

# 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

$$\begin{array}{l} \text{Sig: } 0:0 \quad s:1 \quad +:2 \\ \text{Eqn: } +(0, n) = n \\ \quad \quad \quad +(s(n), m) = s(+(n, m)) \end{array}$$

$$\text{Q: } +(s(0), 0) = +(0, s(0))$$

① by logic

$$\begin{array}{c} \frac{\frac{\frac{}{+(0,0)=0}}{s(+(0,0))=s(0)}{+(s(0),0)=s(+(0,0))}}{+(s(0),0)=s(0)} \quad \frac{\frac{}{+(0,s(0))=s(0)}}{s(0)=+(0,s(0))}}{s(0)=+(0,s(0))}}{+(s(0),0)=+(0,s(0))} \end{array}$$

② by rewriting

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

# Higher-order Equational Reasoning

- Consider the equation

$$\forall x. P(x) \wedge Q(x) = (\forall x. P(x)) \wedge (\forall x. Q(x))$$

binding

↑ first-order var  
↑ second-order var

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

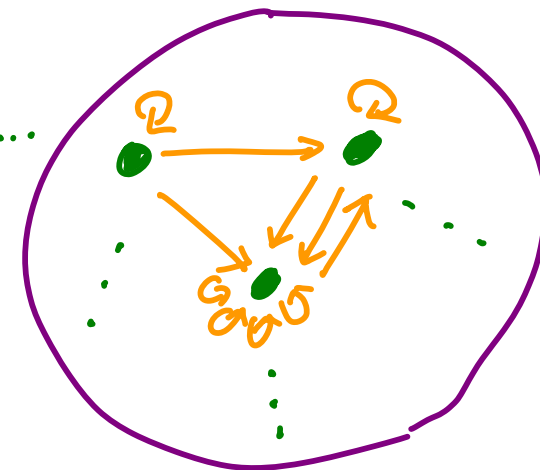
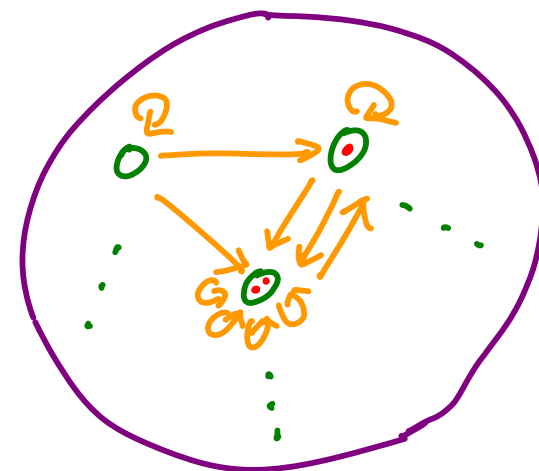
- sets & functions
- groups & homomorphisms
- topological spaces & continuous maps



- 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  $\rightsquigarrow$  sets

②  $\forall A, B \in |\mathcal{C}|$

$\mathcal{C}(A, B)$  : a collection of morphisms from  $A$  to  $B$

③  $\forall A \in |\mathcal{C}|$

$\text{id}_A \in \mathcal{C}(A, A) \rightsquigarrow$  identity function

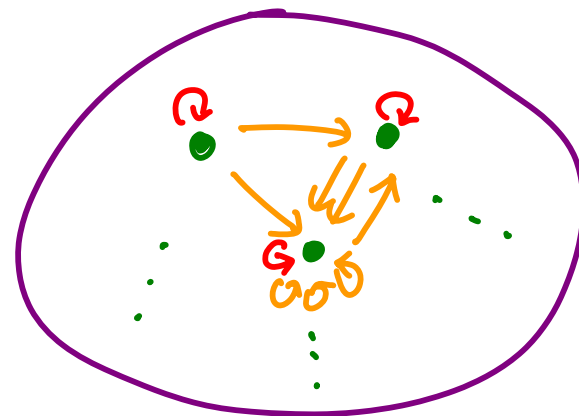
④  $\forall A, B, C \in |\mathcal{C}|$

$\cdot : \mathcal{C}(B, C) \times \mathcal{C}(A, B) \rightarrow \mathcal{C}(A, C)$

