Ordinals in HOL: Transfinite Arithmetic up to (and beyond) ω_1

Michael Norrish[1] and Brian Huffman[2]

[1] Canberra Research Lab., NICTA*
also, Australian National University
Michael.Norrish@nicta.com.au
[2] Galois, Inc.
huffman@galois.com

Abstract. We describe a comprehensive HOL mechanisation of the theory of ordinal numbers, focusing on the basic arithmetic operations. Mechanised results include the existence of fixpoints such as ε_0, the existence of normal forms, and the validation of algorithms used in the ACL2 theorem-proving system.

1 Introduction

The ordinal numbers are an important foundational type in axiomatic set theory; used there, for example, in the definition of the von Neumann hierarchy and the cardinal numbers. In logic, ordinal numbers also provide an important characterisation of the strength of various logical systems.

Unfortunately, the typed logic implemented in the various HOL systems (including Isabelle/HOL) is not strong enough to define a type for all possible ordinal values (a proper class in a set theory like NBG). It turns out, however, that for any fixed $n \in \mathbb{N}$, we *can* model all ordinals of cardinality $\aleph_n$. The user is thus able to choose an ordinal domain of sufficient size for their purposes.

Our approach is to model ordinals as quotients of wellorders with respect to wellorder isomorphism. This approach has not been mechanised before. Within HOL, any wellorder is some underlying domain (represented as a polymorphic type argument). The resulting ordinals are also parameterised by a type argument, indirectly encoding the limit of the type. For example, the type *num ordinal* captures only the countable ordinals.

One important use of ordinal numbers occurs in the ACL2 theorem-proving system, which uses ordinal numbers as part of its termination reasoning for recursive definitions. Recently, Manolios and Vroon [6] improved ACL2's representation of ordinal numbers, and implemented new, more efficient algorithms

* NICTA is funded by the Australian Government as represented by the Department of Broadband, Communications and the Digital Economy and the Australian Research Council through the ICT Centre of Excellence program. The first author also thanks Thomas Forster for productive early discussions. Finally, we thank ITP's anonymous reviewers for helpful comments.

for manipulating those numbers. Their work mechanised proofs of the correspondence between the old and new notational systems, and also proved the expected arithmetic properties. However, ACL2 has no notation-independent theory of the ordinals available to it, and so no way to model the set-theoretic ordinals. In *this* paper, we provide a sufficiently rich model, and are thus able to validate Manolios and Vroon's algorithms.

Contribution This work makes a particular contribution in

- its definition of ordinal supremum,
- the fact that the mechanised notion of ordinal is polymorphic in an underlying universe type (allowing ordinals of large cardinality), and
- its mechanised validation of the ACL2 algorithms for ordinal arithmetic

HOL4 Notation and Theorems All statements appearing with a turnstile ($\vdash$) are HOL4 theorems, automatically pretty-printed to LaTeX. Notation specific to this paper is explained as it is introduced. Otherwise, HOL4's syntax is a generally pleasant combination of quantifiers ($\forall$, $\exists$) and functional programming.

The option type α *option*, often used to encode partial functions, includes values NONE, and SOME x for all possible values x of type α. Hilbert choice is available through the epsilon notation. Read $\varepsilon x.\, P\, x$ as "the x that satisfies (predicate) P".

Sets and characteristic functions (of type $\alpha \to$ *bool* for element type α) are identified. Sets support standard operations such as union ($\cup$), and element removal (s DELETE e). The term BIGUNION s denotes the union of a set of sets. We write f ' s for the image of the set s under function f. BIJ $f\ s_1\ s_2$ means that function f is a bijection between sets s_1 and s_2. The universal set over type α is written $\mathcal{U}(:\alpha)$. Cardinality reasoning is expressed with $s \preccurlyeq t$ ("there is an injection from s to t"), and $s \approx t$ ("there is a bijection between s and t").

2 Wellorders

Definition 1. *We define what it is for a relation R to be a wellorder:*

$$\begin{aligned}&\mathsf{wellorder}\ R \iff \\ &\quad \mathsf{wellfounded}\,(\mathsf{strict}\ R)\ \wedge \\ &\quad \mathsf{linear\_order}\ R\,(\mathsf{domain}\ R\ \cup\ \mathsf{range}\ R)\ \wedge \\ &\quad \mathsf{reflexive}\ R\,(\mathsf{domain}\ R\ \cup\ \mathsf{range}\ R)\end{aligned}$$

As there is at least one value satisfying this definition (the empty set will do), we use HOL's standard type definition mechanism to define a new type (family) α *wellorder* that captures all of the possible wellorders over values drawn from arbitrary types α. The critical relations over wellorders are order-isomorphism and the relation that orders them linearly. The first is straightforward.

Definition 2. *Two wellorders are isomorphic if there is a bijective function (conjuncts two and three below) between their respective fields (conjunct one) that preserves the ordering (conjunct four):*

$$
\begin{array}{l}
w_1 \approx_w w_2 \iff \\
\quad \exists f. \\
\quad\quad (\forall x.\ x \in \mathsf{fld}\ w_1 \Rightarrow f\ x \in \mathsf{fld}\ w_2) \wedge \\
\quad\quad (\forall x_1\ x_2. \\
\quad\quad\quad x_1 \in \mathsf{fld}\ w_1 \wedge x_2 \in \mathsf{fld}\ w_1 \Rightarrow \\
\quad\quad\quad\quad (f\ x_1 = f\ x_2 \iff x_1 = x_2)) \wedge \\
\quad\quad (\forall y.\ y \in \mathsf{fld}\ w_2 \Rightarrow \exists x.\ x \in \mathsf{fld}\ w_1 \wedge f\ x = y) \wedge \\
\quad\quad \forall x\ y.\ (x, y) \in {w_1}^{\neq} \Rightarrow (f\ x, f\ y) \in {w_2}^{\neq}
\end{array}
$$

