ground term.

E.g.: \( B = (\mathbb{N} \cup \{ \Box, \Delta \}, \alpha') \) with

\[
\begin{align*}
\alpha'_0 &= 0 \\
\alpha'_{\text{succ}}(n) &= \begin{cases} 
  n+1 , & \text{if } n \in \mathbb{N} \\
  \Delta , & \text{if } n \in \{ \Box, \Delta \} 
\end{cases} \\
\alpha'_{\text{plus}}(n, m) &= \begin{cases} 
  n+m , & \text{if both } n, m \in \mathbb{N} \\
  n , & \text{if } n \in \{ \Box, \Delta \} \\
  m , & \text{if } n=0, m \in \{ \Box, \Delta \} \\
  \Delta , & \text{if } n>0, m \in \{ \Box, \Delta \}
\end{cases}
\end{align*}
\]

We have \( B \models E \):

\( B \models \text{plus}(\Box, \delta) \equiv \gamma \), since for any var. assignment \( B \) we have

\[
\alpha_{\text{plus}}(\Box_0, B(\gamma)) = B(\gamma) \checkmark
\]

\( B \models \text{plus}(\text{succ}(x), \gamma) \equiv \text{succ}(\text{plus}(x, \gamma)) \), ...

But \( B \not\models \text{plus}(x, \text{succ}(\gamma)) \equiv \text{succ}(\text{plus}(x, \gamma)) \)

To see this, let \( B(x) = \Box \), \( B(\gamma) = \Box \).
\[
\begin{align*}
\alpha_{\text{plus}}(\beta(x), \alpha_{\text{succ}}(\beta(y))) &= \square \\
\alpha_{\text{succ}}(\alpha_{\text{plus}}(\beta(x), \beta(y))) &= \triangle
\end{align*}
\]

So instead of validity in all models, we should check if \( S \vDash T \) holds if one instantiates their variables with ground terms like \( 0, \text{succ}(0), \text{succ}(\text{succ}(0)) \), ...

In other words, we want to know whether a statement about a program holds for all possible data objects.

**Solution:** Define a new notion of truth/validity which only considers instantiations of variables by ground terms.

Variable now stands for "all natural numbers, lists, ..." not for "all elements of the domain of an algebra."

**Def 632 (Inductive Validity)**

Let \( E \) be a set of equations over \( \Sigma \) and \( \mathcal{V} \), let \( s, t \in \mathcal{V}(\Sigma, \mathcal{V}) \).

The equation \( S \vDash T \) is **inductively valid** for \( E \) (denoted \( E \vdash_{I} S \vDash T \)) iff

\[ E \vdash_{I} \forall \sigma \, s \sigma = t \sigma \]
\[ \sigma(x) \in \Sigma \] for all \( x \in \mathcal{V}(s) \cup \mathcal{V}(t) \).

Ex. 6.33

If \( \Sigma \) are the plus equations, then

\[ \exists \ \mathcal{S} \upharpoonright plus(x, \text{succ}(y)) = \text{succ}(\mathcal{S}(x, y)) \quad \text{but} \]

\[ \exists \ \mathcal{S} \upharpoonright plus(x, y) = plus(x, y) \quad \text{and} \]

\[ \exists \ \mathcal{S} \upharpoonright plus(x, y) = plus(x, y) \quad \text{with} \]

\[ \mathcal{S} \upharpoonright plus(x, y) = plus(x, y) \quad \text{and} \]

\[ \mathcal{S} \upharpoonright plus(x, y) = plus(x, y) \quad \text{and} \]

This can be shown by induction.

We have to show that for all ground terms \( t_1, t_2 \), we have:

\[ \exists \mathcal{S} \upharpoonright plus(t_1, \text{succ}(t_2)) = \text{succ}(\mathcal{S}(t_1, t_2)) \]

Let \( \mathcal{S} \) again be the convergent TRS that is equivalent to \( \Sigma \).

We have to show

\[ \text{plus}(t_1, \text{succ}(t_2)) \Downarrow \text{succ}(\text{plus}(t_1, t_2)) \]

Since \( \text{plus} \) is "completely defined" in \( \mathcal{S} \), we can first rewrite \( t_1, t_2 \)

until they don't contain \( \text{plus} \) anymore.

Thus, it suffices to show

\[ \text{plus}(\text{succ}^n(\theta), \text{succ}^{m+n}(\theta)) \Downarrow \text{succ}(\text{plus}(\text{succ}^n(\theta), \text{succ}^{m+n}(\theta))) \]

This is easy to prove by induction on \( n \).

Goal: Prove \( \exists \mathcal{S} \upharpoonright s \equiv t \) automatically.

One could try to perform an induction proof on all possible ground terms.

Problems for automation: find suitable suitable induction variables.
induction relations, ...

Alternative approach: do not perform induction explicitly, but re-use (a slight variant of) the completion algorithm. Here, the induction is only performed implicitly.