$\rightsquigarrow$  function composition

Satisfying

$$\forall f, g, h \quad \text{id} \cdot f = f, f \cdot \text{id} = f, (f \cdot g) \cdot h = f \cdot (g \cdot h)$$



functions from  $A$  to  $B$



# Examples of categories

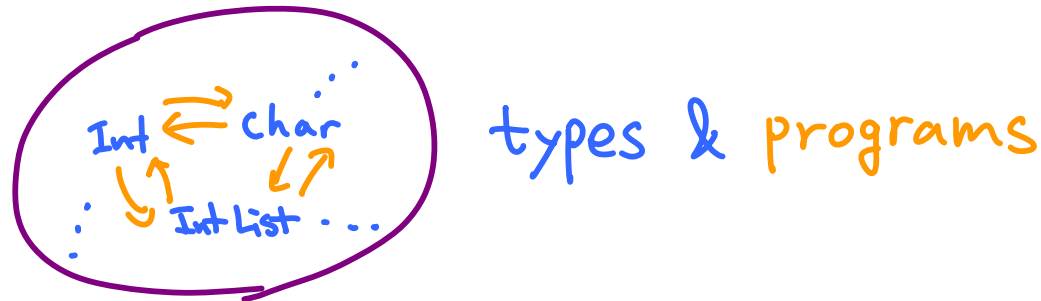
**Set** : sets & functions

**Grp** : groups & homomorphisms

**Top** : topological spaces & continuous functions

**Cpo** : chain-complete partial orders & continuous functions

⋮



# Limits and Colimits

- Initial object  $\rightsquigarrow$  Empty set  
 $0 \in |\mathcal{C}|$  is initial iff  $\forall x \in |\mathcal{C}| \exists ! f: 0 \rightarrow x$
- Terminal object  $\rightsquigarrow$  singleton set  
 $1 \in |\mathcal{C}|$  is terminal iff  $\forall x \in |\mathcal{C}| \exists ! f: x \rightarrow 1$
- Product  $\rightsquigarrow$  product set  
for  $A, B \in |\mathcal{C}|$   
 $A \times B \in |\mathcal{C}|$  with  $\pi_1: A \times B \rightarrow A, \pi_2: A \times B \rightarrow B$  is a product of  $A, B$   
iff  
 $\forall x \in |\mathcal{C}|$  with  $p: x \rightarrow A, q: x \rightarrow B$   
 $\exists ! f: x \rightarrow A \times B$  s.t. 
$$\begin{array}{ccc} & x & \\ p \swarrow & \downarrow f & \searrow q \\ A & \xleftarrow{\pi_1} & A \times B & \xrightarrow{\pi_2} & B \end{array}$$
 commutes.
- Coproducts, pull backs, pushouts, equalizers, coequalizers  
 $\downarrow$   
disjoint unions

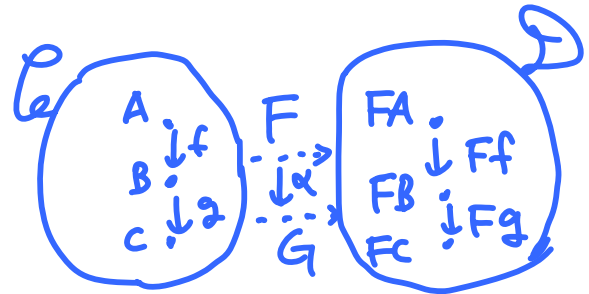
## Other Categorical Notions

- monomorphism  $\rightsquigarrow$  injective function  
 $m: A \rightarrow B$  is monic iff  $\forall f, g: X \rightarrow A \quad f \cdot m = g \cdot m \Rightarrow f = g$
- epimorphism  $\rightsquigarrow$  surjective function  
 $e: A \rightarrow B$  is epic iff  $\forall f, g: B \rightarrow X \quad e \cdot f = e \cdot g \Rightarrow f = g$
- We can also generalize many other notions:
  - exponentiation
  - union
  - intersection,
  - relation,
  - equivalence relation,
  - ⋮

