Term Equational Systems and Logics

Chung-kil Hur
Joint work with Marcelo Fiore

Computer Laboratory
University of Cambridge

11th Aug 2008
@ KAIST

→ Equational Reasoning

Category Theory

Term Equational Systems & Logics

Automated Theorem Proving

- Systems
  - ISABELLE (Univ. of Cambridge & Technische Univ. München)
  - HOL (Univ. of Cambridge)
  - COQ (INRIA)
  - AGDA (Chalmers Univ.)
  - TWELF (C.M.U.)
  - ⋮
- Applications
  - Correctness of security protocols
  - Soundness of programming languages
  - Formal proof of mathematical theorems
  - Verification of hardware design
  - ⋮

First-order Equational Reasoning

- Example: Natural number arithmetic

Sig: $0:0 \quad S:1 \quad +:2$

Eqn: $+(0,n) = n$

$+(s(n),m) = s(+(n,m))$

Q: $+(s(0),0) = +(0,s(0))$

① by logic

$$\dfrac{\dfrac{}{+(s(0),0) = s(+(0,0))} \quad \dfrac{\dfrac{}{+(0,0) = 0}}{s(+(0,0)) = s(0)}}{+(s(0),0) = s(0)} \quad \dfrac{\dfrac{}{+(0,s(0)) = s(0)}}{s(0) = +(0,s(0))}$$

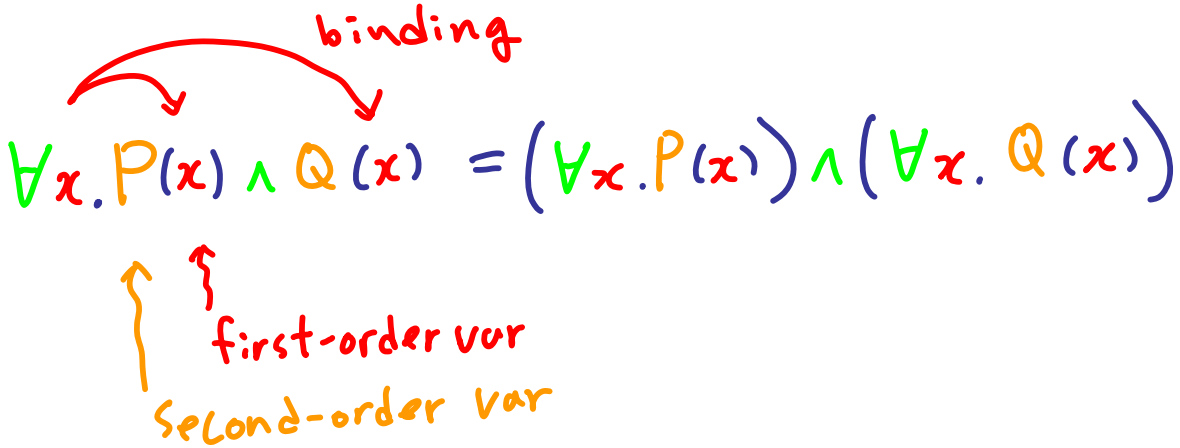
$$+(s(0),0) = +(0,s(0))$$

② by rewriting

$+(s(0),0) \rightarrow s(+(0,0)) \rightarrow s(0) \qquad +(0,s(0)) \rightarrow s(0)$

Higher-order Equational Reasoning

- Consider the equation



We need

① first & second-order variables

② variable binding

- Higher-order Equational Reasoning
  - Combinatory Reduction System (Klop 1980)
  - Higher-order Eq. Log./R.W. Sys. (Nipkow 1991)
  - Binding Term Eq. Log./R.W. Sys. (Hamana 2003)
  - Nominal Eq. Log. (Gabbay & Mathijssen '07, Clouston & Pitts '07)

