Wellfounded and Extensional Ordinals in Homotopy Type Theory

Nicolai Kraus

joint work with
Fredrik Nordvall Forsberg and Chuangjie Xu
(arXiv: Connecting Constructive Notions of Ordinals in Homotopy Type Theory)

Developments in Computer Science, Budapest/online, 17–19 June 2021

(1) What are ordinals?

Simple answer: **Numbers** for counting/ordering, e.g.

$0, 1, 2, 3, \ldots, \omega, \omega+1, \omega+2, \ldots, \underset{= \omega+\omega}{\omega\cdot 2}, \omega\cdot 2+1, \ldots, \underset{= \omega\cdot\omega}{\omega^2}, \ldots, \omega^\omega, \ldots, \omega^{\omega^{\omega^{\omega}}}$

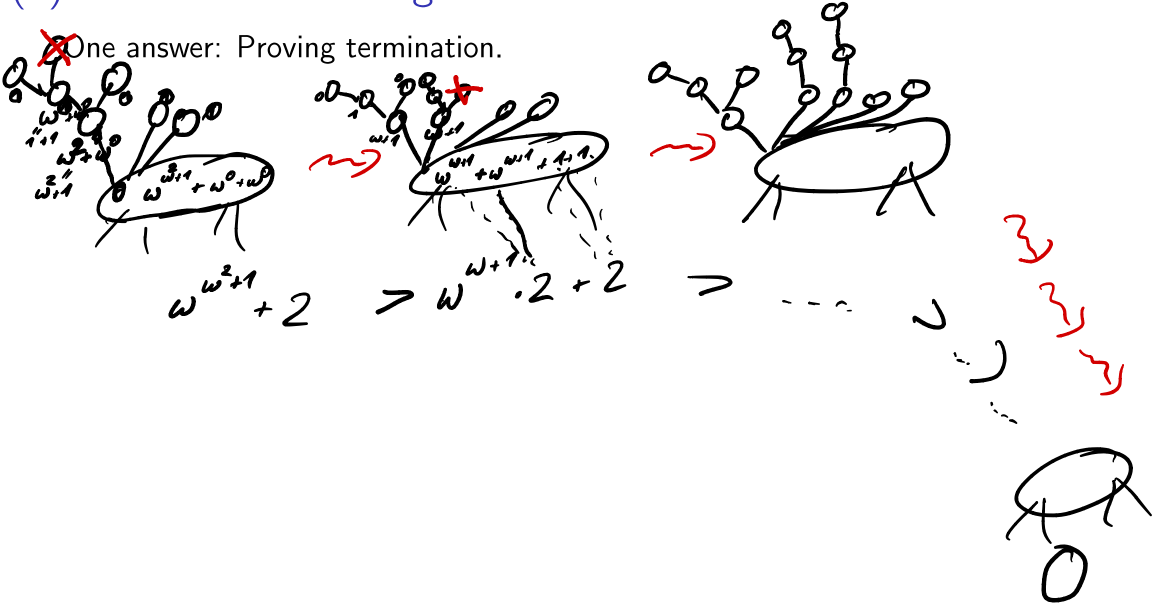
Caveat: $\mathbb{N} \uplus \mathrm{Bool} \simeq \mathbb{N}$, $\omega \neq \omega+2$

Better answer: **Sets with an order** $<$ which is

- transitive $x<y \to y<z \to x<z$
- wellfounded every sequence $x_0 > x_1 > x_2 > \ldots$ terminates
- and trichotomous $\forall x y.\ x<y \uplus x=y \uplus y<x$
- . . . or extensional (instead of trichotomous) $\left(\forall z.\ (z<x \leftrightarrow z<y)\right) \to x=y$

(2) What are ordinals good for?

One answer: Proving termination.



$$\omega^{\omega^2+1}+2 > \omega^{\omega+1}\cdot 2+2 > \dots$$

(3) How can we define ordinals in type theory?

Problem/feature of a constructive setting: different definition differ.

In our work (with Fred and Chuangjie), we study:

- Cantor normal forms decidable
- Brouwer trees partially decidable
- wellfounded and extensional orders. undecidable

(3A) Cantor normal forms

Motivation: $\alpha = \omega^{\beta_1} + \omega^{\beta_2} + \cdots + \omega^{\beta_n}$ with $\beta_1 \geq \beta_2 \geq \cdots \geq \beta_n$

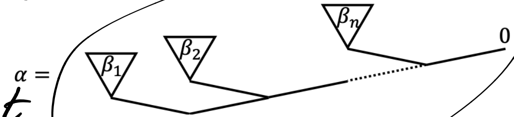
Definition

- Let $\mathcal{T}$ be the type of *unlabeled binary trees*:

leaf $\to$ $0 \quad : \mathcal{T}$

node $\to$ $\omega^{-} + - \quad : \mathcal{T} \to \mathcal{T} \to \mathcal{T}$

node(s,t) write $\omega^{s} + t$



- Let $<$ be the *lexicographical order* on $\mathcal{T}$.
- Define $\mathsf{isCnf}(\alpha)$ to express $\beta_1 \geq \beta_2 \geq \cdots \geq \beta_n$.