# Structures between Categories

- Functor  $F: \mathcal{C} \rightarrow \mathcal{D}$

↪ map between categories

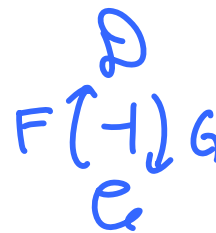


- Natural transformation  $\alpha: F \rightarrow G$

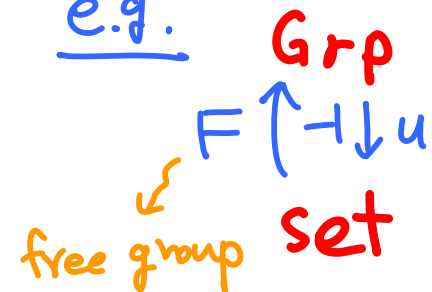
↪ map between functors

- Adjunction  $F \dashv G$

↪ free construction



e.g.



- Monad  $T: \mathcal{C} \rightarrow \mathcal{C}$

↪ 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

$$\forall t = t'$$

- Example

The theory  $G = (\Sigma_G, E_G)$  of groups

-  $\Sigma_G(0) = \{e\}$ ,  $\Sigma_G(1) = \{\cdot\}$ ,  $\Sigma_G(2) = \{m\}$

-  $E_G$  of group axioms

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

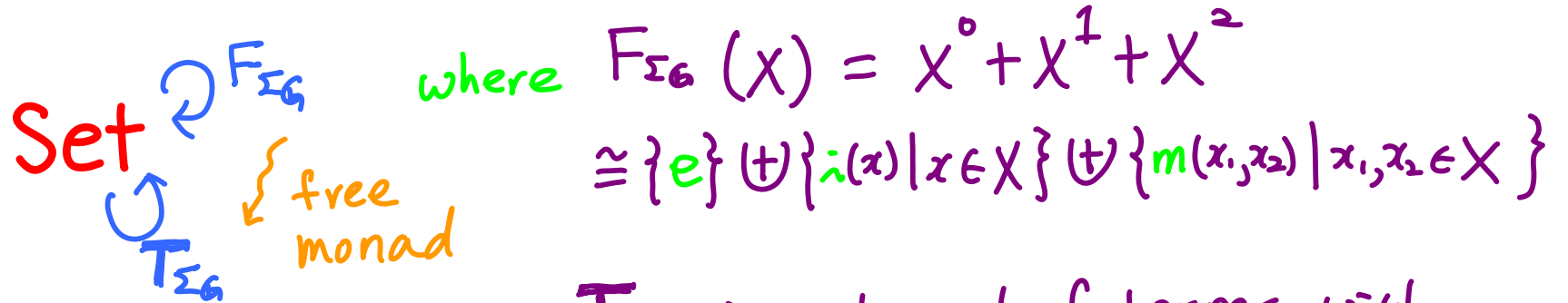
$$\{x\} \vdash m(\cdot(x), x) = e$$

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

# Definition of Term Equational System

- Motivation

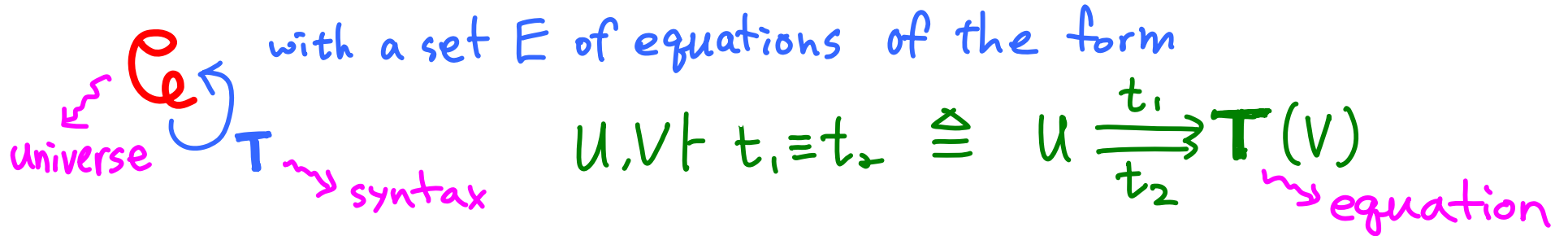
For  $G = (\Sigma_G, E_G)$



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

$$\begin{aligned} V \models t_1 = t_2 \\ \Leftrightarrow t_1, t_2 \in T_{\Sigma_G}(V) \\ \Leftrightarrow 1 \xrightarrow[t_2]{t_1} T_{\Sigma_G}(V) \end{aligned}$$