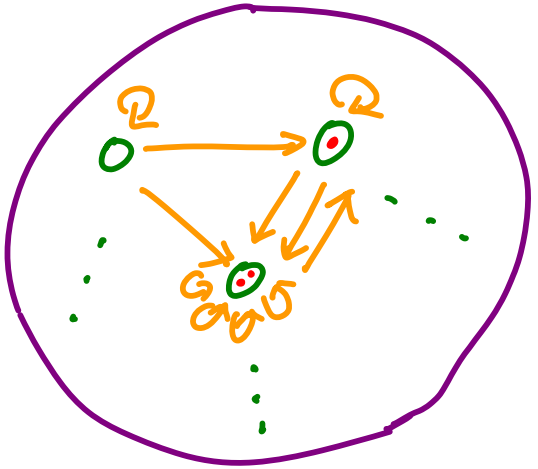
Equational Reasoning

→ Category Theory

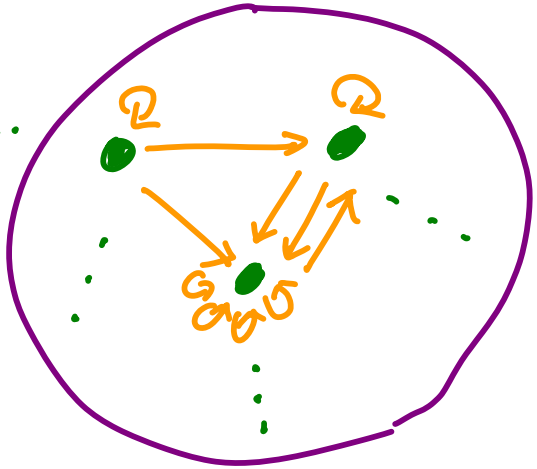
Term Equational Systems & Logics

Motivation for category Theory

- Mathematical structures
  - sets & functions
  - groups & homomorphisms
  - topological spaces & continuous maps

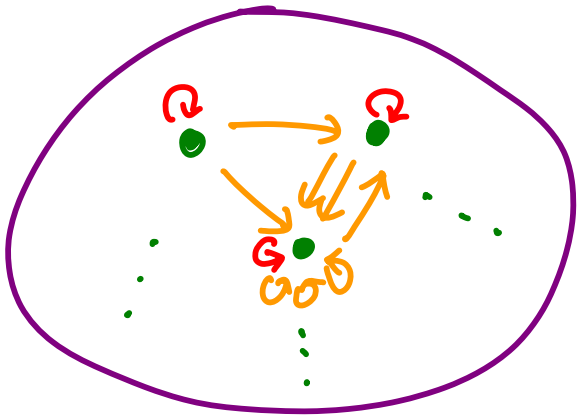


- Common notions
  - empty sets, groups, topological spaces ...
  - product of sets, groups, topological spaces ...
  - injective functions, homomorphisms, continuous maps ...



Definition of Category

A category $\mathcal{C}$ is given by



① $|\mathcal{C}|$: a collection of objects ⇝ sets

② $\forall A,B \in |\mathcal{C}|$
$\mathcal{C}(A,B)$: a collection of morphisms from A to B ⇝ functions from A to B

③ $\forall A \in |\mathcal{C}|$
$id_A \in \mathcal{C}(A,A)$ ⇝ identity function

④ $\forall A,B,C \in |\mathcal{C}|$ ⇝ function composition
$\cdot : \mathcal{C}(B,C) \times \mathcal{C}(A,B) \longrightarrow \mathcal{C}(A,C)$

Satisfying

$\forall f,g,h \quad id \cdot f = f, \; f \cdot id = f, \; (f \cdot g) \cdot h = f \cdot (g \cdot h)$

