Hereditarily Finite Sets in Constructive Type Theory

joint work with Gert Smolka

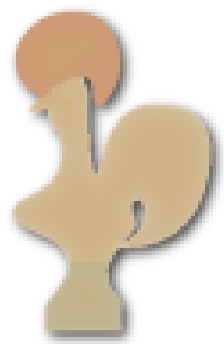
Kathrin Stark
Advisor: Prof. Dr. Gert Smolka

SAARLAND UNIVERSITY
COMPUTER SCIENCE

15th March 2016

Constructive Type Theory

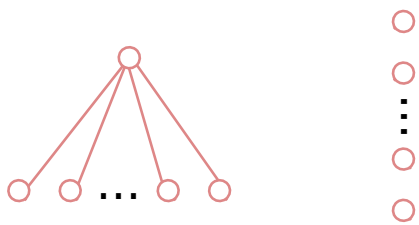
- based on the Curry-Howard Isomorphism:
  propositions as types, proofs as programs
- working with
  - dependent function types: $\forall$
  - dependent pair types: $\exists$
- Coq: an interactive theorem prover working on the Calculus of Inductive Constructions



What are Hereditarily Finite (HF) Sets?

$$\frac{}{\emptyset : HF} \qquad \frac{x : HF \quad y : HF}{\underbrace{\{x\} \cup y}_{x.y} : HF}$$

$\Rightarrow$ finite and well-founded sets whose members are again HF



Sources

Moto-o Takahashi, 1977.
A foundation of finite mathematics.

Steven Givant, Alfred Tarski, 1977.
Peano arithmetic and the Zermelo-like theory of sets with finite rank.

Flavio Previale, 1994.
Induction and foundation in the theory of hereditarily finite sets.

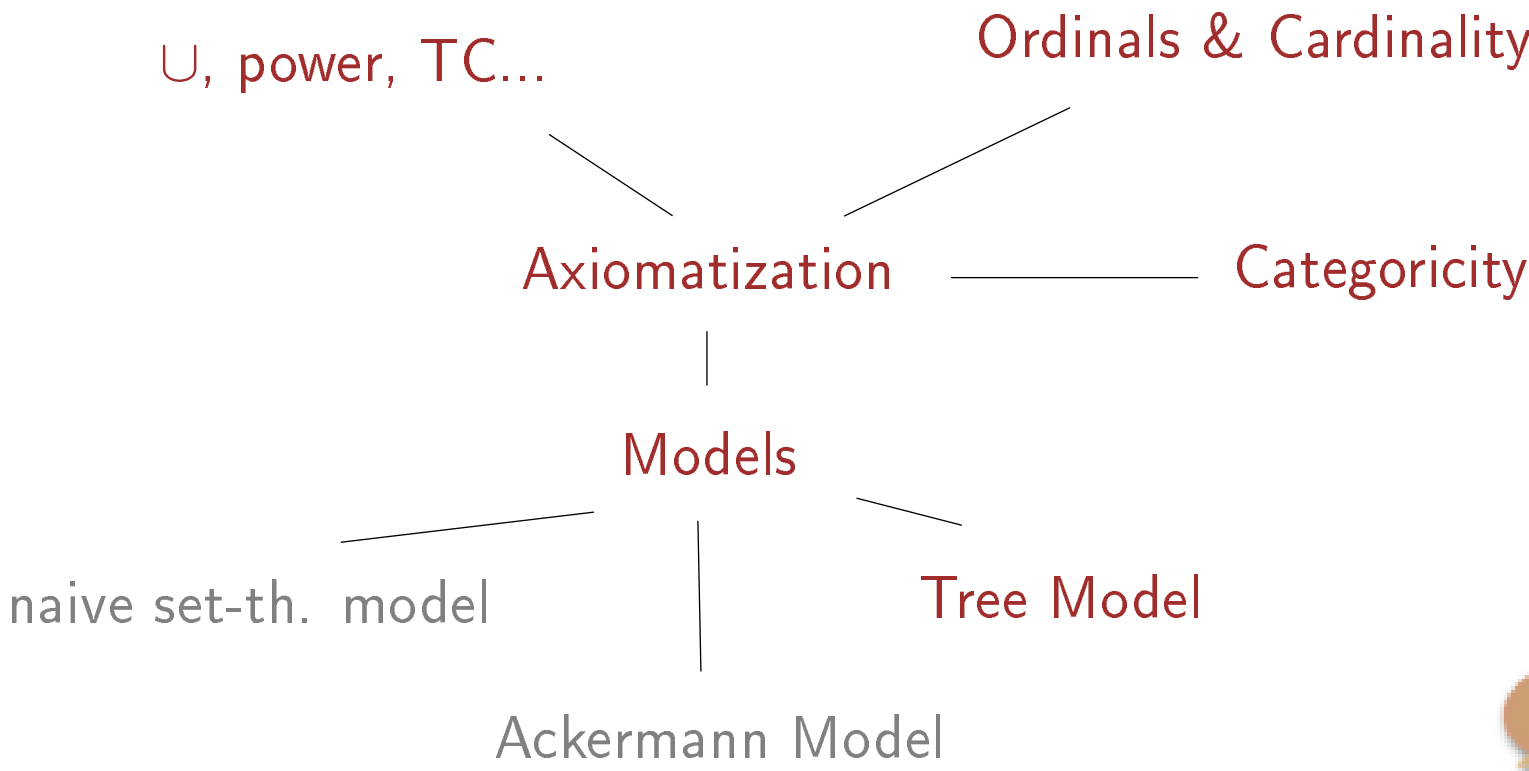
S. Świerczowski, 2003.
Finite sets and Gödel's incompleteness theorems.