- Definition of TES





## Models of first-order equational system

- Example

A model for the theory  $G$  of groups is

- a set  $G$  with

- functions  $[e]: 1 \rightarrow G$ ,  $[i]: G \rightarrow G$ ,  $[m]: G \times G \rightarrow G$

such that

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

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

$$[m]([m](x, y), z) = [m](x, [m](y, z))$$

$\cong \rightarrow$  a group in the usual sense

- Definition

A model of a theory  $(\Sigma, E)$  is

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

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  $\llbracket e \rrbracket, \llbracket i \rrbracket, \llbracket m \rrbracket$
- $\cong G$  with a function  $1 \uplus G \uplus G^2 \rightarrow G$
- $\cong G$  with a function  $F_{\Sigma_G}(G) \rightarrow G$
- $\cong G$  with a function  $T_{\Sigma_G}(G) \rightarrow G$  satisfying ...

such that

called "Eilenberg-moore algebra for  $T_{\Sigma_G}$ "

$$\forall x, y, z \in G \quad \llbracket m \rrbracket(\llbracket m \rrbracket(x, y), z) = \llbracket m \rrbracket(x, \llbracket m \rrbracket(y, z)) \quad \leftarrow 1 \Rightarrow T_{\Sigma_G}\{x, y, z\}$$

$G^3 \times 1 \xrightarrow{\quad} G$

- Definition

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

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

such that

$$\forall (u, v \vdash t_1 \equiv t_2) \in E \quad [v, M] \otimes u \xrightarrow{\llbracket t_1 \rrbracket} M \xrightarrow{\llbracket t_2 \rrbracket} M$$

## First-order equational logic

- For a theory  $(\Sigma, E)$

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

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

$$\text{Subst} \frac{V \vdash t = t' \quad V \vdash s_1 = s'_1, \dots, V \vdash s_n = s'_n}{V \vdash t[\frac{s_1}{x_1}, \dots, \frac{s_n}{x_n}] = t'[\frac{s'_1}{x_1}, \dots, \frac{s'_n}{x_n}]}$$

- Soundness & completeness

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

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

# Term Equational Logic

• For a TES  $\mathcal{C}^{\mathcal{Q}T}$  with  $E$

- Equivalence relation

$$\frac{}{u, v \vdash t = t}$$

$$\frac{u, v \vdash t \equiv t'}{u, v \vdash t' \equiv t}$$

$$\frac{u, v \vdash t \equiv t' \quad u, v \vdash t' \equiv t''}{u, v \vdash t \equiv t''}$$

- Axiom

$$\frac{}{u, v \vdash t \equiv t'} \quad (u, v \vdash t \equiv t') \in E$$

• Substitution

$$\frac{u, w \vdash t \equiv t' \quad w, v \vdash s \equiv s'}{u, v \vdash t[s] \equiv t'[s']}$$

- Tensor extension

$$\frac{u, v \vdash t \equiv t'}{w \otimes u, w \otimes v \vdash \langle w \rangle t \equiv \langle w \rangle t'}$$

• Local character

$$\frac{u_i, v \vdash t \cdot e_i \equiv t' \cdot e_i \quad (i \in I)}{u, v \vdash t \equiv t'} \quad \{e_i: u_i \rightarrow u\}_{i \in I} \text{ jointly epi}$$