Examples of categories

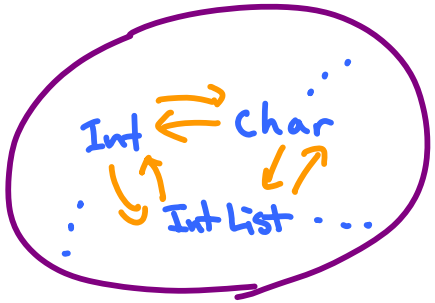
Set : sets & functions

Grp : groups & homomorphisms

Top : topological spaces & continuous functions

Cpo : chain-complete partial orders & continuous functions

⋮



types & programs

Limits and Colimits

- Initial object $\rightsquigarrow$ Empty set

  $0 \in |\mathcal{C}|$ is initial iff $\forall x \in |\mathcal{C}| \;\; \exists! f : 0 \to x$

- Terminal object $\rightsquigarrow$ singleton set

  $1 \in |\mathcal{C}|$ is terminal iff $\forall x \in |\mathcal{C}| \;\; \exists! f : x \to 1$

- Product $\rightsquigarrow$ product set

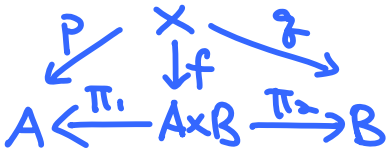
  for $A, B \in |\mathcal{C}|$

  $A \times B \in |\mathcal{C}|$ with $\pi_1 : A \times B \to A$, $\pi_2 : A \times B \to B$ is a product of A B

  iff

  $\forall \; X \in |\mathcal{C}|$ with $p : X \to A$, $q : X \to B$

  $\exists! \; f : X \to A \times B$ s.t.



commutes.

- Coproducts, pull backs, push outs, equalizers, coequalizers

  $\Big\downarrow$

  disjoint unions

Other Categorical Notions

- monomorphism $\rightsquigarrow$ injective function

  $m : A \rightarrowtail B$ is monic iff $\forall f, g : X \to A \quad f \cdot m = g \cdot m \Rightarrow f = g$

- epimorphism $\rightsquigarrow$ surjective function

  $e : A \twoheadrightarrow B$ is epic iff $\forall f, g : B \to X \quad e \cdot f = e \cdot g \Rightarrow f = g$

- We can also generalize many other notions:

  exponentiation

  union

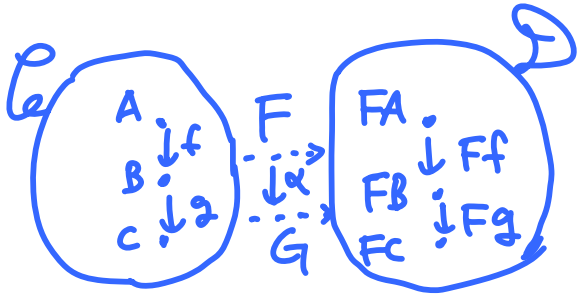
  intersection,

  relation,

  equivalence relation,

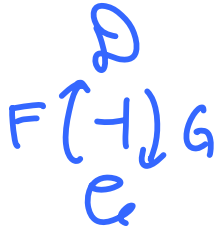
  ⋮

Structures between Categories

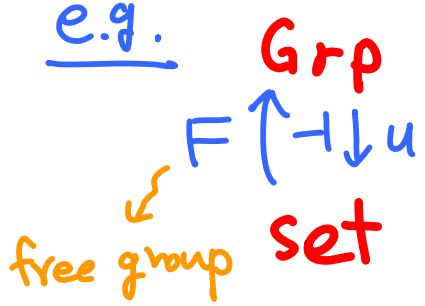


- Functor $F : \mathcal{C} \to \mathcal{D}$
  - map between categories
- Natural transformation $\alpha : F \Rightarrow G$
  - map between functors

- Adjunction $F \dashv G$
  - free construction



e.g.