(We are using syntax overloading to simplify notation: the formula $(x, y) \in {w_1}^{\neq}$ *means that the pair* (x, y) *is a strict inequality in the relation (a set of pairs) that represents the wellorder value* w_1*. Alternatively, read* $(x, y) \in {w_1}^{\neq}$ *as "*x *is strictly less than* y *in* w_1*". Read* $\mathsf{fld}\ w$ *as the union of the domain and range of the relation representing* w*.)*

The definition of the ordering relation on wellorders depends on the wobound function, which truncates a wellorder so that it includes only those elements below a particular point. There are two important theorems about wobound:

$$
\begin{array}{l}
\vdash\ (x, y) \in (\mathsf{wobound}\ z\ w)^{\neq} \iff \\
\qquad (x, z) \in w^{\neq} \wedge (y, z) \in w^{\neq} \wedge (x, y) \in w^{\neq} \\
\vdash\ (x, y) \in w^{\neq} \Rightarrow \mathsf{wobound}\ x\ (\mathsf{wobound}\ y\ w) = \mathsf{wobound}\ x\ w
\end{array}
$$

Definition 3. *The ordering relation for wellorders (written* $w_1 \prec_w w_2$*) can then be defined*

$$w_1 \prec_w w_2 \iff \exists x.\ x \in \mathsf{fld}\ w_2 \wedge w_1 \approx_w \mathsf{wobound}\ x\ w_2$$

Transitivity of $\prec_w$ follows from the transitivity of order-isomorphism and the second result about wobound above. Well-foundedness for $\prec_w$ follows easily from the well-foundedness of the underlying relation. Well-foundedness is also the basis for the proof that $\prec_w$ is irreflexive. Finally, we show that $\prec_w$ is trichotomous:

Theorem 1.

$$\vdash\ w_1 \prec_w w_2\ \vee\ w_1 \approx_w w_2\ \vee\ w_2 \prec_w w_1$$

The proof of this result is the most involved of this section.

Proof. Let w_1 and w_2 be wellorders over α and β respectively. We define f of type $\alpha \to \beta$ *option* by well-founded recursion. The value of $f\ x$ is $\mathsf{SOME}\ y$ when y is the least element in w_2 not in the image of f applied to all elements less than x. If there is no such y, then $f\ x = \mathsf{NONE}$. If there is an x such that $f\ x = \mathsf{NONE}$, then w_2 is less than w_1, and the least value x where $f\ x = \mathsf{NONE}$ is the bound needed to demonstrate this. If f never has value NONE, then w_2 is at least as big as w_1. If the image of f on the elements of w_1 is all the elements of w_2, then f is the bijection we need to demonstrate order-isomorphism of w_1 and w_2. Otherwise, there is an element of w_2 not in the image of f. Take the least such element to be the bound demonstrating $w_1 \prec_w w_2$. □

3 Constructing the Ordinals

With $\approx_w$ an equivalence relation, we can quotient all possible wellorders over the type α, giving us a natural type of ordinals over α. However, if α is a finite type, then there are only finitely many ordinals over this type. Clearly, all the interesting ordinals are those over infinite types, and so our approach is to make the new type α *ordinal* a quotient over the wellorders over the sum type $\alpha + num$. Henceforth, this type is abbreviated as α *inf*.

This construction means that the distinct types *unit ordinal*, *bool ordinal* and *num ordinal* will all be isomorphic (they will all be copies of the countable ordinals). On the other hand, the type $(num \to bool)$ *ordinal* is large enough to include the first uncountable ordinal, ω_1.

When we quotient, and create the new type α *ordinal*, the $(\prec_w)$ relation lifts to the new type, defining $(<)$. This relation inherits the irreflexivity, transitivity, well-foundedness and trichotomy results of $(\prec_w)$. Using these, it is trivial to show that the ordinals themselves form a well-order.

Definition 4. *Well-foundedness also allows the definition of a "least" operator for ordinals:*

$$\begin{aligned}&(\mathsf{oleast})\ (P : \alpha\ ordinal \to bool) = \\ &\quad \varepsilon(x : \alpha\ ordinal).\ P\ x\ \wedge\ \forall(y : \alpha\ ordinal).\ y < x\ \Rightarrow\ \neg P\ y\end{aligned}$$

This is well-defined as long as the predicate (or set) P is not everywhere false (the empty set).

Syntactically, we make (oleast) a binder, allowing us to write terms such as $(\mathsf{oleast}\, x.\, y < x)$ (the definition of the successor of y, written y^+), and $(\mathsf{oleast}\, x.\, \mathsf{T})$ (the zero-ordinal).

This copy of the natural numbers is a good starting point. It is straightforward to inject HOL's natural numbers with a new constant: $\mathsf{\&} : num \to \alpha\ ordinal$, which is also the basis for ordinal numerals (0, 1, 2 *etc*).

