Constructive Ordinal Exponentiation in Homotopy Type Theory

Tom de Jong[1] Nicolai Kraus[1]
Fredrik Nordvall Forsberg[2] Chuangjie Xu[3]

[1]University of Nottingham, UK
[2]University of Strathclyde, UK
[3]SonarSource GmbH, Germany

TYPES 2024, Copenhagen, 13 June 2024

Come to the Scottish Programming Languages and Verification summer school at the University of Strathclyde! 29 July–2 August.

Ordinals in homotopy type theory

- In the HoTT book, an ordinal is defined as a type X with a prop-valued binary relation $\prec$ that is transitive, extensional and wellfounded.
- Extensionality means that we have

$$x = y \iff \forall (u : X).(u \prec x \iff u \prec y).$$

  It follows that X is an hset.
- Wellfoundedness is defined in terms of accessibility, but is equivalent to the assertion that for every $P : X \to \mathcal{U}$, we have $\Pi(x : X).P(x)$ as soon as $\Pi(x : X).(\Pi(y : X).(y \prec x \to P(y))) \to P(x)$.

Many other more specialised (and well behaved) notions of ordinals [Martin-Löf 1970; Taylor 1996; Coquand, Lombardi and Neuwirth 2023, ...] , but here we focus on the most general notion.

The ordinal of ordinals

The type of (small) ordinals Ord can itself be given the structure of a (large) ordinal by defining

$$\alpha < \beta :\equiv \Sigma(b : \beta).(\alpha = (\Sigma(x : \beta).x \prec b)).$$

Proving that $<$ is extensional makes crucial use of the univalence axiom.

The ordinal of ordinals

The type of (small) ordinals Ord can itself be given the structure of a (large) ordinal by defining

$$\alpha < \beta :\equiv \Sigma(b : \beta).(\alpha = (\Sigma(x : \beta).x \prec b)).$$

Proving that $<$ is extensional makes crucial use of the univalence axiom.

Similarly, we define $\alpha \leq \beta$ if "α embeds into β without gaps":

$$\alpha \leq \beta :\equiv \Sigma(f : \alpha \xrightarrow{o.p.} \beta).(y \prec f\,x \to \Sigma(x_0 : \alpha).(x_0 \prec x) \times (y = f\,x_0)).$$

The ordinal of ordinals

The type of (small) ordinals Ord can itself be given the structure of a (large) ordinal by defining

$$\alpha < \beta :\equiv \Sigma(b : \beta).(\alpha = (\Sigma(x : \beta).x \prec b)).$$

Proving that $<$ is extensional makes crucial use of the univalence axiom.

Similarly, we define $\alpha \leq \beta$ if "α embeds into β without gaps":

$$\alpha \leq \beta :\equiv \Sigma(f : \alpha \xrightarrow{o.p.} \beta).(y \prec f\, x \to \Sigma(x_0 : \alpha).(x_0 \prec x) \times (y = f\, x_0)).$$

Ord is closed under suprema of (small) families of ordinals $\mathsf{sup} : (I \to \mathsf{Ord}) \to \mathsf{Ord}$.

Ordinal arithmetic

$$\alpha + 0 = \alpha$$
$$\alpha + (\beta + 1) = (\alpha + \beta) + 1$$
$$\alpha + \sup \gamma_i = \sup(\alpha + \gamma_i) \qquad \text{(if index set } I \text{ inhabited)}$$

$$\alpha \times 0 = 0$$
$$\alpha \times (\beta + 1) = (\alpha \times \beta) + \alpha$$
$$\alpha \times \sup \gamma_i = \sup(\alpha \times \gamma_i)$$

$$\alpha^0 = 1$$
$$\alpha^{\beta+1} = \alpha^\beta \times \alpha$$
$$\alpha^{\sup \gamma_i} = \sup(\alpha^{\gamma_i}) \qquad \text{(if } I \text{ inhabited, and } \alpha \neq 0)$$
$$0^\beta = 0 \qquad \text{(if } \beta \neq 0)$$