- Monad $T : \mathcal{C} \to \mathcal{C}$
  - endo-functor equipped with special structures

Equational Reasoning

Category Theory

→ Term Equational Systems & Logics

Overview of Term Equational System

TES is a Categorical framework for equational reasoning and can accommodate

- the first-order equational system
- Combinatory Reduction System
- Binding Term Equational Logic
- Nominal Equational Logic

Definition of first-order equational system

- An algebraic theory is given by
  - a signature $\Sigma = \{\Sigma(n)\}_{n \in \mathbb{N}}$ and
  - a set E of equations of the form

$$V \vdash t = t'$$

- Example

The theory $\mathbb{G} = (\Sigma_{\mathbb{G}}, E_{\mathbb{G}})$ of groups

- $\Sigma_{\mathbb{G}}(0) = \{e\}$, $\Sigma_{\mathbb{G}}(1) = \{\dot{\sim}\}$, $\Sigma_{\mathbb{G}}(2) = \{m\}$
- $E_{\mathbb{G}}$ of group axioms

$$\{x\} \vdash m(e, x) = x$$

$$\{x\} \vdash m(\dot{\sim}(x), x) = e$$

$$\{x, y, z\} \vdash m(m(x, y), z) = m(x, m(y, z))$$

Definition of Term Equational System

- Motivation

  For $\mathbb{G} = (\Sigma_{\mathbb{G}}, E_{\mathbb{G}})$

  $\mathbf{Set}$ with $F_{\Sigma_{\mathbb{G}}}$ and $T_{\Sigma_{\mathbb{G}}}$ (free monad)

  where $F_{\Sigma_{\mathbb{G}}}(X) = X^0 + X^1 + X^2$

  $\cong \{e\} + \{i(x) \mid x \in X\} + \{m(x_1, x_2) \mid x_1, x_2 \in X\}$

  $T_{\Sigma_{\mathbb{G}}}(X) \cong$ the set of terms with variables in X

  $V \vdash t_1 = t_2$

  $\Leftrightarrow t_1, t_2 \in T_{\Sigma_{\mathbb{G}}}(V)$

  $\Leftrightarrow 1 \rightrightarrows T_{\Sigma_{\mathbb{G}}}(V)$ (parallel pair t_1, t_2)

- Definition of TES

  with a set E of equations of the form

  $\mathbb{C}$ (universe), $\mathbf{T}$ (syntax)

  $U, V \vdash t_1 \equiv t_2 \triangleq U \rightrightarrows \mathbf{T}(V)$ (parallel pair t_1, t_2)

  $\mathbf{T}(V)$ (equation)

Models of first-order equational system

- Example

  A model for the theory $\mathbb{G}$ of groups is

  - a set G with
  - functions $[\![e]\!] : 1 \to G$, $[\![i]\!] : G \to G$, $[\![m]\!] : G \times G \to G$

  such that

  for all $x, y, z \in G$

  $$[\![m]\!]([\![e]\!], x) = x, \quad [\![m]\!]([\![i]\!](x), x) = [\![e]\!],$$
  $$[\![m]\!]([\![m]\!](x,y), z) = [\![m]\!](x, [\![m]\!](y,z))$$

  $\tilde{\tilde{\leadsto}}$ a group in the usual sense

- Definition

  A model of a theory (Σ, E) is

  - a set M with $\{[\![o]\!] : M^n \to M\}_{n \in \mathbb{N}, o \in \Sigma(n)}$

  such that for each $(x_1, \dots, x_k \vdash t = t') \in E$

  $$\forall m_1, \dots, m_k \in M \quad [\![t]\!](m_1, \dots, m_k) = [\![t']\!](m_1, \dots, m_k)$$

Models of Term Equational System

- Motivation

G with $[\![e]\!], [\![i]\!], [\![m]\!]$

$\cong$ G with a function $1 \uplus G \uplus G^2 \to G$

$\cong$ G with a function $F_{\Sigma_G}(G) \to G$

$\cong$ G with a function $T_{\Sigma_G}(G) \to G$

satisfying ...