Definition 5. *Write* $\mathsf{preds}\, \alpha$ *to denote the set of all predecessors of an ordinal.*

Definition 6. *Define the notion of a set being downward closed:*

$$\vdash \mathsf{downward\_closed}\, s \iff \forall a\, b.\, a \in s \wedge b < a \Rightarrow b \in s$$

Von Neumann famously characterised the ordinal numbers as those sets equal to their own predecessors. HOL's type system doesn't allow this: instead we must replace "equal" with the existence of a bijection:

Theorem 2. *The* preds *function forms a bijection between all possible ordinals and all but one of the downward closed sets of ordinals. The one omission is the universal set.*

$$\vdash \mathsf{BIJ}\ \mathsf{preds}\ \mathcal{U}(:\alpha\ ordinal)\ (\mathsf{downward\_closed}\ \mathsf{DELETE}\ \mathcal{U}(:\alpha\ ordinal))$$

3.1 Cardinality Arguments and Supremum

We want a constant $(\mathsf{sup} : (\alpha\, ordinal \to bool) \to \alpha\, ordinal)$, that takes a set of ordinals as an argument and returns their supremum. In our setting, this function can't be well-defined on all possible arguments: when passed the universal set of all α-ordinals, there is no possible value to return. Nonetheless, we can characterise those situations when $\mathsf{sup}\, s$ does have a reasonable value. First, the definition:

Definition 7. *The supremum of a set is the least element not in the set's collective predecessors.*

$$\mathsf{sup}\ oset = \mathsf{oleast}\, \alpha.\, \alpha \notin \mathsf{BIGUNION}\, (\mathsf{preds}\ `\ oset)$$

To characterise the reasonable arguments to sup, we need a definition and two further theorems.

Definition 8. *Let* allOrds *be the wellorder of all the* α*-ordinals (ordered by* $(<)$*).*

$$(\mathsf{allOrds} : \alpha\, ordinal\, wellorder) = \mathsf{mkWO}\, \{(x, y) \mid x = y \vee x < y\}$$

(The constant mkWO *lifts a relation into the type* α *wellorder. It is necessary to separately show that the relation satisfies the* wellorder *predicate from Definition 1.)*

Theorem 3. *Any wellorder w over the type α inf is order-isomorphic to the segment of* allOrds *below the element of α ordinal to which the quotienting (*mkOrdinal*) maps w.*

$$\begin{aligned} \vdash\ & (w : \alpha\ \textit{inf wellorder}) \approx_w \\ & \mathsf{wobound}\ (\mathsf{mkOrdinal}\ w)\ (\mathsf{allOrds} : \alpha\ \textit{ordinal wellorder}) \end{aligned}$$

Note how w is a wellorder over α inf, but that the right-hand side of the isomorphism is a wellorder over all possible ordinals *over α inf.*

Proof. By contradiction. Then, by well-foundedness, there is a least w where the isomorphism doesn't hold. If the two wellorders are not order-isomorphic, one is smaller than the other, by trichotomy of $(\prec_w)$. If w is smaller, there is a bound b (an ordinal) in allOrds, smaller still than mkOrdinal w, such that

$$w \approx_w \mathsf{wobound}\ b\ \mathsf{allOrds}$$

There is a wellorder bw that is a member of b's equivalence class. As $(\prec_w)$ is reflected by $(<)$, we have $bw \prec_w w$. Because w was least, bw must be order-isomorphic to wobound b allOrds. So, bw and w are order-isomorphic to the same ordinal (wobound b allOrds), but $bw \prec_w w$, contradicting the irreflexivity of $(\prec_w)$. The other direction (when w is larger) is similar. □

This result means that the predecessors of any given α *ordinal* must be equinumerous to a wellorder over α *inf*.

Corollary 1. *The predecessors of any ordinal have cardinality no greater than that of (all of) the underlying set, α inf.*

$$\vdash\ \mathsf{preds}\ a \preccurlyeq \mathcal{U}(:\alpha\ \textit{inf})$$

Theorem 4. *The cardinality of all of the type α ordinal is strictly greater than that of the type α inf.*

$$\vdash\ \mathcal{U}(:\alpha\ \textit{inf}) \prec \mathcal{U}(:\alpha\ \textit{ordinal})$$

Proof. By contradiction. If $\mathcal{U}(:\alpha\ \textit{ordinal}) \preccurlyeq \mathcal{U}(:\alpha\ \textit{inf})$, then the injection from left-to-right copies the wellorder allOrds into a wellorder wo of type α *inf wellorder*. This gives allOrds $\approx_w wo$. By Theorem 3, this wo is also order-isomorphic to wobound (mkOrdinal wo) allOrds. Transitivity of $(\approx_w)$ then gives us that allOrds is less than itself, which is impossible. □

These results then combine to give us the important characterising theorem about sup:

Theorem 5. *As long as the cardinality of the set s is not greater than that of $\mathcal{U}(:\alpha\ \mathit{inf})$, an arbitrary ordinal α is less than that set's supremum iff there is an element of s that is bigger than α.*

$$\begin{aligned}\vdash\ \ & s \preccurlyeq \mathcal{U}(:\alpha\ \mathit{inf}) \Rightarrow \\ & \forall\alpha.\, \alpha < \mathsf{sup}\ s \iff \exists\beta.\, \beta \in s \wedge \alpha < \beta\end{aligned}$$

Proof. sup takes the union of all the predecessors of all the elements of s (Definition 7). Let κ be the cardinality of $\mathcal{U}(:\alpha\ \mathit{inf})$. By Corollary 1 above, the predecessors of each element of set s have that cardinality. If s has no more than the same cardinality, then from the fact that $\kappa \times \kappa \approx \kappa$ and Theorem 3 above, the union calculated in the definition of sup cannot be the universal set of all possible ordinals. There must then be a least ordinal not within that union, and so sup s will be well-defined.