Laurence Kirby, 2009.
Finitary set theory.

Lawrence C. Paulson, 2015.
A mechanised Proof of Gödel's Incompleteness Theorem using Nominal Isabelle.

Lawrence C. Paulson, 2015.
A formalisation of finite automata using hereditarily finite sets.

Outline


∪, power, TC...
Ordinals & Cardinality
Axiomatization
Categoricity
Models
naive set-th. model
Tree Model
Ackermann Model

ZF with Negated Infinity

Primitives: $\emptyset, \in$

- $(\forall z.z \in x \leftrightarrow z \in y) \rightarrow x = y$ **Extensionality**
- $(\forall x.(\forall z \in x.p(x)) \rightarrow \forall x.p(x))$ **Epsilon induction**
- $z \notin \emptyset$ **Empty Set**
- $z \in pair\ x\ y \leftrightarrow z = x \vee z = y$ **Unordered Pair**
- $z \in \cup\ x\ y \leftrightarrow z \in x \vee z \in y$ **Union**
- $z \in \mathcal{P}\ x \leftrightarrow z \subseteq x$ **Power**
- $z \in f[x] \leftrightarrow \exists a \in x.f\ a = z$ **Replacement**
- $z \in x|p \leftrightarrow z \in x \wedge p\ z$ **Separation**
- $+$ restriction to get just the finite sets?

Takahashi (1977), Givant & Tarksi (1977), Świerczkowski (2003)

Primitives: $\emptyset,\ x.y,\ x \in y$

- $(\forall z.z \in x \leftrightarrow z \in y) \rightarrow x = y$ **Extensionality**
- $z \notin \emptyset$ **Empty Set**
- $z \in x.y \leftrightarrow z = x \vee z \in y$ **Membership**
- $p(\emptyset) \rightarrow (\forall ax.p(a) \rightarrow p(x) \rightarrow p(a.x)) \rightarrow \forall x.p(x)$ **Induction**

Previale, 1994

Primitives: $\emptyset,\ x.y,\ x\backslash y,\ x \in y,\ x < y$

• $(\forall z.z \in x \leftrightarrow z \in y) \rightarrow x = y$	**Extensionality**
• $z \notin \emptyset$	**Empty Set**
• $z \in x.y \leftrightarrow z = x \vee z \in y$	**Membership**
• $p(\emptyset) \rightarrow (\forall xy.p(x) \rightarrow p(y) \rightarrow y \notin x \rightarrow p(x.y)) \rightarrow \forall x.p(x)$	**Induction**
• $z \in x\backslash y \leftrightarrow z \in x \wedge z \neq y$	**Without**
• $z \not< \emptyset$	**Size $\emptyset$**
• $z < x.y \leftrightarrow z < x \vee z \leq y$	**Size Adj.**