↑ called "Eilenberg-moore algebra for $\mathbb{T}_G$"

such that

$\forall x,y,z \in G \quad [\![m]\!]([\![m]\!](x,y),z) = [\![m]\!](x,[\![m]\!](y,z))$ ⟵ $1 \rightrightarrows T_{\Sigma_G}\{x,y,z\}$

$\vdots$ ↘ $G^3 \times 1 \rightrightarrows G$

- Definition

A model of a TES $\mathcal{C} \wr \mathbb{T}$ with E is

$M \in |\mathcal{C}|$ with a morphism $s : TM \to M$ satisfying ...

such that

$\forall (U, V \vdash t_1 \equiv t_2) \in E \quad [V, M] \otimes U \overset{[\![t_1]\!]}{\underset{[\![t_2]\!]}{\rightrightarrows}} M$

First-order equational logic

- For a theory (Σ, E)

$$\text{Ref}\ \frac{}{V \vdash t = t} \qquad \text{Sym}\ \frac{V \vdash t = t'}{V \vdash t' = t} \qquad \text{Tran}\ \frac{V \vdash t = t' \quad V \vdash t' = t''}{V \vdash t = t''}$$

$$\text{Axiom}\ \frac{}{V \vdash t = t'}\ (V \vdash t = t') \in E$$

$$\text{Subst}\ \frac{V \vdash t = t' \quad V \vdash s_1 = s_1' \ , \cdots , \ V \vdash s_n = s_n'}{V \vdash t[s_1/x_1, \cdots, s_K/x_K] = t'[s_1'/x_1, \cdots, s_K'/x_K]}$$

- Soundness & completeness

$V \vdash t = t'$ is provable from E

iff $V \vdash t = t'$ is satisfied by all models of (Σ, E)

Term Equational Logic

- For a TES $\mathcal{C} \wr \mathbb{T}$ with E
  - Equivalence relation

$$\frac{}{U,V \vdash t = t} \qquad \frac{U,V \vdash t \equiv t'}{U,V \vdash t' \equiv t} \qquad \frac{U,V \vdash t \equiv t' \quad U,V \vdash t' \equiv t''}{U,V \vdash t \equiv t''}$$

  - Axiom

$$\frac{}{U,V \vdash t \equiv t'} \; (U,V \vdash t \equiv t') \in E$$

  - Tensor extension

$$\frac{U,V \vdash t \equiv t'}{W \otimes U, W \otimes V \vdash \langle W \rangle t \equiv \langle W \rangle t'}$$

- Substitution

$$\frac{U,W \vdash t \equiv t' \quad W,V \vdash s \equiv s'}{U,V \vdash t[s] \equiv t'[s']}$$

- Local character

$$\frac{U_i,V \vdash t \cdot e_i \equiv t' \cdot e_i \;\; (i \in I)}{U,V \vdash t \equiv t'} \quad \{e_i : U_i \to U\}_{i \in I} \text{ jointly epi}$$

- Soundness

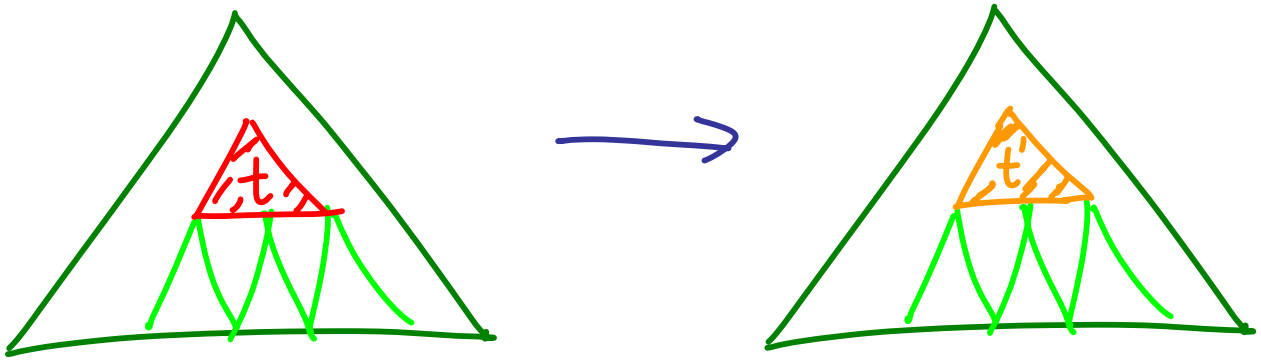
$U,V \vdash t \equiv t'$ is provable from E