Moreover, the set of all the combined predecessors (call it ps) is also downward closed, and so, by Theorem 2, there must be an ordinal α whose predecessors are exactly ps. So, $\mathsf{sup}\ s = \alpha$, and it is easy to show that the theorem's characterisation of its predecessors is correct. □

An easy corollary is that there is no maximal ordinal. For any ordinal α, we observe that $s = \mathsf{preds}\ \alpha \cup \{\alpha\}$ is downward closed and not equal to $\mathcal{U}(:\alpha\ \mathit{ordinal})$. Then, by Theorem 2 there must be a $\beta > \alpha$, with $s = \mathsf{preds}\ \beta$.

3.2 Limit ordinals

Definition 9. *With* sup *defined, it is possible to define ω. This, the first limit ordinal, is the supremum of the copy of the natural numbers that injects into the ordinals* via (&).

$$(\omega : \alpha\ \mathit{ordinal}) = \mathsf{sup}\ \{((\&i) :\alpha\ \mathit{ordinal}) \mid \mathsf{T}\}$$

Definition 10. *We also define a constant* omax*, which returns the maximal element of a set of ordinals, if any. The option type is used to encode the partiality of this function, so the type of* omax *is $(\alpha\ \mathit{ordinal} \to \mathit{bool}) \to \alpha\ \mathit{ordinal}\ \mathit{option}$. If* omax (preds a) *is* NONE*, we abbreviate this condition as* islimit a.

Theorem 6. *One simple consequence of these definitions is that every natural number is less than ω, and that only the natural numbers are less than ω:*

$$\vdash\ (a : \alpha\ \mathit{ordinal}) < (\omega : \alpha\ \mathit{ordinal}) \iff \exists(n : \mathit{num}).\ a = ((\&n) :\alpha\ \mathit{ordinal})$$

4 Arithmetic

Theorem 7. *With access to a total well-founded relation* $(<)$*, we have always been able to define functions by well-founded recursion. However, we can now recast this in a more palatable form, one that makes the ordinals look a little like an algebraic type generated by constructors* 0*,* x^+ *and* $\mathsf{sup}\, s$ *(with* s *not including its own upper bound):*

$$\begin{array}{l}\vdash\ \forall(z:\beta)\,(sf:\alpha\,\mathit{ordinal}\to\beta\to\beta)\,(lf:\alpha\,\mathit{ordinal}\to(\beta\to\mathit{bool})\to\beta).\\ \quad\exists(h:\alpha\,\mathit{ordinal}\to\beta).\\ \quad\ h\,(0:\alpha\,\mathit{ordinal})=z\ \wedge\ (\forall(a:\alpha\,\mathit{ordinal}).\,h\,a^+=sf\ a\,(h\ a))\ \wedge\\ \quad\ \forall(a:\alpha\,\mathit{ordinal}).\\ \quad\quad(0:\alpha\,\mathit{ordinal})<a\ \wedge\ \mathsf{islimit}\ a\ \Rightarrow\ h\,a=lf\ a\,((h\ \text{`}\,(\mathsf{preds}\ a)):\beta\to\mathit{bool})\end{array}$$

This recursion theorem allows the user to specify three cases: z, a value in the desired range (β) for zero; sf, a function for constructing a result when h is passed a successor; and lf when the argument to h is a limit ordinal. The lf function is given the original limit ordinal a as well as the set of all the values given by recursive calls of h on a's predecessors.

The recursion theorem is all we need to define ordinal addition, multiplication and exponentiation. Working out the details for addition $(a+b)$: we will recurse on b, and let z be the value a, sf be $(\lambda x\ r.\ r^+)$, and lf be $(\lambda x\ rs.\ \mathsf{sup}\ rs)$. This gives

Definition 11. *Ordinal addition:*

$$\begin{array}{l}a+0=a\\ a+b^+=(a+b)^+\\ 0<b\ \wedge\ \mathsf{islimit}\ b\ \Rightarrow\ a+b=\mathsf{sup}\,((+)\ a\ \text{`}\,(\mathsf{preds}\ b))\end{array}$$

The definitions of multiplication and exponentiation are as straightforward. For example:

Definition 12. *Ordinal exponentiation:*

$$\begin{array}{l}a^0=1\\ a^{b^+}=a^b\cdot a\\ 0<b\ \wedge\ \mathsf{islimit}\ b\ \Rightarrow\ a^b=\mathsf{sup}\,((^{**})\ a\ \text{`}\,(\mathsf{preds}\ b))\end{array}$$

$((^{**})\ a)$ is equivalent to $(\lambda b.\ a^b)$; the pretty-printing obscures this because the underlying constant prints as $(^{**})$ when it doesn't have two arguments.

Reasoning about these operations is made easier by the observation that all three are *continuous* (in their second arguments). For addition, the continuity result is

$$\vdash\ s \preccurlyeq \mathcal{U}(:\alpha\ \mathit{inf})\ \wedge\ s \neq \emptyset\ \Rightarrow\ a + \mathsf{sup}\ s = \mathsf{sup}\ ((+)\ a\ `\ s)$$

Rewriting with these theorems allows operators such as $(+)$ to move under sup arguments, where further simplification is usually possible. For example, the proofs (by induction) that addition and multiplication are associative are greatly simplified by their continuity theorems.

4.1 Division and Modulus

The various arithmetic operations on ordinal numbers do not satisfy many of the typical properties of number systems. For example, addition and multiplication are not commutative. However, they both enjoy cancellation properties for common arguments on the left:

$$\vdash\ \alpha + \beta = \alpha + \gamma\ \Longleftrightarrow\ \beta = \gamma$$
$$\vdash\ \alpha \cdot \beta = \alpha \cdot \gamma\ \Longleftrightarrow\ \alpha = 0\ \vee\ \beta = \gamma$$

These then lead to the existence of unique quotients and remainders.