• Soundness

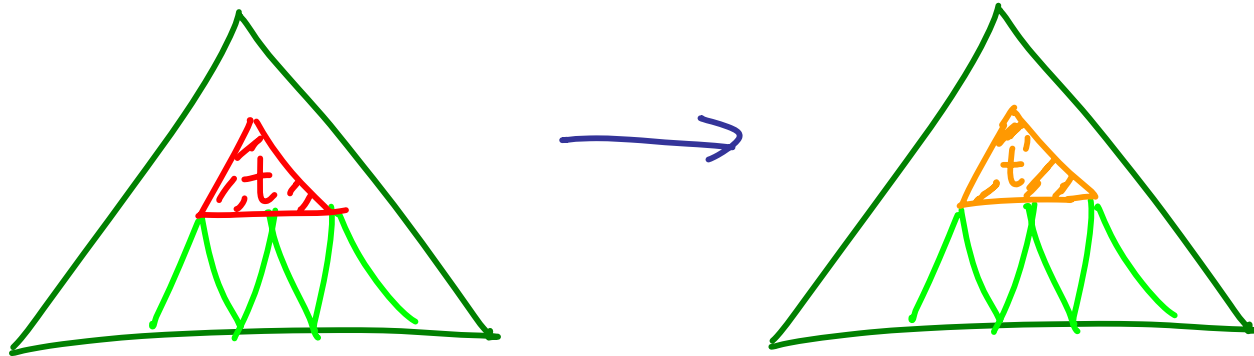
$u, v \vdash t \equiv t'$  is provable from  $E$

$\Rightarrow u, v \vdash t \equiv t'$  is satisfied by all models of  $\mathcal{C}^{\mathcal{Q}T}$  with  $E$

# First-order rewriting system

- Rewriting rule

$$(\forall t = t') \in E$$



- Example

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

- Soundness & Completeness

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

$$\Leftrightarrow \forall t = t' \text{ is satisfied by all models of } (\Sigma, E)$$

## Simplification of Completeness condition

For  $S = \mathcal{E}^{\mathcal{T}}$  with  $E$

$u, v \vdash t \equiv t'$  is satisfied by all models of  $S$

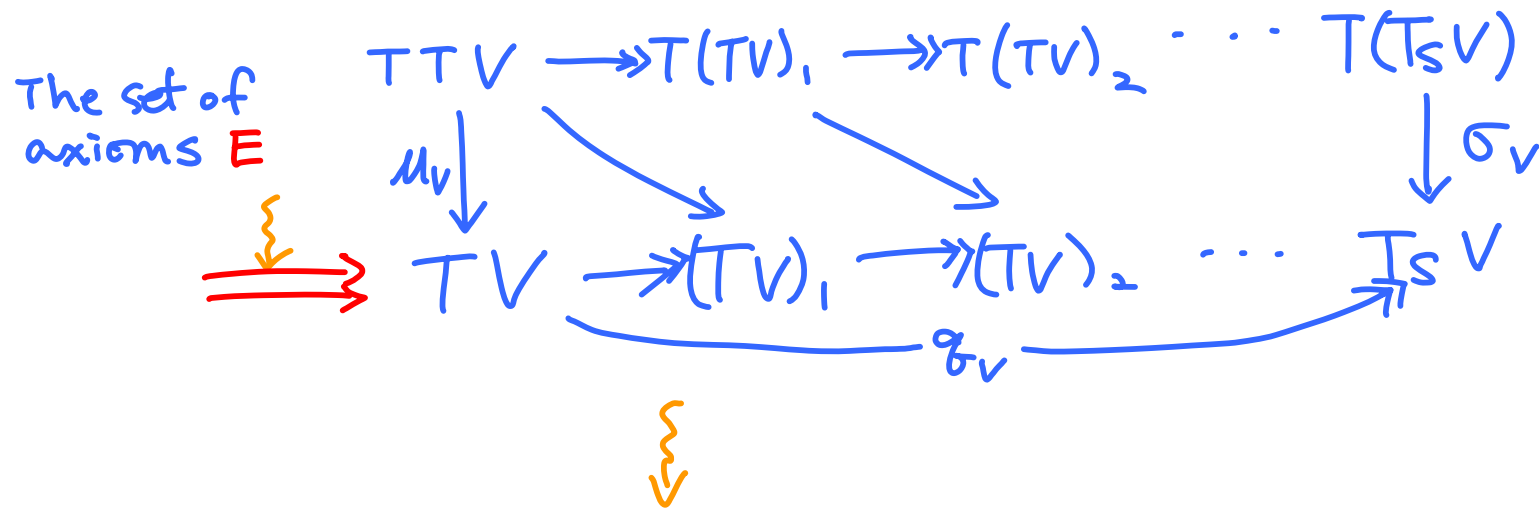
$\Leftrightarrow u, v \vdash t \equiv t'$  is satisfied by the free model on  $V$   
( $T_S V, \sigma_V: T(T_S V) \rightarrow (T_S V)$ )

$\Leftrightarrow u \xrightarrow[t']{t} TV \xrightarrow{\sigma_V} T_S V$

\* Here, we assume that free models for  $S$  exist.