Ordinal arithmetic

$$\boxed{\begin{aligned} \alpha + 0 &= \alpha \\ \alpha + (\beta + 1) &= (\alpha + \beta) + 1 \end{aligned}}$$

$$\alpha + \sup \gamma_i = \sup(\alpha + \gamma_i) \qquad \text{(if index set } I \text{ inhabited)}$$

$$\boxed{\begin{aligned} \alpha \times 0 &= 0 \\ \alpha \times (\beta + 1) &= (\alpha \times \beta) + \alpha \end{aligned}}$$

$$\alpha \times \sup \gamma_i = \sup(\alpha \times \gamma_i)$$

$$\boxed{\begin{aligned} \alpha^0 &= 1 \\ \alpha^{\beta+1} &= \alpha^\beta \times \alpha \end{aligned}}$$

$$\alpha^{\sup \gamma_i} = \sup(\alpha^{\gamma_i}) \qquad \text{(if } I \text{ inhabited, and } \alpha \neq 0)$$

$$0^\beta = 0 \qquad \text{(if } \beta \neq 0)$$

Ordinal arithmetic

$$\alpha + 0 = \alpha$$

$$\alpha + (\beta + 1) = (\alpha + \beta) + 1$$

$$\alpha + \sup \gamma_i = \sup(\alpha + \gamma_i) \qquad \text{(if index set } I \text{ inhabited)}$$

$$\alpha \times 0 = 0$$

$$\alpha \times (\beta + 1) = (\alpha \times \beta) + \alpha$$

$$\alpha \times \sup \gamma_i = \sup(\alpha \times \gamma_i)$$

$$\alpha^0 = 1$$

$$\alpha^{\beta+1} = \alpha^\beta \times \alpha$$

$$\alpha^{\sup \gamma_i} = \sup(\alpha^{\gamma_i}) \qquad \text{(if } I \text{ inhabited, and } \alpha \neq 0)$$

$$0^\beta = 0 \qquad \text{(if } \beta \neq 0)$$

Not a definition, constructively! But a good specification.

Addition and multiplication

For addition and multiplication, there are well known explicit constructions:

$$\langle \alpha + \beta \rangle :\equiv \langle \alpha \rangle + \langle \beta \rangle$$

with $\mathsf{inl}\ a \prec \mathsf{inr}\ b$, and

$$\langle \alpha \times \beta \rangle :\equiv \langle \alpha \rangle \times \langle \beta \rangle$$

ordered reverse lexicographically:

$$(a, b) \prec (a', b') :\equiv (b \prec b') + ((b = b') \times (a \prec a')).$$

Theorem. The operations $\alpha + \beta$ and $\alpha \times \beta$ satisfy the specifications for addition and multiplication, respectively.

What about exponentiation?

Surprisingly, there is no nice "geometric" construction of ordinal exponentiation.

What about exponentiation?

Surprisingly, there is no nice "geometric" construction of ordinal exponentiation.

Sierpiński [1958] constructs, for α with a least element $\bot : \alpha$, the exponential α^β as

$$\Sigma(f : \beta \to \alpha).\, \mathsf{supp}(f) \text{ finite}$$

where $\mathsf{supp}(f) :\equiv \Sigma(x : \beta).(f\, x > \bot)$.

What about exponentiation?

Surprisingly, there is no nice “geometric” construction of ordinal exponentiation.

Sierpiński [1958] constructs, for α with a least element $\bot : \alpha$, the exponential α^β as

$$\Sigma(f : \beta \to \alpha).\,\mathsf{supp}(f) \text{ finite}$$

where $\mathsf{supp}(f) :\equiv \Sigma(x : \beta).(f\,x > \bot)$.

The order is defined by

$$f \prec g :\equiv f(b^*) \prec_\alpha g(b^*),$$

where b^* is the largest element x such that $f(x) \neq g(x)$ — such b^* exists by the finite support assumption.

This is not nice, constructively!

A more concrete construction

Assume α has a detachable least element, i.e., $\alpha = 1 + \gamma$.

Examples. $\omega = 1 + \omega$, and $17 = 1 + 16$.

A more concrete construction

Assume α has a detachable least element, i.e., $\alpha = 1 + \gamma$.

Examples. $\omega = 1 + \omega$, and $17 = 1 + 16$.

We can try to make Sierpiński's construction more concrete.

Definition. For ordinals γ and β, let

$$[1+\gamma]^{\beta} :\equiv \Sigma(xs : \mathsf{List}(\gamma \times \beta)).\,(\mathsf{map\ snd}\ xs)\ \mathsf{decreasing}.$$

- $[1+\gamma]^{\beta}$ represents a function $\beta \to (1+\gamma)$ as a list of output-input pairs; elements not in the list are sent to $\mathsf{inl}\ \star$.
- Being strictly decreasing in the second component ensures that each input has at most one output.
- It also ensures that each "function" has at most one representation.

$[1+\gamma]^\beta$ is an ordinal

We can give $[1+\gamma]^\beta$ an order by inheriting the (ordinary) lexicographic order on $\mathsf{List}(\gamma \times \beta)$.

Theorem. $[1+\gamma]^\beta$ is an ordinal if γ and β are ordinals.