Theorem 8.

$$\vdash\ 0 < b\ \Rightarrow\ a = b \cdot (a\ /\ b) + a \bmod b\ \wedge\ a \bmod b < b$$
$$\vdash\ 0 < b\ \wedge\ a = b \cdot q + r\ \wedge\ r < b\ \Rightarrow\ q = a\ /\ b\ \wedge\ r = a \bmod b$$

Proof. The existence of the division and modulus constants is shown by taking the quotient d to be $\mathsf{sup}\,\{c \mid b \cdot c \leq a\}$. (The supremum is well-defined because the set is bounded above.) Then $b \cdot d \leq a$ follows from the continuity of multiplication. The existence of the remainder follows from an earlier result that $\vdash\ a \leq b \Longleftrightarrow \exists c.\ b = a + c$.

The uniqueness result proceeds by first showing the uniqueness of the quotient (uniqueness of the modulus then follows from additive cancellation). If there is another quotient q' not equal to $a\ /\ b$ (write q), then it is either larger or smaller. If larger, then $q' = q + \delta$, for some non-zero δ, and $a = b(q + \delta) + r'$, where r' is the remainder accompanying q'. Then $a = bq + b\delta + r$, and cancellation and associativity then give us that $b\delta + r = a \bmod b$. But $0 < \delta$, making $a \bmod b$ too large. The other case is similar. □

4.2 Cantor Normal Forms

In a discrete domain such as the ordinals, division approximates multiplication's inverse, leaving a remainder. Analogously, with exponentiation we can construct a discrete logarithm. If working with base b, and e is the largest value such that b^e is under the target a, then we can "drop down" to the level of multiplication and find how many whole copies of b^e fit into a, giving us a c such that $b^e \cdot c \leq a$. Then we can repeat the process with the remainder.

Done over the natural numbers with $b = 10$, we derive a's decimal representation (strictly, the non-zero coefficients along with their indices). Over all ordinals, with $b = \omega$, we derive the *Cantor Normal Form* of a.

Definition 13. *The sequence of exponents and coefficients we derive in the above construction is the same as the information needed to specify a polynomial over a single variable. We define* eval_poly *to evaluate such sequences with respect to arbitrary bases:*

$$\begin{aligned}&\mathsf{eval\_poly}\ b\ [\,] = 0\\ &\mathsf{eval\_poly}\ b\ ((c, e) :: t) = b^e \cdot c + \mathsf{eval\_poly}\ b\ t\end{aligned}$$

Definition 14. *We define* is_polyform *to capture well-formed "polynomial" sequences, requiring that the exponents are decreasing, and that the coefficients are always strictly between* 0 *and* b*:*

$$\begin{aligned}&\mathsf{is\_polyform}\ b\ [\,] \iff \mathsf{T}\\ &\mathsf{is\_polyform}\ b\ [(c, e)] \iff 0 < c \ \wedge\ c < b\\ &\mathsf{is\_polyform}\ b\ ((c_1, e_1) :: (c_2, e_2) :: t) \iff\\ &\quad 0 < c_1 \ \wedge\ c_1 < b \ \wedge\ e_2 < e_1 \ \wedge\ \mathsf{is\_polyform}\ b\ ((c_2, e_2) :: t)\end{aligned}$$

Then, just as with division, we are able to prove that "polynomial forms" always exist, and that they are unique.

Theorem 9. *For all ordinals* a*, and bases* b *greater than* 1*, it is possible to express* a *as the sum of a sequence of pairs of coefficients and powers-of-*b*. In the sequence each successive exponent is smaller than its predecessors.*

$$\vdash\ 1 < b\ \Rightarrow\ \exists ces.\ \mathsf{is\_polyform}\ b\ ces\ \wedge\ a = \mathsf{eval\_poly}\ b\ ces$$

Define the new constant polyform *to return such a sequence when given parameters* b *and* a *(if* $b < 2$*, allow that the function has no definite value). We show that all possible sequences with the desired property have* polyform*'s value:*

$$\begin{aligned}\vdash\ & 1 < b \ \wedge\ \mathsf{is\_polyform}\ b\ ces\ \wedge\ a = \mathsf{eval\_poly}\ b\ ces\ \Rightarrow\\ & \mathsf{polyform}\ b\ a = ces\end{aligned}$$

Proof. Both proofs are by induction on the argument a. The first proof is similar to the proof of the existence of a quotient: the leading exponent is taken to be $\mathsf{sup}\,\{e \mid b^e \leq a\}$. After the coefficient c is calculated by division, and $b^e \cdot c$ subtracted out, the remaining ordinal is smaller and the inductive hypothesis applies. The uniqueness proof hinges on the following important lemma:

$$\vdash\ 1 < b \ \wedge\ \mathsf{is\_polyform}\ b\ ((c, e) :: t)\ \Rightarrow\ \mathsf{eval\_poly}\ b\ t < b^e$$

4.3 Fixpoints and ε_0

A function $(f : \alpha\ \mathit{ordinal} \to \alpha\ \mathit{ordinal})$ can be iterated any number of times from a starting value x. The resulting set $\{x, f(x), f(f(x)), \ldots, f^n(x), \ldots\}$ is clearly only countably infinite, and so will always have a supremum. Under certain conditions, that supremum will also be a fixpoint for f.