Surprising observation: $E \vdash S \sqsubseteq T$ iff
adding $S \sqsubseteq T$ to $E$ does not result in an "inconsistent" set of equations.

The set is considered inconsistent if one can now prove equations $u \equiv v$ between ground terms that did not hold before.

Theorem 634 (Proof by Consistency)

$E \vdash S \sqsubseteq T$ iff for all ground terms $u, v$:

$E \not\vdash u \equiv v$ implies $E \cup \{ S \sqsubseteq T \} \not\vdash u \equiv v$.

Proof: $\Rightarrow$: Let $E \vdash S \sqsubseteq T$, let $E \cup \{ S \sqsubseteq T \} \vdash u \equiv v$.
We have to show that $E \not\vdash u \equiv v$.

By Birkhoff's Theorem (Thm 3.1, Mu) we have:

$u = u_0 \leftrightarrow u_1 \leftrightarrow \ldots \leftrightarrow u_n = v$

Let $\sigma$ be a substitution that instantiates all variables of $u_0, \ldots, u_n$ by arbitrary ground terms. Then stability of $\leftrightarrow$ implies:

$E \cup \{ S \sqsubseteq T \} \vdash \sigma (u_0) \equiv \sigma (u_n)$
Since all $u, \tau$ are ground terms, this derivation could also be done with $
rightarrow \text{ Ev}_s \{ s = \tau \mid \text{g. subst.} \}$.

By Birkhoff’s Thm., this means

$$\text{Ev}_s \{ s = \tau \mid \text{g. subst.} \} \models u \equiv v,$$

i.e. every model of $\text{Ev}_s \{ s = \tau \mid \text{g. subst.} \}$ is also a model of $u \equiv v$.

Since $\xi \models \equiv$, every model of $\xi$ is also a model of $\{ s = \tau \mid \text{g. subst.} \}$.

Then $\xi \models u \equiv v$.

"⇒": Prerequisite: $\text{Ev}_s \{ s = t \} \models u \equiv v$ implies $\xi \models u \equiv v$.

Clearly: $\text{Ev}_s \{ s = t \} \models s = \tau$ for all ground subst. $\sigma$

To use this theorem for automated proofs, we would have to inspect all possible ground terms $u, v$ where $\xi \models u \equiv v$ and check whether $\text{Ev}_s \{ s = t \} \not\models u \equiv v$. Problematic, since there are infinitely many such ground
terms $u,v$.

The next observation shows:

- We use a convergent TNS $R$ that is equivalent to $E$.
- Instead of all ground terms $u,v$ with $E \models u \equiv v$, we only have to inspect all ground normal forms $q_1,q_2$ of $R$ where $q_1 \neq q_2$.

Ground normal forms:

$$NF(R) = \{ q \downarrow_R \mid q \in J(\Sigma) \}.$$ 

For the plus-TNS $R$:

$$NF(R) = \{ \emptyset, \text{succ}(\emptyset), \text{succ}^2(\emptyset), \ldots \} \quad (\subseteq \mathbb{N})$$

So to prove $E \models I \vdash \text{plus}(x,\text{succ}(y)) \equiv \text{succ} (\text{plus}(x,y))$, we can now check whether there are $q_1,q_2 \in NF(R)$ with $q_1 \neq q_2$ such that $E \models \{ \text{plus}(x,\text{succ}(y)) \equiv \text{succ} (\text{plus}(x,y)) \} \vdash q_1 = q_2$.

Theorem 6.35 (Proof by Consistency with Convergent TNSs)

Let $R$ be a convergent TNS that is equivalent to $E$.

$E \models I \vdash s \equiv t$ iff for all $q_1,q_2 \in NF(R)$

$$q_1 \neq q_2 \text{ implies } E \{ s \equiv t \} \not\models q_1 \equiv q_2.$$

Proof: $\Rightarrow$: Let $E \models I \vdash s \equiv t$, let $q_1,q_2 \in NF(R)$ with $E \{ s \equiv t \} \models q_1 \equiv q_2$ where $q_1 \neq q_2$.

By Thm 6.3.4: $E \models q_1 \equiv q_2$.
Since $S$ is convergent and equivalent to $E$: $q_1 \downarrow_S q_2$

As $q_1, q_2$ are normal forms, this implies $q_1 = q_2$. 

$\therefore$: We assume $E \not\vdash S \equiv t$

By Thm 6.34, there exist ground terms $m, n$ such that $E \not\vdash m \equiv n$ and $E \cup \{S \equiv t\} \not\vdash m \equiv n$.

Let $q_1 = m \downarrow_S$, $q_2 = n \downarrow_S$. We must have $q_1 \neq q_2$, because otherwise the equivalence of $S$ and $E$ would imply $E \vdash m \equiv n$.

Moreover:

$E \cup \{S \equiv t\} \not\vdash q_1 \equiv m \equiv n \equiv q_2 \not\vdash$ to the pre-

... requisit...