Remark. In general, the lexicographic order on $\mathsf{List}(\alpha)$ is not wellfounded, but it is for decreasing lists.

$[1 + \gamma]^\beta$ satisfies the specification

Theorem. (dJKNFX) $[1 + \gamma]^\beta$ satisfies the specification for the exponential $(1 + \gamma)^\beta$.

$[1 + \gamma]^\beta$ satisfies the specification

Theorem. (dJKNFX) $[1 + \gamma]^\beta$ satisfies the specification for the exponential $(1 + \gamma)^\beta$.

Proof sketch.

$[1 + \gamma]^\beta$ satisfies the specification

Theorem. (dJKNFX) $[1 + \gamma]^\beta$ satisfies the specification for the exponential $(1+\gamma)^\beta$.

Proof sketch.

- $[1 + \gamma]^0 = \mathsf{List}(\gamma \times 0) = 1$

$[1+\gamma]^\beta$ satisfies the specification

Theorem. (dJKNFX) $[1+\gamma]^\beta$ satisfies the specification for the exponential $(1+\gamma)^\beta$.

Proof sketch.

- $[1+\gamma]^0 = \mathsf{List}(\gamma \times 0) = 1$
- A snd-decreasing list over $\gamma \times (\beta+1)$ either starts with an element $(c, \mathsf{inr}\ \star)$, or it is snd-decreasing over $\gamma \times \beta$. Hence

$$[1+\gamma]^{\beta+1} = [1+\gamma]^\beta \times (1+\gamma)$$

$[1+\gamma]^\beta$ satisfies the specification

Theorem. (dJKNFX) $[1+\gamma]^\beta$ satisfies the specification for the exponential $(1+\gamma)^\beta$.

Proof sketch.

- $[1+\gamma]^0 = \mathsf{List}(\gamma \times 0) = 1$
- A snd-decreasing list over $\gamma \times (\beta + 1)$ either starts with an element $(c, \mathsf{inr}\ \star)$, or it is snd-decreasing over $\gamma \times \beta$. Hence

$$[1+\gamma]^{\beta+1} = [1+\gamma]^\beta \times (1+\gamma)$$

- For $[1+\gamma]^{\sup \gamma_i}$, being decreasing in the second component is crucial.

Can we do better?

David Wärn suggested an alternative definition to us, based on the following lemma:

Lemma. Every ordinal β is the supremum of the successors of its initial segments, i.e.,

$$\beta = \sup_{b:\beta}((\beta \downarrow b) + \mathbf{1})$$

where $\beta \downarrow b :\equiv (\Sigma(x : \beta).x \prec b)$.

Can we do better?

David Wärn suggested an alternative definition to us, based on the following lemma:

Lemma. Every ordinal β is the supremum of the successors of its initial segments, i.e.,

$$\beta = \sup_{b:\beta}((\beta \downarrow b) + \mathbf{1})$$

where $\beta \downarrow b :\equiv (\Sigma(x : \beta).x \prec b)$.

Definition by wishful thinking:

$$\alpha^{\beta} \quad = \quad \alpha^{\sup_{b:\beta}\left((\beta \downarrow b)+\mathbf{1}\right)}$$

Can we do better?

David Wärn suggested an alternative definition to us, based on the following lemma:

Lemma. Every ordinal β is the supremum of the successors of its initial segments, i.e.,

$$\beta = \sup_{b:\beta}((\beta \downarrow b) + \mathbf{1})$$

where $\beta \downarrow b :\equiv (\Sigma(x : \beta).x \prec b)$.

Definition by wishful thinking:

$$\alpha^{\beta} \quad = \quad \alpha^{\sup_{b:\beta}\left((\beta\downarrow b)+\mathbf{1}\right)} \quad \overset{\text{WT}}{=} \quad \sup_{b:\beta} \alpha^{(\beta\downarrow b)+\mathbf{1}}$$

Can we do better?

David Wärn suggested an alternative definition to us, based on the following lemma:

Lemma. Every ordinal β is the supremum of the successors of its initial segments, i.e.,

$$\beta = \sup_{b:\beta}((\beta \downarrow b) + \mathbf{1})$$

where $\beta \downarrow b :\equiv (\Sigma(x:\beta).x \prec b)$.

Definition by wishful thinking:

$$\alpha^{\beta} \quad = \quad \alpha^{\sup_{b:\beta}\left((\beta \downarrow b)+\mathbf{1}\right)} \quad \overset{\text{WT}}{=} \quad \sup_{b:\beta} \alpha^{(\beta \downarrow b)+\mathbf{1}} \quad \overset{\text{WT}}{=} \quad \sup_{b:\beta} \left(\alpha^{\beta \downarrow b} \times \alpha\right)$$

Can we do better?

