Ordinals in HOL: transfinite arithmetic up to (and beyond) ω_1

Michael Norrish   Brian Huffman

Wednesday, 24 July 2013

Why?

Ordinals are **cool**: where else can we say something as mind-blowing as *"the set of countable ordinals is uncountable"*?

Previous approaches in typed higher order logics have not allowed

- suitably arbitrary uses of supremum; or
- modelling of ω_1

Also, Ordinals in ACL2

ACL2 uses ordinals to justify recursive definitions:

1. find a suitable ordinal when making definition (automatically or interactively);
2. system admits definition

But, ACL2's ordinals are actually an ordinal notation, with no verified connection to "real" ordinals.

ACL2's Ordinals

ACL2's notation is Cantor Normal Form up to ε_0

- *e.g.*, $\omega^2 + \omega \cdot 2 + 1$ or $\omega^{\omega^{\omega+1}} + \omega^3 \cdot 4 + \omega \cdot 10 + 4$

Kaufmann and Slind show that $<$ on this type is well-founded; this is all that's really necessary.

However, we *have* shown the ACL2 type and operations are valid ordinal arithmetic.

Notational Approaches

Generally, a notational approach is easy to mechanise.

Do the equivalent of

```
Hol_datatype`ord = End of num
                 | Plus of ord × num × ord`
```

But, this only captures countably many ordinals.

Another Algebraic Approach

Based on understanding of ordinals as *'just like the naturals with a* sup *(or* limit*) function'*.

```
Hol_datatype`ord = Z
                 | S of ord
                 | Lim of (num → ord)`
```

Using num above still only gets countable ordinals (and sup over countable sets).

More importantly, tricky quotienting still required (see paper for how to make this work).

von Neumann's Approach

An ordinal number is a set α such that

- α is transitive (that is, every member of α is also a subset of α); and
- $\forall x, y \in \alpha$ one of the following holds: $x \in y$, $x = y$ or $y \in x$.

And so, every ordinal is equal to the set of its own predecessors.

Simple Types and von Neumann

If the type of an ordinal α has to equal the type of a set of ordinals (α's predecessors), we must solve "τ `set` $= \tau$", which is clearly impossible in HOL.

The best we can hope for is to show that ordinals are in bijection with predecessor sets...

von Neumann is a Distraction

"Really," ordinals are just canonical wellorders of a given order type.

In set theory (ZFC, NBG, ...) we can't say "*ordinals are equivalence classes of wellorders*" because this phrase does not denote a set.

But we *can* do just this in HOL.

Ordinals *are* Wellorder Equivalence Classes

This works in HOL because the wellorders, and thus the ordinals, are with respect to some underlying set.

Start with α `wellorder`, the type of sets of pairs of αs where the relation is a wellorder.

And so, the α `wellorder`s are in bijection with a (strict) subset of all possible values of type $(\alpha \times \alpha)$ `set`.

Necessary Properties of Wellorders

Need to **define** notions of

- wellorder isomorphism;
- initial segments on wellorders; and
- wellorder $<$: $u < v$ iff there is an e in v such that u is order isomorphic to the initial segment of v up to e

Need to **prove**:

- isomorphism an equivalence;
- ordering is a partial order, well-founded, trichotomous.

Next Step: Quotient

All the important properties lift through quotienting.

Thanks to well-foundedness, can define oleast operator, returning minimal ordinal of a non-empty set.

- $\mathsf{oleast}\{x \mid \mathsf{T}\}$ is the zero ordinal.

Cardinalities

If the type α is finite, α `wellorder` only has finitely many elements too.

So, let the α `ordinal` type be a quotient of wellorders over the (sure to be infinite) type α + `num`.

- $\mathsf{oleast}\{x \mid y < x\}$ is the successor of y
- some work (still to come) to show this always exists

The Critical Cardinality Result

There are strictly more values in α `ordinal` than there are in α + `num`

- follows from the observation that α `ordinal` itself forms a wellorder, and
- that every wellorder over α + `num` is isomorphic to an initial segment of the α `ordinal` wellorder

Defining Supremum

Let

$$\mathsf{sup}\ S = \mathsf{oleast}\{\alpha \mid \alpha \notin \bigcup_{\beta \in S} \mathsf{preds}\ \beta\}$$

I.e., the least ordinal not in the combined predecessors of all the elements in *S*.

Supremum Works

"*The least ordinal not in the combined predecessors of all the elements in S*" is OK because:

- any given ordinal in α `ordinal` has no more predecessors than α + `num`; and
- cardinal $\kappa \times \kappa \approx \kappa$, so there must be a minimal element not in the collective predecessors

The Supremum Rule

It is legitimate to write

$$\mathsf{sup}\ S$$

when S is a set of α `ordinals` if

$$S \preceq \alpha + \mathtt{num}$$

And so...

Can define $\omega = \mathsf{sup}\{\&n \mid \mathsf{T}\}$

- where & is the injection from natural numbers into ordinals

Can distinguish limit and successor ordinals.

Can prove a recursion theorem by cases...

A Recursion Theorem

With $<$ on ordinals well-founded, one could always define functions by well-founded recursion.

A Recursion Theorem

With $<$ on ordinals well-founded, one could always define functions by well-founded recursion.

However, this pseudo-algebraic principle is nicer to use:

$$\forall z\, sf\, lf.\ \exists! f.$$
$$\begin{array}{rcl} f(0) & = & z \\ f(\alpha^+) & = & sf(\alpha, f(\alpha)) \\ f(\beta) & = & lf(\beta, \{f(\eta) \mid \eta < \beta\}) \end{array}$$

(where β has to be a non-zero limit ordinal).

Arithmetic Comes Next

The recursion principle makes it easy to define

- addition,
- multiplication,
- exponentiation

Some more work results in definitions and properties of division, remainder, and discrete logarithm.

See Paper For:

Cantor Normal Forms:

- Every ordinal can be expressed as a unique "polynomial" over bases ≥ 2

See Paper For:

Cantor Normal Forms:

- Every ordinal can be expressed as a unique "polynomial" over bases ≥ 2

Existence of Fixed Points:

- Every increasing, continuous function has infinitely many fixed points
- *E.g.*, can define ε_0, first fixed point for $x \mapsto \omega^x$

Countable Ordinals and ω_1

A *countable ordinal* is one with countably many predecessors.

In α `ordinal`, which is over α + `num`, all ordinals may be countable.

- Critical cardinality result tells us there are uncountably many of them!

To get more, instantiate α in α + `num` to $\alpha + ($`num` $\rightarrow$ `bool`$)$

The First Uncountable Ordinal

First, prove that cardinality of $\{\beta \mid \beta \text{ is countable}\}$ is $\preceq$ cardinality of $(\alpha + (\mathtt{num} \to \mathtt{bool})) + \mathtt{num}$

Then, it's legitimate to write

$$\omega_1 \stackrel{\text{def}}{=} \mathsf{sup}\{\beta \mid \beta \text{ is countable}\}$$

when β has type $(\alpha + (\mathtt{num} \to \mathtt{bool}))\ \mathtt{ordinal}$

ω_1 and so on

ω_1 is the first uncountable ordinal:

$$\beta < \omega_1 \iff \beta \text{ is countable}$$

To capture ω_2 we might instantiate type variable

$$\alpha \mapsto \alpha + ((\texttt{num} \to \texttt{bool}) \to \texttt{bool})$$

Conclusions

The "obvious" way to mechanise ordinals, as equivalence classes of wellorders, works well.

Supremum can be defined naturally, taking sets of ordinals as an argument.

- Usual arithmetic falls out

Just as naturally, large ordinals such as ω_1 can be defined.