Theorem 10. *If f is non-decreasing and continuous, then it has a fixpoint. In fact, for* any *lower bound a, the function f has a fixpoint at least as large as a.*

$$\begin{aligned}\vdash\ & (\forall s.\ s \neq \emptyset \wedge s \preccurlyeq \mathcal{U}(:\alpha\ \mathit{inf}) \Rightarrow f\,(\mathsf{sup}\ s) = \mathsf{sup}\,(f\ `\ s)) \wedge \\ & (\forall x.\ x \leq f\,x) \Rightarrow \\ & \quad \forall a.\ \exists b.\ a \leq b \wedge f\,b = b\end{aligned}$$

Proof. Let s be the set above (all the f-iterates of a). Take the fixpoint to be the supremum of s. We have that $f\,(\mathsf{sup}\ s) = \mathsf{sup}\,(f\ `\ s)$, and are required to show that $\mathsf{sup}\,(f\ `\ s) = \mathsf{sup}\ s$. This follows straightforwardly because f is non-decreasing. □

Our arithmetic operations (addition, multiplication and exponentiation) are all continuous in their right arguments and non-decreasing. So, for example, the first fixpoint of $((\cdot)\,2)$ is 0; the next is ω, and the third is $\omega \cdot 2$. The first non-zero fixpoint of $((\cdot)\,\omega)$ is ω^ω. However, it turns out that the first fixpoint of $((^{**})\,\omega)$ is not expressible with any of the notation we have developed thus far.

Definition 15. *Let ε_0 be the least fixpoint of $((^{**})\,\omega)$:*

$$\varepsilon_0 = \mathsf{oleast}\ x.\ \omega^x = x$$

This is well-defined because of Theorem 10, giving us the following characterisations of ε_0:

$$\vdash\ \omega^{\varepsilon_0} = \varepsilon_0$$

$$\vdash\ a < \varepsilon_0 \ \Rightarrow\ a < \omega^a \ \wedge\ \omega^a < \varepsilon_0$$

Theorem 11. *As suggested, the arithmetic operations are all closed under ε_0:*

$$\vdash\ a < \varepsilon_0 \ \wedge\ b < \varepsilon_0 \ \Rightarrow\ a + b < \varepsilon_0 \qquad \vdash\ a < \varepsilon_0 \ \wedge\ b < \varepsilon_0 \ \Rightarrow\ a \cdot b < \varepsilon_0$$

$$\vdash\ a < \varepsilon_0 \ \wedge\ b < \varepsilon_0 \ \Rightarrow\ a^b < \varepsilon_0$$

5 Uncountable Ordinals

Definition 16. *The "countable ordinals" are those with countably many predecessors. Write* countableOrd a *for an* a *with this property.*

An immediate consequence of Theorem 4 is that there are uncountably many countable ordinals. To guarantee even larger ordinals, we must instantiate the α type-parameter with known-to-be-larger types:

Definition 17. *The* α *ucinf type has at least the cardinality of* $2^{\aleph_0}$*, and is thus at least as big as* $\aleph_1$*. The* α *ucord type contains ordinals that are quotients of wellorders over* α *ucinf:*

$$\alpha \textit{ ucinf} = (\alpha + (\textit{num} \to \textit{bool}))\ \textit{inf}$$
$$\alpha \textit{ ucord} = (\alpha + (\textit{num} \to \textit{bool}))\ \textit{ordinal}$$

Note that these abbreviations mean that every α *ucord is also an ordinal. Every theorem about values of type* α *ordinal applies to values of type* α *ucord.*

Lemma 1. *The countable ordinals are not larger than the universe of* α *ucinf (which contains* $\mathcal{U}(:\textit{num} \to \textit{bool})$ *as a subset).*

$$\vdash\ \{a \mid \mathsf{countableOrd}\ a\} \preccurlyeq \mathcal{U}(:\alpha\ \textit{ucinf})$$

Proof. By contradiction. Then $\mathcal{U}(:\alpha\ \textit{ucinf})$ injects into the countable ordinals *via* some f, but there is no bijection between the two. Let $a = \mathsf{sup}\ (f\ `\mathcal{U}(:\alpha\ \textit{ucinf}))$. (The supremum is well-defined because the image cannot have greater cardinality than $\mathcal{U}(:\alpha\ \textit{ucinf})$.) We now consider whether or not a is a countable ordinal.

If so, then we show that there is an injection from $\mathcal{U}(:\alpha\ \textit{ucinf})$ into the (countable) predecessors of a, which gives an immediate contradiction. If the image of f doesn't includes the supremum, the injection is f itself. If there is a u such that $f\ u = a$, then f is an injection from $\mathcal{U}(:\alpha\ \textit{ucinf})$ $\mathsf{DELETE}\ u$ into the predecessors, and deleting a single element from an infinite set doesn't change its cardinality, so the contradiction can still be obtained.

If a is not a countable ordinal, then all of the countable ordinals must be among its predecessors. So, $\{b \mid \mathsf{countableOrd}\ b\} \preccurlyeq \mathsf{preds}\ a$. But we also have that $\mathsf{preds}\ a \preccurlyeq \mathcal{U}(:\alpha\ \textit{ucinf})$, giving a contradiction by the transitivity of $(\preccurlyeq)$. □

Definition 18.

$$(\omega_1 : \alpha\ \textit{ucord}) = \mathsf{sup}\ \{a \mid \mathsf{countableOrd}\ a\}$$

The supremum is well-defined because of Lemma 1 above.

Theorem 12. *The ordinal* ω_1 *is the first uncountable ordinal:*

$$\vdash\ x < \omega_1 \iff \mathsf{countableOrd}\ x$$

(The irreflexivity of $(<)$ *means that* ω_1 *cannot itself be countable.)*

6 Validating Algorithms on ACL2's Ordinals

The ACL2 system models ordinals up to ε_0 with a representation based on Cantor Normal Form. ACL2's manipulations of those values are defined by recursive functions over that syntax. ACL2 then takes as axiomatic that these recursive functions are correct; that, for example, its less-than relation on these values really does correspond to $(<)$.