David Wärn suggested an alternative definition to us, based on the following lemma:

Lemma. Every ordinal β is the supremum of the successors of its initial segments, i.e.,

$$\beta = \sup_{b:\beta}((\beta \downarrow b) + \mathbf{1})$$

where $\beta \downarrow b :\equiv (\Sigma(x : \beta).x \prec b)$.

Definition by wishful thinking (and transfinite induction):

$$\alpha^{\beta} \quad = \quad \alpha^{\sup_{b:\beta}\left((\beta\downarrow b)+\mathbf{1}\right)} \quad \overset{\text{WT}}{=} \quad \sup_{b:\beta} \alpha^{(\beta\downarrow b)+\mathbf{1}} \quad \overset{\text{WT}}{=} \quad \sup_{b:\beta}\left(\alpha^{\beta\downarrow b} \times \alpha\right)$$

Can we do better?

David Wärn suggested an alternative definition to us, based on the following lemma:

Lemma. Every ordinal β is the supremum of the successors of its initial segments, i.e.,

$$\beta = \sup_{b:\beta}((\beta \downarrow b) + \mathbf{1})$$

where $\beta \downarrow b :\equiv (\Sigma(x : \beta).x \prec b)$.

Definition by wishful thinking (and transfinite induction)

$$\alpha^{\beta} \quad = \quad \alpha^{\sup_{b:\beta}((\beta\downarrow b)+\mathbf{1})} \quad \overset{\text{WT}}{=} \quad \sup_{b:\beta} \alpha^{(\beta\downarrow b)+\mathbf{1}} \quad \overset{\text{WT}}{=} \quad \sup_{b:\beta} \left(\alpha^{\beta\downarrow b} \times \alpha\right)$$

but do not forget the base case:

$$\alpha^{\beta} :\equiv \sup_{\mathbf{1}+\beta} \begin{cases} \mathsf{inl}\ \star \mapsto \mathbf{1} \\ \mathsf{inr}\ b \mapsto \alpha^{\beta\downarrow b} \times \alpha \end{cases}$$

Can we do better?

David Wärn suggested an alternative definition to us, based on the following lemma:

Lemma. Every ordinal β is the supremum of the successors of its initial segments, i.e.,

$$\beta = \sup_{b:\beta}((\beta \downarrow b) + \mathbf{1})$$

where $\beta \downarrow b :\equiv (\Sigma(x : \beta).x \prec b)$.

Definition by wishful thinking (and transfinite induction)

$$\alpha^{\beta} \quad = \quad \alpha^{\sup_{b:\beta}((\beta\downarrow b)+\mathbf{1})} \quad \overset{\text{WT}}{=} \quad \sup_{b:\beta} \alpha^{(\beta\downarrow b)+\mathbf{1}} \quad \overset{\text{WT}}{=} \quad \sup_{b:\beta} \left(\alpha^{\beta\downarrow b} \times \alpha\right)$$

but do not forget the base case:

$$\alpha^{\beta} := \sup_{\mathbf{1}+\beta} \begin{cases} \mathsf{inl}\ \star \mapsto \mathbf{1} \\ \mathsf{inr}\ b \mapsto \alpha^{\beta\downarrow b} \times \alpha \end{cases}$$

Theorem. (dJKNFX) α^{β} satisfies the exponentiation specification for $\alpha \geq \mathbf{1}$.

Relating the notions

For α of the form $\alpha = 1 + \gamma$, the two constructions coincide:

Theorem. (dJKNFX) We have $(1+\gamma)^{\beta} = [1+\gamma]^{\beta}$.

Relating the notions

For α of the form $\alpha = 1 + \gamma$, the two constructions coincide:

Theorem. (dJKNFX) We have $(1 + \gamma)^\beta = [1 + \gamma]^\beta$.

Remark. It is straightforward to see that $[1 + \gamma]^\beta$ (defined using decreasing lists) preserves e.g. decidable equality and trichotomy, but not at all so for $(1 + \gamma)^\beta$ (defined using suprema).

Ordinal exponentiation, in general?

Can we define α^β for arbitrary α, constructively?

Ordinal exponentiation, in general?

Can we define α^β for arbitrary α, constructively?

Theorem. (dJKNFX) There is $\mathsf{exp} : \mathsf{Ord} \to \mathsf{Ord} \to \mathsf{Ord}$ satisfying the specification for ordinal exponentiation if and only if Excluded Middle holds.

Ordinal exponentiation, in general?

Can we define α^β for arbitrary α, constructively?