$\Rightarrow$ $U,V \vdash t \equiv t'$ is satisfied by all models of $\mathcal{C} \wr \mathbb{T}$ with E

First-order rewriting system

- Rewriting rule

$$(V \vdash t = t') \in E$$



- Example

$$i(m(m(i(x), e), x)) \longrightarrow i(m(i(x), m(e, x)))$$

- Soundnes & Completness

$$t \overset{*}{\longleftrightarrow} t' \text{ from } E$$

$\Leftrightarrow$ $V \vdash t = t'$ is satisfied by all models of (Σ, E)

Simplification of Completness condition

For $\mathbf{S} = \mathfrak{C}^{\mathbf{T}}$ with E

$U, V \vdash t \equiv t'$ is satisfied by all models of $\mathbf{S}$

$\Leftrightarrow$ $U, V \vdash t \equiv t'$ is satisfied by the free model on V

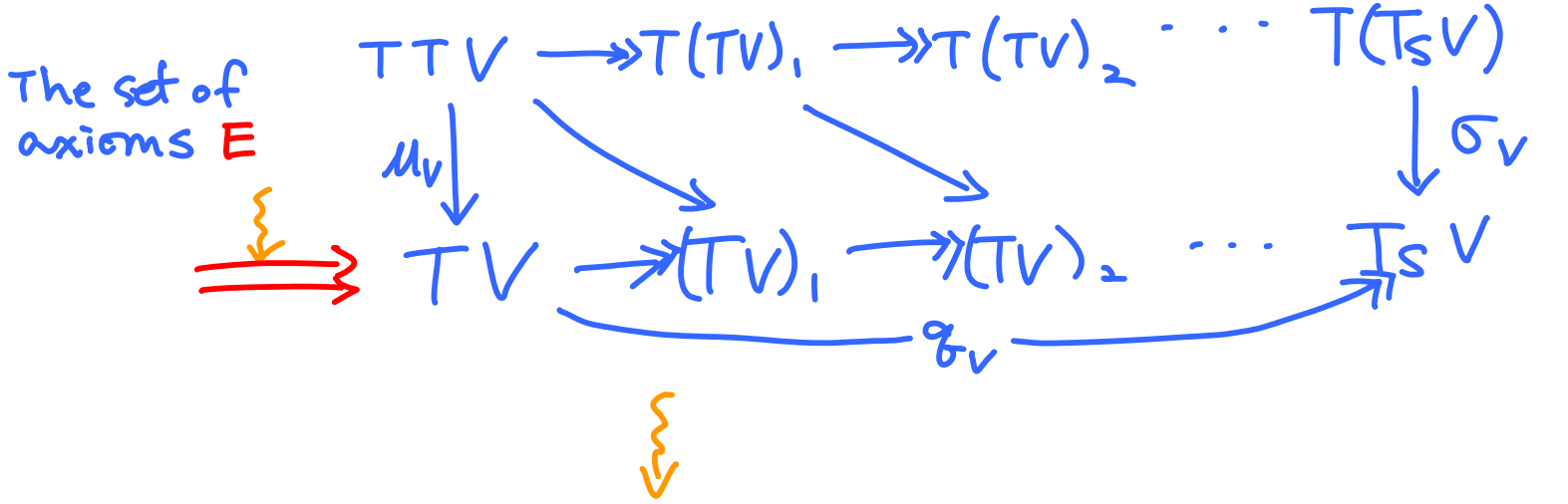
$\left(\mathbf{T}_{\mathbf{S}}V, \sigma_V : \mathbf{T}(\mathbf{T}_{\mathbf{S}}V) \to (\mathbf{T}_{\mathbf{S}}V)\right)$

$\Leftrightarrow$ $U \overset{t}{\underset{t'}{\rightrightarrows}} \mathbf{T}V \xrightarrow{q_V} \mathbf{T}_{\mathbf{S}}V$

※ Here, we assume that free models for $\mathbf{S}$ exist.