We write $\mathsf{Cnf} :\equiv \Sigma(t : \mathcal{T}).\mathsf{isCnf}(t)$ for the type of *Cantor normal forms*.

(3B.1) Brouwer trees (a.k.a. Brouwer ordinal trees)

How about this inductive type $\mathcal{O}$ of Brouwer trees?

$$\text{zero} : \mathcal{O} \qquad \text{succ} : \mathcal{O} \to \mathcal{O} \qquad \text{sup} : (\mathbb{N} \to \mathcal{O}) \to \mathcal{O}$$

$$\text{sup}(0, 1, 2, 3, \ldots)$$

$$\neq \text{sup}(1, 2, 3, \ldots)$$

(3B.2) Brouwer trees quotient inductive-inductively

```
data Brw where
  zero  : Brw
  succ  : Brw → Brw
  limit : (f : ℕ → Brw) → {f↑ : increasing f} → Brw
  bisim : ∀ f {f↑} g {g↑} →
          f ≈ g →
          limit f {f↑} ≡ limit g {g↑}
  trunc : isSet Brw
```

f simulated by g $:\equiv$
$\forall i. \exists j. f i \leq g j$

```
data _≤_ where
  ≤-zero      : ∀ {x} → zero ≤ x
  ≤-trans     : ∀ {x y z} → x ≤ y → y ≤ z → x ≤ z
  ≤-succ-mono : ∀ {x y} → x ≤ y → succ x ≤ succ y
  ≤-cocone    : ∀ {x} f {f↑ k} → (x ≤ f k) → (x ≤ limit f {f↑})
  ≤-limiting  : ∀ f {f↑ x} → ((k : ℕ) → f k ≤ x) → limit f {f↑} ≤ x
  ≤-trunc     : ∀ {x y} → isProp (x ≤ y)
```

(3C.1) Extensional wellfounded orders

Definition

The type Ord consists of pairs $(X : \mathrm{Type}, \prec : X \to X \to \mathrm{Prop})$ such that:

- $\prec$ is transitive
  - $x \prec y \to y \prec z \to x \prec z$;
- $\prec$ is extensional
  - elements with the same $\prec$-predecessors are equal;
- $\prec$ is wellfounded
  - every element is accessible, where x is accessible if every $y \prec x$ is accessible.

data Acc : $A \to$ Type where
  acc : $(a : A) \to (\forall b < a, \mathrm{Acc}\ b) \to \mathrm{Acc}\ a$

$\prec$ is wellfounded if $\forall a.\ \mathrm{Acc}\ a$

(3C.2) Extensional wellfounded orders

Let $(X, \prec_X)$, $(Y, \prec_Y)$: Ord.

$X \leq Y$ is:

- a *monotone* function $f : X \to Y$
- such that: if $y \prec_Y f\, x$, then there is $x_0 \prec_X x$ such that $f\, x_0 = y$.

Such an f is a *simulation*.

For $y : Y$, define $Y_{/y} :\equiv \Sigma(y' : Y).y' \prec y$.

$X < Y$ is:

- a simulation $f : X \leq Y$
- such that there is $y : Y$ and f factors through $X \simeq Y_{/y}$.

$f : X < Y$ is a *bounded simulation*.

(4) Abstract setting

What do Cnf, Brw, Ord have to do with each other?
Why are they "types of ordinals"?

Assume we have a set A with relations $<, \leq$ such that:

- $<$ is transitive and irreflexive;
- $\leq$ is transitive, reflexive, and antisymmetric;
- $(<) \subset (\leq)$;
- $(< \circ \leq) \leq (<)$. $(x<y) \to (y \leq z) \to (x<z)$

Caveat: $(x \leq y) \to (y < z) \to (x < z)$
is <u>not</u> constructively true for Ord

(4.1) Abstract setting: first properties

When is $(A, <, \leq)$ a "type of ordinals"?