# Towards complete rewriting system for TES

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

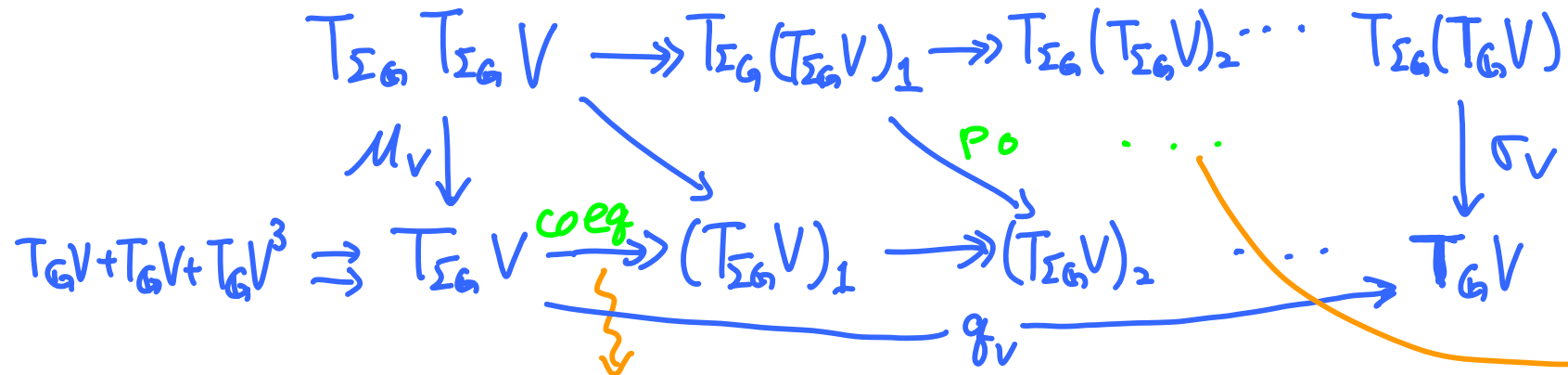


intuitively defines a rewriting system

# Example: Rewriting system for the TES of groups

For the TES Set  $\mathcal{Q}_{T_{\Sigma_G}}$  with  $E_G$

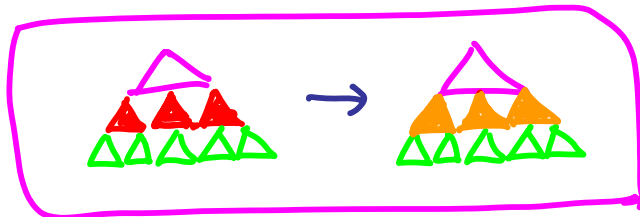
$$Q: 1, V \vdash t_1 \equiv t_2 \iff 1 \xrightarrow[t_2]{t_1} T_{\Sigma_G} V \xrightarrow{q_V} T_G V$$



$$\frac{t \in T_G V}{m(t, e) \approx (t)}$$

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

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



$$\frac{t \in T_{\Sigma_G} \{x_1, \dots, x_k\}, s_i \approx s'_i, \dots, s_k \approx s'_k}{t(s_1, \dots, s_k) \approx t(s'_1, \dots, s'_k)}$$

- $T_G V = T_{\Sigma_G} V / \approx$
- $1 \xrightarrow[t_2]{t_1} T_{\Sigma_G} V \xrightarrow{q_V} T_{\Sigma_G} V / \approx$   
 $\iff [t_1]_{\approx} = [t_2]_{\approx} \iff t_1 \overset{*}{\leftrightarrow} t_2$



## Concluding Remarks

- Applications
  - First-order equational logic (Set)
  - Combinatory Reduction System (Set<sup>FF</sup>)
  - Binding Term Equational Logic (Set<sup>II</sup>)
  - Nominal Equational Logic (Nom)
- Further work
  - Abstract condition for confluence
  - Abstract condition for termination