Towards complete rewriting system for TES

- "Equational systems and free construction" (Fiore & Hur, ICALP 07) provides a construction of free models.



intuitively defines a rewriting system

Example : Rewriting system for the TES of groups

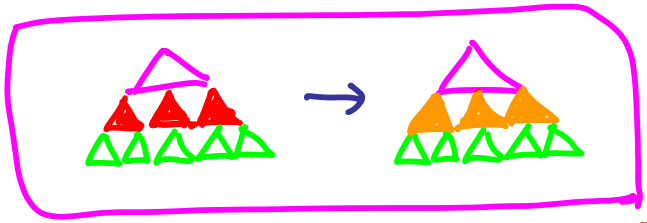
For the TES $\mathbf{Set}^{\mathbb{T}_{\Sigma_G}}$ with E_G

$$Q : 1, V \vdash t_1 \equiv t_2 \quad \Leftrightarrow \quad 1 \rightrightarrows \mathbb{T}_{\Sigma_G} V \xrightarrow{q_V} T_G V$$

$$\begin{array}{ccccccccc}
\mathbb{T}_{\Sigma_G}\mathbb{T}_{\Sigma_G}V & \twoheadrightarrow & \mathbb{T}_{\Sigma_G}(\mathbb{T}_{\Sigma_G}V)_1 & \twoheadrightarrow & \mathbb{T}_{\Sigma_G}(\mathbb{T}_{\Sigma_G}V)_2 & \cdots & \mathbb{T}_{\Sigma_G}(T_G V) & & \\
\downarrow{\scriptstyle \mu_V} & & & \searrow & \downarrow{\scriptstyle \text{po}} & & \downarrow{\scriptstyle \varepsilon_V} & & \\
T_G V + T_G V + T_G V^3 & \rightrightarrows & \mathbb{T}_{\Sigma_G} V & \xrightarrow{\text{coeq}} & (\mathbb{T}_{\Sigma_G} V)_1 & \twoheadrightarrow & (\mathbb{T}_{\Sigma_G} V)_2 & \cdots & T_G V
\end{array}$$

$$q_V$$

$$\frac{t \in T_G V}{m(t, e) \approx (t)} \qquad \frac{t \in T_G V}{m(i(t), t) \approx e} \qquad \frac{t_1, t_2, t_3 \in T_G V}{m(m(t_1, t_2), t_3) \approx m(t_1, m(t_2, t_3))}$$



$$\frac{t \in T_{\Sigma_G}\{x_1, \ldots, x_k\},\ s_1 \approx s_1', \ldots, s_k \approx s_k'}{t(s_1, \ldots, s_k) \approx t(s_1', \ldots, s_k')}$$

- $T_G V = T_{\Sigma_G} V / \approx$
- $1 \rightrightarrows \mathbb{T}_{\Sigma_G} V \xrightarrow{q_V} T_{\Sigma_G} V / \approx$

$\Leftrightarrow [t_1]_\approx = [t_2]_\approx \Leftrightarrow t_1 \overset{*}{\leftrightarrow} t_2$

Concluding Remarks

- Applications
  - First-order equational logic (Set)
  - Cominatory Reduction System ($Set^{\mathbb{F}}$)
  - Binding Term Equational Logic ($Set^{\mathbb{I}}$)
  - Nominal Equational Logic (Nom)

- Further work
  - Abstract condition for confluence
  - Abstract condition for termination