First properties:

- A is set, $<$ and $\leq$ valued in props
- $<$ is wellfounded
- $<$ and $\leq$ are extensional

✓ for Cnf, Brw, Ord

(4.2) Abstract setting: Zero, successor, limit "classification"

Obvious definitions:

$a : A$ is *zero* if $\forall b. a \leq b$.

a is a *successor* of b if $a > b$ and $\forall x > b. x \geq a$.
The successor is *strong* if b is the predecessor of a.

a is a *supremum* of $f : \mathbb{N} \to A$ if $\forall i. f_i \leq a$ and $(\forall i. f_i \leq x) \to a \leq x$.
If f is increasing, we say that a is its limit.

"Concrete" results: 1) Cnf, Brw, Ord uniquely have zero and strong successor.
2) Brw, Ord uniquely have limits.
3) For Cnf, Brw, we can decide in which case we are.

"Abstract" result: is-zero$(a) \uplus$ is-str-suc$(a) \uplus$ is-limit(a) is a proposition.

(4.3) Abstract arithmetic: addition

Definition

$(A, <, \leq)$ *has addition* if we have a function $+ : A \to A \to A$ such that:

$$\text{is-zero}(a) \to c + a = c$$
$$a \text{ is-suc-of } b \to d \text{ is-suc-of } (c + b) \to c + a = d$$
$$a \text{ is-lim-of } f \to b \text{ is-sup-of } (\lambda i. c + f_i) \to c + a = b$$

$c + \bigsqcup f = \bigsqcup c + f_i$

$(A, <, \leq)$ *has unique addition* if there is exactly one function $+$ with these properties.

Concrete result: Cnf and Brw have unique addition.
Ord has addition (Q: is it unique?).

(4.4) Abstract arithmetic: multiplication

Assume that $(A, <, \leq)$ has addition.

Definition

$(A, <, \leq)$ *has multiplication* if we have $\cdot : A \to A \to A$ such that:

$$\text{is-zero}(a) \to c \cdot a = a$$
$$a \text{ is-suc-of } b \to c \cdot a = c \cdot b + c$$
$$a \text{ is-lim-of } f \to b \text{ is-sup-of } (\lambda i. c \cdot f_i) \to c \cdot a = b$$

$(A, <, \leq)$ *has unique multiplication* if it has unique addition and there is exactly one function $\cdot$ with the above properties.

Concrete result: Cnf and Brw have unique multiplication.
Ord has multiplication (Q: is it unique?).

(4.5) Abstract arithmetic: exponentation

Assume that $(A, <, \leq)$ has addition and multiplication.

Definition

A *has exponentation with base* c if there is $\text{exp}(c, -) : A \to A$ such that:

$$\text{is-zero}(b) \to a \text{ is-suc-of } b \to \text{exp}(c, b) = a$$
$$a \text{ is-suc-of } b \to \text{exp}(c, a) = \text{exp}(c, b) \cdot c$$
$$a \text{ is-lim-of } f \to \neg\text{is-zero}(c) \to b \text{ is-sup-of } (\text{exp}(c, f_i)) \to \text{exp}(c, a) = b$$
$$a \text{ is-lim-of } f \to \text{is-zero}(c) \to \text{exp}(c, a) = c$$

A *has unique exponentation with base* c if it has unique addition and multiplication, and if $\text{exp}(c, -)$ is unique.

Concrete result: Cnf and Brw have unique exponentation (with base ω). (Q: Can you show a constructive taboo if Ord has the same?)

(5) Connections between the notions

decidable — partially decidable — undecidable

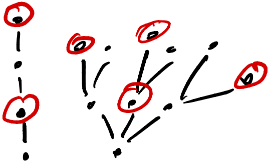
$$\boxed{\mathsf{Cnf}} \xhookrightarrow{\mathsf{CtoB}} \boxed{\mathsf{Brw}} \xhookrightarrow{\mathsf{BtoO}} \boxed{\mathsf{Ord}}$$

$(\omega^a + b) \mapsto \omega^{\mathsf{CtoB}(a)} + \mathsf{CtoB}(b)$

$0 \mapsto 0$

$A \mapsto \Sigma(Y : \mathsf{Brw}).Y < A$

- injective
- preserves and reflects $<$, $\leq$
- commutes with $+$, $*$, ω^x
- bounded (by ϵ_0)



- injective
- preserves $<$, $\leq$
- over-approximates $+$, $*$:
  $\mathsf{BtoO}(x + y) \geq \mathsf{BtoO}(x) + \mathsf{BtoO}(y)$
- commutes with limits
  (but not successors)
- BtoO is a simulation $\Rightarrow$ WLPO
- LEM $\Rightarrow$ BtoO is a simulation
- bounded (by Brw)