Theorem. (dJKNFX) There is $\mathsf{exp} : \mathsf{Ord} \to \mathsf{Ord} \to \mathsf{Ord}$ satisfying the specification for ordinal exponentiation if and only if Excluded Middle holds.

Proof. ($\Leftarrow$) Use EM to define α^β by cases on β.

Ordinal exponentiation, in general?

Can we define α^β for arbitrary α, constructively?

Theorem. (dJKNFX) There is $\mathsf{exp} : \mathsf{Ord} \to \mathsf{Ord} \to \mathsf{Ord}$ satisfying the specification for ordinal exponentiation if and only if Excluded Middle holds.

Proof. ($\Leftarrow$) Use EM to define α^β by cases on β.
($\Rightarrow$) If such an exp exists, it is continuous, hence it is monotone.

Ordinal exponentiation, in general?

Can we define α^β for arbitrary α, constructively?

Theorem. (dJKNFX) There is $\mathsf{exp} : \mathsf{Ord} \to \mathsf{Ord} \to \mathsf{Ord}$ satisfying the specification for ordinal exponentiation if and only if Excluded Middle holds.

Proof. ($\Leftarrow$) Use EM to define α^β by cases on β.
($\Rightarrow$) If such an exp exists, it is continuous, hence it is monotone.
Let $P : \mathsf{Prop}$ be given.

Ordinal exponentiation, in general?

Can we define α^β for arbitrary α, constructively?

Theorem. (dJKNFX) There is $\mathsf{exp} : \mathsf{Ord} \to \mathsf{Ord} \to \mathsf{Ord}$ satisfying the specification for ordinal exponentiation if and only if Excluded Middle holds.

Proof. ($\Leftarrow$) Use EM to define α^β by cases on β.
($\Rightarrow$) If such an exp exists, it is continuous, hence it is monotone.
Let $P : \mathsf{Prop}$ be given. We have

$$1 = \mathsf{exp}\,(P+1)\,0 \leq \mathsf{exp}\,(P+1)\,1 = P+1$$

Ordinal exponentiation, in general?

Can we define α^β for arbitrary α, constructively?

Theorem. (dJKNFX) There is $\mathsf{exp} : \mathsf{Ord} \to \mathsf{Ord} \to \mathsf{Ord}$ satisfying the specification for ordinal exponentiation if and only if Excluded Middle holds.

Proof. ($\Leftarrow$) Use EM to define α^β by cases on β.
($\Rightarrow$) If such an exp exists, it is continuous, hence it is monotone.
Let $P : \mathsf{Prop}$ be given. We have

$$1 = \mathsf{exp}\,(P + 1)\,0 \leq \mathsf{exp}\,(P + 1)\,1 = P + 1$$

and P or $\neg P$ holds depending on if $\star : 1$ hits $\mathsf{inl}\ p$ or $\mathsf{inr}\ \star$ for $f : 1 \to P + 1$.

Summary

Ordinals are closed under well behaved addition and multiplication.

New: However, a fully general exponentiation operation is possible if and only if Excluded Middle holds.

The best we can do is α^β separately for $\alpha = 0$ and $\alpha \geq 1$.

For $\alpha = 1 + \gamma$, α^β can be defined concretely using decreasing lists, or abstractly using suprema, and the two constructions coincide.

Fully formalised in Agda.
Building on Escardó's TypeTopology.
https://github.com/fredrikNordvallForsberg/TypeTopology/blob/exponentiation/source/Ordinals/Exponentiation/

References

Thierry Coquand, Henri Lombardi and Stefan Neuwirth. "Constructive theory of ordinals". In: *Mathematics for Computation*. Ed. by Marco Benini et al. World Scientific, 2023, pp. 287–318. DOI: 10.1142/12500.

Martín Hötzel Escardó et al. "Ordinals in univalent type theory in Agda notation". Agda development, HTML rendering available at: https://www.cs.bham.ac.uk/~mhe/TypeTopology/Ordinals.index.html. 2018.

Nicolai Kraus, Fredrik Nordvall Forsberg and Chuangjie Xu. "Type-Theoretic Approaches to Ordinals". In: *Theoretical Computer Science* 957 (2023). DOI: 10.1016/j.tcs.2023.113843.

Per Martin-Löf. *Notes on constructive mathematics*. Almqvist & Wiksell, 1970.

Wacław Sierpiński. *Cardinal and Ordinal Numbers*. Vol. 34. Monografie Matematyczne. Państwowe Wydawnictwo Naukowe, 1958.

Paul Taylor. "Intuitionistic Sets and Ordinals". In: *The Journal of Symbolic Logic* 61.3 (1996), pp. 705–744. DOI: 10.2307/2275781.