Kirby, 2009

Primitives: $\emptyset$, $x.y$

• $x.\emptyset \neq \emptyset$	**Empty Set**
• $x.(x.y) = x.y$	**Cancel**
• $x.(y.z) = y.(x.z)$	**Swap**
• $z \in x.y \leftrightarrow z = x \vee z \in y$	**Membership**
• $z.x.y = x.y \rightarrow z = x \vee z.y = y$	**Membership**
• $p(\emptyset) \rightarrow (\forall ax.p(a) \rightarrow p(x) \rightarrow p(a.x)) \rightarrow \forall x.p(x)$	**Induction**

Define $x \in y := x.y = y$.
Extensionality is still provable.

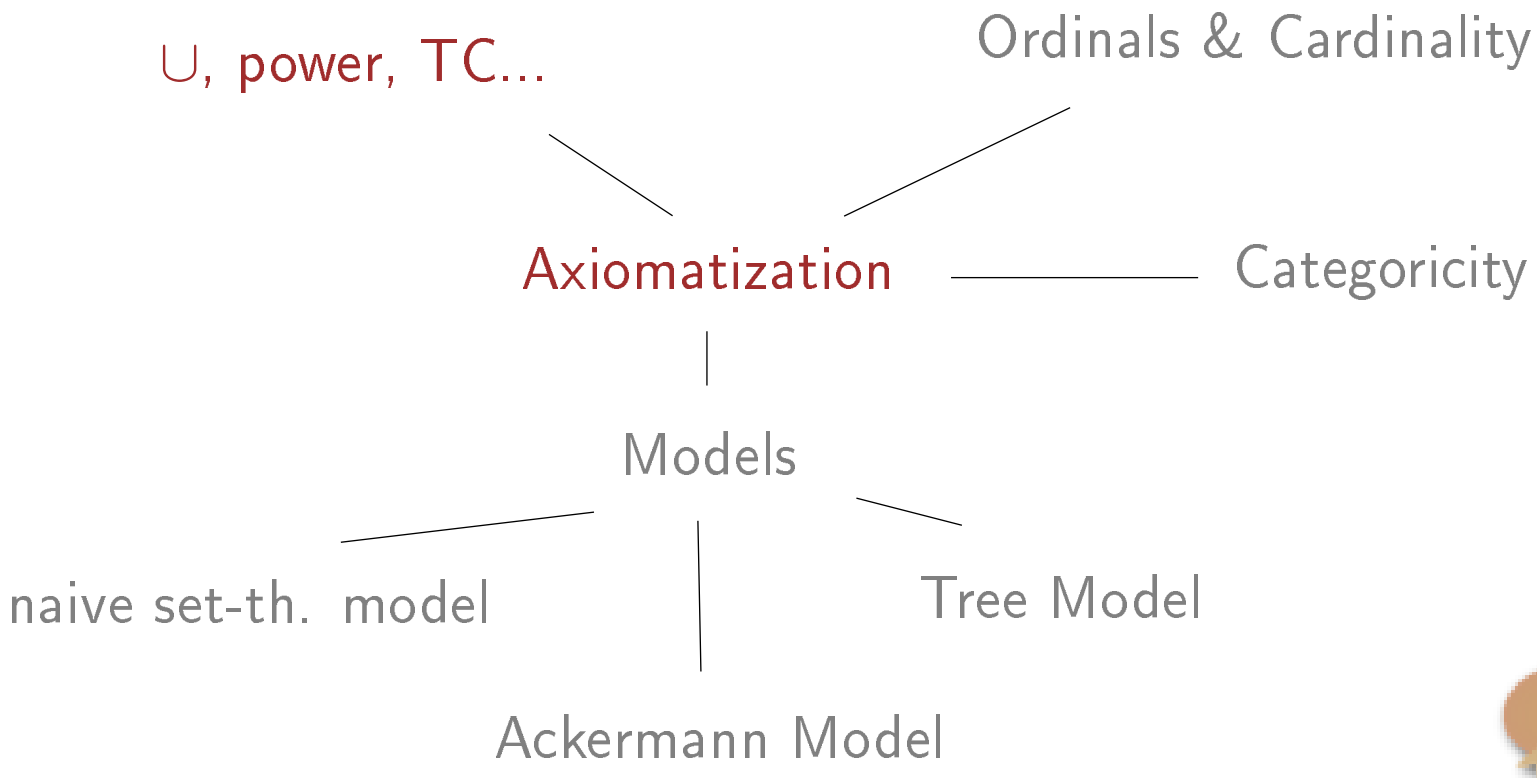
Our Axiomatization

Primitives: $\emptyset,\ x.y$

- $\forall x\ y : HF. x = y \ \overline{\vee}\ x \neq y$ **Discreteness**
- $x.y \neq \emptyset$ **Empty Set**
- $x.(x.y) = x.y$ **Cancel**
- $x.(y.z) = y.(x.z)$ **Swap**
- $z.x.y = x.y \ \rightarrow \ z = x \vee z.y = y$ **Membership**
- $\forall p : X \rightarrow Type.$

  $p(\emptyset) \rightarrow (\forall ax.p(a) \rightarrow p(x) \rightarrow p(a.x)) \rightarrow \forall x.p(x)$ **Induction**

Outline


∪, power, TC...
Ordinals & Cardinality
Axiomatization
Categoricity
Models
naive set-th. model
Tree Model
Ackermann Model

Defining Union

Functional Programming

1. Define recursive equations.
   $\Rightarrow x \cup y :=$
   $R \underbrace{y}_{\emptyset \cup y} (\lambda a\, x \underbrace{pa}_{a \cup y} \underbrace{px}_{x \cup y} .(a.px))\, x$
2. Prove specification.