In isolation, these axiomatic assertions can only be checked manually. However, thanks to work started by Gordon *et al.* [2], much of the ACL2 axiomatic system has been embedded in HOL4. More recently, the "ACL2 in HOL" project was completed by Kaufmann and Slind [5], who showed that ACL2's less-than relation is well-founded, justifying ACL2's recursion and induction principles. Kaufmann and Slind note in passing:

> *... we are not ascribing any semantics at all to the notation; a separate proof would be needed to show that indeed the following definitions do correspond to the ordinals up to* ε_0.

A little earlier, Manolios and Vroon [6] improved ACL's representation of the ordinals-up-to-ε_0, and developed efficient arithmetic algorithms for that representation. They noted:

> *Note that these proofs are not mechanically verified. To do so would require using a theorem prover that can reason both about ACL2 and set theory.*

HOL4 can reason about ACL2, thanks to the embedding above, and can now also reason about ordinals in a way that captures their nature as canonical wellorders. Thus we are now in a position to do the mechanised proofs that could not be done in [5, 6].

Kaufmann and Slind's HOL4 theory file defines the ACL2 ordinals to be

$$\mathit{osyntax} = \mathsf{End}\ \texttt{of}\ \mathit{num} \mid \mathsf{Plus}\ \texttt{of}\ \mathit{osyntax} \Rightarrow \mathit{num} \Rightarrow \mathit{osyntax}$$

That is, *osyntax* is an algebraic type with two constructors: End takes a natural number argument, and Plus takes a number and two *osyntax* values as arguments.

Definition 19. *The osyntax type can be given a semantics in* α *ordinal:*

$$[\![\mathsf{End}\ n]\!] = \&n$$
$$[\![\mathsf{Plus}\ e\ c\ t]\!] = \omega^{[\![e]\!]} \cdot \&c + [\![t]\!]$$

Kaufmann and Slind define functions oless and is_ord, with the following equations for the interesting cases:

$$\begin{array}{l}\mathsf{oless}\,(\mathsf{Plus}\;e_1\;k_1\;t_1)\,(\mathsf{Plus}\;e_2\;k_2\;t_2)\iff\\ \quad \mathtt{if}\;\mathsf{oless}\;e_1\;e_2\;\mathtt{then}\;\mathsf{T}\\ \quad \mathtt{else\,if}\;e_1=e_2\;\wedge\;k_1<k_2\;\mathtt{then}\;\mathsf{T}\\ \quad \mathtt{else\,if}\;e_1=e_2\;\wedge\;k_1=k_2\;\wedge\;\mathsf{oless}\;t_1\;t_2\;\mathtt{then}\;\mathsf{T}\\ \quad \mathtt{else}\;\mathsf{F}\\ \mathsf{is\_ord}\,(\mathsf{Plus}\;e\;k\;t)\iff\\ \quad \mathsf{is\_ord}\;e\;\wedge\;e\neq\mathsf{End}\,0\;\wedge\;0<k\;\wedge\;\mathsf{is\_ord}\;t\;\wedge\\ \quad \mathsf{oless}\,(\mathsf{expt}\;t)\;e\end{array}$$

The is_ord function is the analogue of is_polyform from Definition 14, capturing whether or not the notation is well-formed (non-zero coefficients and decreasing exponents). (The expt function returns e when applied to Plus $e\;c\;t$, and End 0 otherwise.)

Theorem 13. *The* oless *function is correct on well-formed osyntax values:*

$$\vdash\ \mathsf{is\_ord}\;x\;\wedge\;\mathsf{is\_ord}\;y\;\Rightarrow\;(\mathsf{oless}\;x\;y\iff[\![x]\!]<[\![y]\!])$$

And, ultimately:

Theorem 14. *The model function ($[\![\_]\!]$) is a bijection from well-formed osyntax values into the ordinals less than ε_0.*

$$\vdash\ \mathsf{BIJ}\;(\lambda x.\;[\![x]\!])\;\{x\mid\mathsf{is\_ord}\;x\}\;\{a\mid a<\varepsilon_0\}$$

6.1 Arithmetic

The ACL2 definitions of addition and multiplication over *osyntax* are correct:
Theorem 15.

$$\vdash\ \mathsf{is\_ord}\;x\;\wedge\;\mathsf{is\_ord}\;y\;\Rightarrow\;[\![\mathsf{ord\_add}\;x\;y]\!]=[\![x]\!]+[\![y]\!]$$

$$\vdash\ \mathsf{is\_ord}\;x\;\wedge\;\mathsf{is\_ord}\;y\;\Rightarrow\;[\![\mathsf{ord\_mult}\;x\;y]\!]=[\![x]\!]\cdot[\![y]\!]$$

Manolios and Vroon [6] note that ord_mult is very inefficient, and prove a version with better complexity, based on new constants pmult, c1 and c2. In order to embed it in ACL2, Manolios and Vroon have already mechanically proved pmult equivalent to ord_mult. Nonetheless, we also proved a version of their Theorem 10:

Theorem 16 (after Manolios and Vroon). *The efficient* pmult *algorithm correctly calculates ordinal multiplication. (The natural number parameter n can be set to zero initially.)*

$$\vdash\ \mathsf{is\_ord}\;a\;\wedge\;\mathsf{is\_ord}\;b\;\wedge\;n\;\leq\;\mathsf{c1}\,(\mathsf{expt}\;a)\,(\mathsf{expt}\;b)\;\Rightarrow\;[\![\mathsf{pmult}\;a\;b\;n]\!]=[\![a]\!]\cdot[\![b]\!]$$