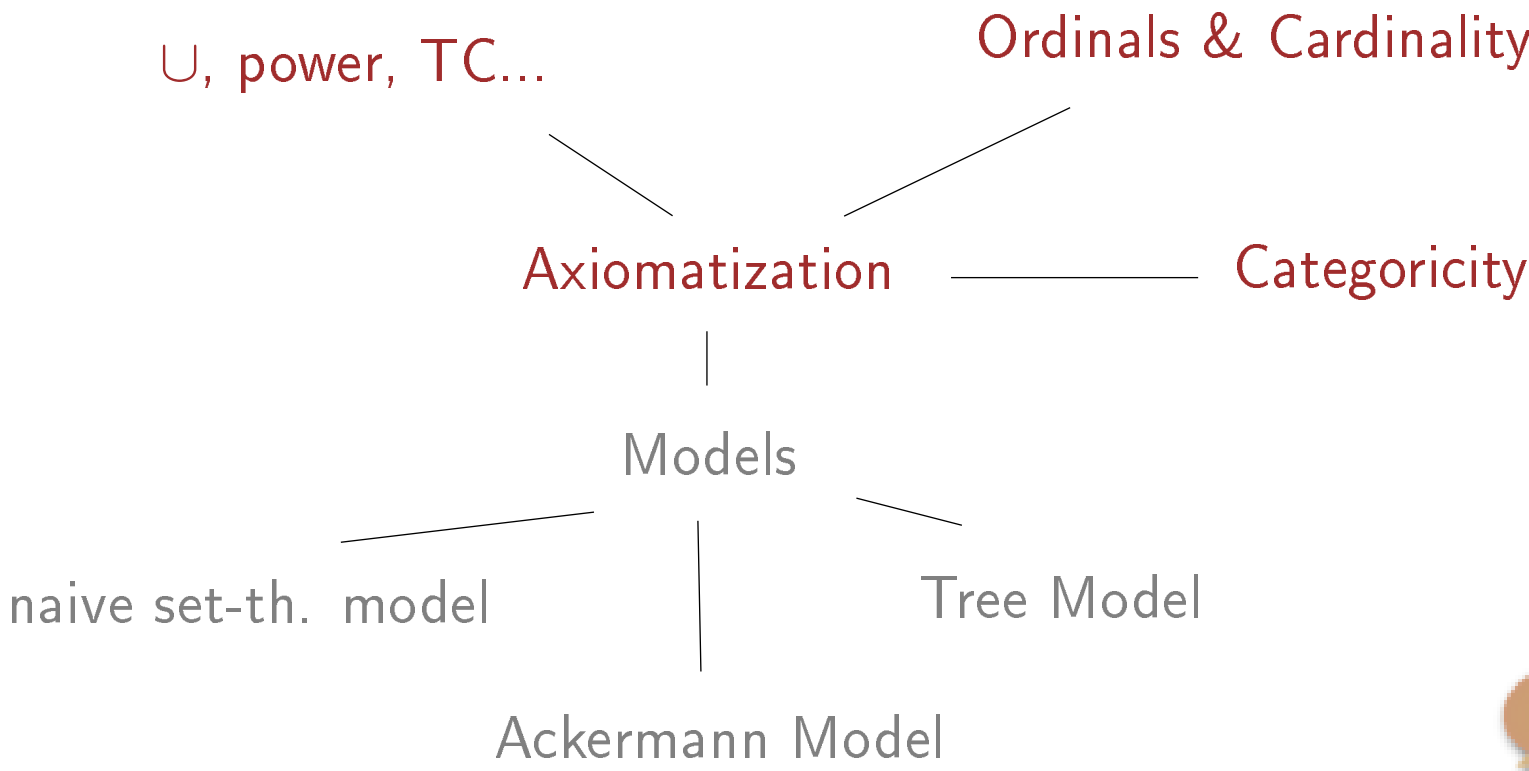
Recursion Principle

But: We have no equations for the recursor! So how to prove that $x \cup y$ satisfies the desired properties?

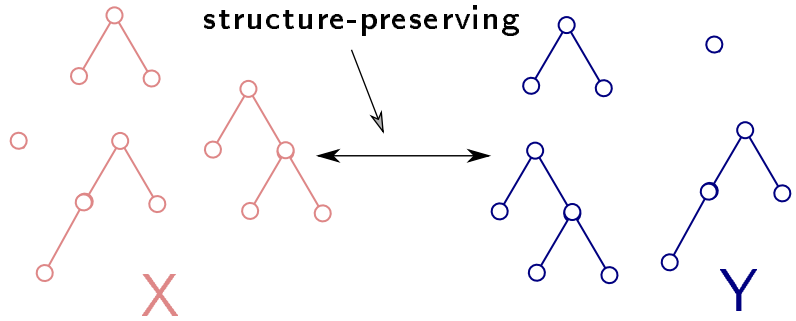
1. Define specification.
   $x \cup' y :$
   $\overline{\exists} u. \forall z.\, z \in u \leftrightarrow z \in x \vee z \in y$
2. Prove recursive equations.

$$R : \forall p : X \to Type.p(\emptyset) \to (\forall ax.p(a) \to p(x) \to p(a.x)) \to \forall x.p\ x$$

Outline


∪, power, TC...
Ordinals & Cardinality
Axiomatization
Categoricity
Models
naive set-th. model
Tree Model
Ackermann Model

Categoricity



algebraic isomorphism + homomorphism + bisimulation

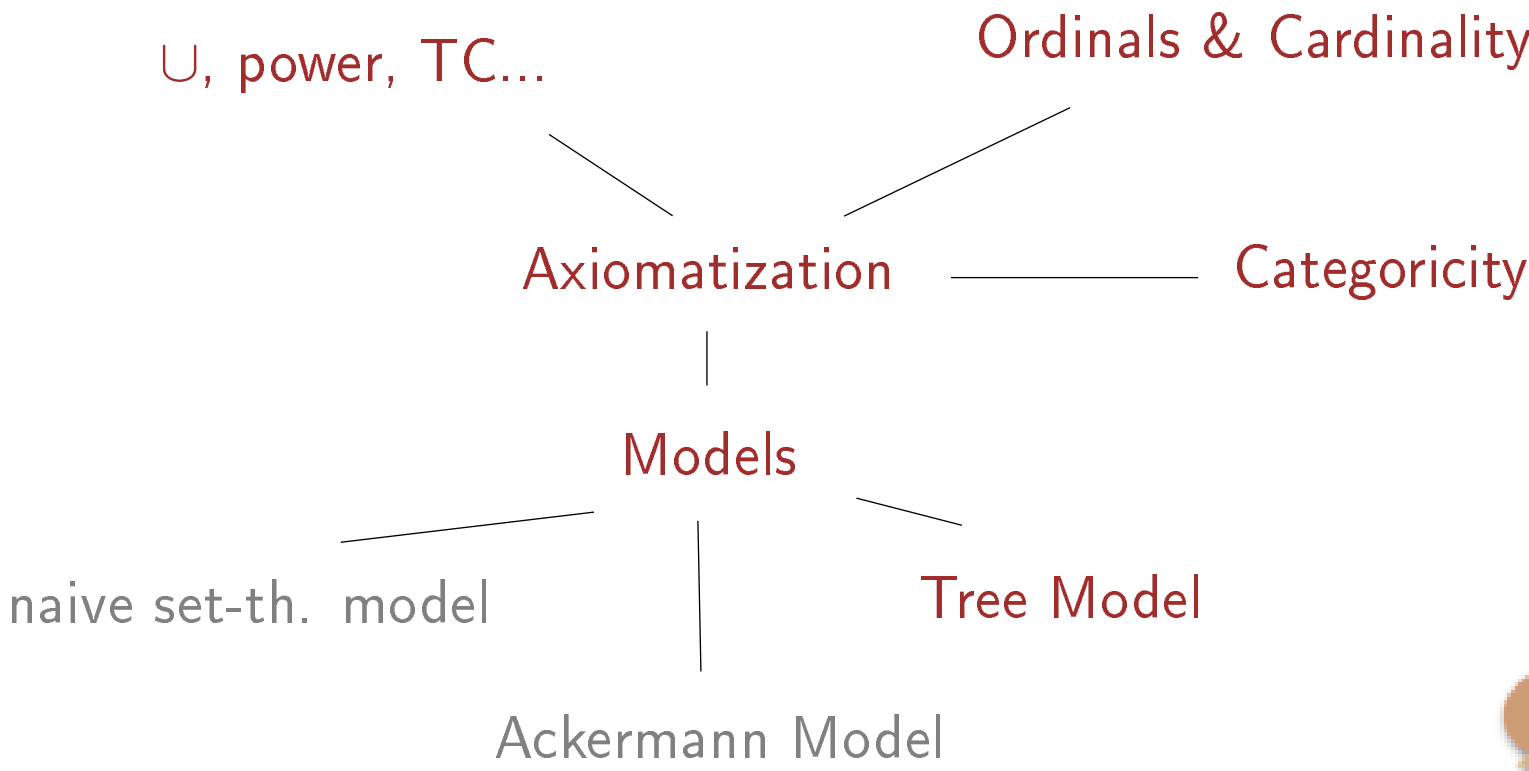
$$\frac{}{R\ \emptyset\ \emptyset} \qquad \frac{R\ a\ b \quad R\ x\ y}{R\ (a.x)\ (b.y)}$$