7 Another Model

Sections 2 and 3 showed how to construct a type $\alpha\,\mathit{ordinal}$ using wellorders. In this section, we describe an alternative, earlier construction of ordinals that starts with the infinitely-branching tree datatype shown below.[1] The goal is to construct a wellordered type *ordinal* that has upper bounds for all countable sets; from this foundation, an Isabelle formalization by the second author [4] develops ordinal arithmetic as described in Section 4.

$$\mathit{preordinal} \;=\; \mathsf{Zero} \mid \mathsf{StrictLim}(\mathit{num} \to \mathit{preordinal})$$

We define the subterm relation $\lhd$ as the least transitive relation satisfying $f(x) \lhd \mathsf{StrictLim}(f)$ for all f, x. The wellfoundedness of $\lhd$ follows from the datatype induction rule for *preordinal*. However, $\lhd$ is not a wellorder because it is not linear. To construct a wellorder, we will need to quotient *preordinal* by a suitable equivalence relation.

We define relations $\preceq$ and $\prec$ as the smallest relations satisfying the following rules. Intuitively, $x \preceq y$ iff $(\preceq)$ relates every subterm of x to some subterm of y. We then define $x \approx y$ iff $x \preceq y \wedge y \preceq x$.

$$(\forall x.\; x \lhd y \Rightarrow x \prec z) \Rightarrow y \preceq z$$

$$x \preceq y \wedge y \lhd z \Rightarrow x \prec z$$

Wellfounded inductions (using $\lhd$) show that $\preceq$ is reflexive and transitive. It directly follows that $\approx$ is an equivalence relation. We can similarly prove further transitivity rules for various combinations of $\prec$ and $\preceq$. Finally we can prove the order trichotomy rule $x \prec y \vee y \prec x \vee x \approx y$ by nested inductions on x and y.

We then define type *ordinal* as a quotient $\mathit{preordinal}/{\approx}$. The various transitivity rules show that $\prec$ and $\preceq$ respect $\approx$, so we can lift them to relations $<$ and $\leq$ on the quotient type *ordinal*. The order trichotomy rule implies that *ordinal* is wellordered by $<$. Finally, we can construct a (strict) upper bound for any countably infinite set by lifting the constructor function StrictLim to type *ordinal*.

8 Conclusion

The HOL4 theory of ordinals demonstrates that ordinals can be cleanly modelled as a quotient of wellorders, that this approach supports ordinals of large cardinalities, and that supremum can be modelled as a function taking a set as an

[1] If we replaced *num* with $\alpha\,\mathit{inf}$ in this data type, we might (this has not been pursued) then capture uncountable ordinals as in Section 5. Similarly, it is also plausible that a supremum constant akin to that in the model of Sections 2 and 3 should be definable for this type.

argument. All these contributions are novel with this work. In addition, the utility of the approach has been demonstrated by validating practically important algorithms in the ACL2 theorem-prover.

Related Work There is relatively little published work on mechanisations of ordinals within a non-set-theoretic setting. One early development is John Harrison's `wellorder` library [3]. Originally developed for HOL88, this remains part of the HOL Light library. This theory picks out certain wellorders to be ordinals using Hilbert-choice, and proves some consequences of the Axiom of Choice, such as Zorn's Lemma. It does not include any ordinal arithmetic.

In similar vein, there is a large theory of ordinals and cardinals behind Traytel *et al.* [7]. This work is available at Isabelle's Archive of Formal Proofs. It defines wellorders and develops a number of important facts about cardinalities. It does not quotient its wellorder type, and emulates ordinal arithmetic "synthetically" (*e.g.*, addition as wellorder concatenation). This work does not define ordinal multiplication nor exponentiation.

Finally, as in ACL2, it is possible to use ordinal *notations* (capturing countably many ordinals). A great deal of interesting ordinal theory (up to Γ_0) has been mechanised in this style in Coq by Castéran and Contejean [1].

Availability Most of the HOL4 theory of the ordinals described here is in the current release of HOL4. Newer material, including the validation of the ACL2 algorithms, was in the HOL4 repository by the time of commit `e3bd872ec1` and will appear in the next release. The sources for this paper are at `github.com/mn200/ordinals-paper`.

References

1. Castéran, P., Contejean, É.: On ordinal notations, available from `http://coq.inria.fr/V8.2pl1/contribs/Cantor.html`
2. Gordon, M.J.C., Reynolds, J., Hunt, Jr., W.A., Kaufmann, M.: An integration of HOL and ACL2. In: Proceedings of Formal Methods in Computer-Aided Design (FMCAD). pp. 153–160. IEEE Computer Society (2006)
3. Harrison, J.: The HOL wellorder library (May 1992), HOL88 documentation
4. Huffman, B.: Countable ordinals. Archive of Formal Proofs (Nov 2005), `http://afp.sf.net/entries/Ordinal.shtml`, Formal proof development
5. Kaufmann, M., Slind, K.: Proof pearl: Wellfounded induction on the ordinals up to ε_0. In: Schneider, K., Brandt, J. (eds.) TPHOLs. Lecture Notes in Computer Science, vol. 4732, pp. 294–301. Springer (2007)
6. Manolios, P., Vroon, D.: Ordinal arithmetic: Algorithms and mechanization. Journal of Automated Reasoning 34(4), 387–423 (2005)
7. Traytel, D., Popescu, A., Blanchette, J.C.: Foundational, compositional (co)datatypes for higher-order logic: Category theory applied to theorem proving. In: Proceedings of the 27th Annual IEEE Symposium on Logic in Computer Science. pp. 596–605. IEEE (2012)