Totality: $\forall x \overline{\exists} y.R\ x\ y$

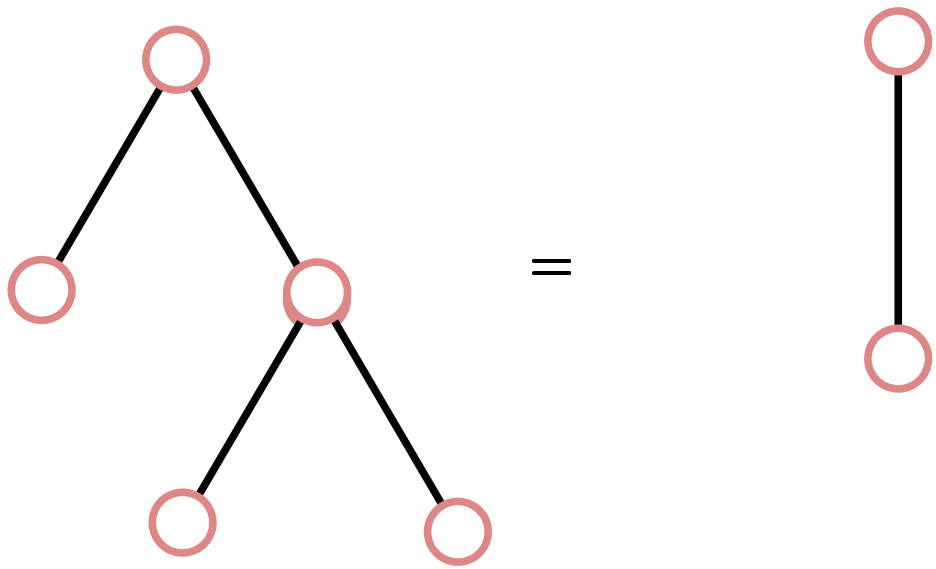
Simulation: $R\ x\ y \to a \in x \to \exists b.b \in y \wedge R\ a\ b$

Functionality: $R\ x\ y \to R\ x\ y' \to y = y'$

Outline

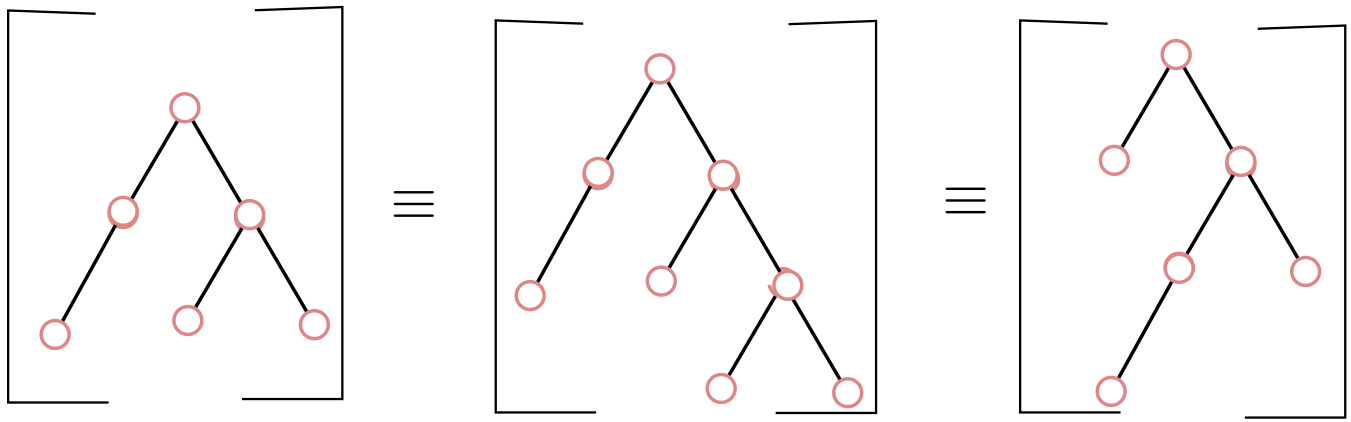

∪, power, TC...
Ordinals & Cardinality
Axiomatization
Categoricity
Models
naive set-th. model
Tree Model
Ackermann Model

Equality of HF Sets



$\{\emptyset, \emptyset\}$

Constructing a Model From Binary Trees



$$\{\{\emptyset\}, \emptyset\}$$

$\Rightarrow$ Construct a normalizer σ and then a quotient of binary trees.

Denis Müller. A Syntactic Theory of Finitary Sets. Bachelor Thesis, 2015.

Future Work

- Construct the Ackermann model.
- Finite sets of decidable types.
- Extension to non-wellfounded sets.

Thank you for your attention!