Measures & Intro to Set Theory

Pete Manolios
Northeastern

Formal Methods, Lecture 3

September 2008

Termination examples

- We saw that ACL2s can prove termination for:

```
(ack x y) =
(cond ((zp x)
       (1+ y))
      ((zp y)
       (ack (1- x) 1))
      (t (ack (1- x) (ack x (1- y)))))
```

- Challenge problem: What is the largest n for which compute (ack n n)?
- Physically impossible to compute (ack 4 3)
- How do we prove termination?
- How else might you show that this equation doesn't lead to inconsistency?

Termination: “Printing Problem”

“The checker has to verify that the process comes to an end. Here again he should be assisted by the programmer giving a further definite assertion to be verified. This may take the form of a quantity which is asserted to decrease continually and vanish when the machine stops. To the pure mathematician it is natural to give an ordinal number. In this problem the ordinal might be $(n - r)\omega^2 + (r - s)\omega + k$.”

-Alan M. Turing (1949)

Introduction to Ordinals

- Basis of Cantor's set theory (1897, *Mathematische Annalen*)

  "... the finest product of mathematical genius and one of the supreme achievements of purely intellectual human activity"

  - Hilbert
- Intuition:
  - Start with 0, close under +1
  - The smallest ordinal, 0, is really {}
  - 1 = {0} is next, obtained by 0 + 1
  - 2 = {0, 1} is next, and so on to get all naturals
  - ...
- Can't we stop now? (Aren't the naturals enough?)
- How do we use ordinals?

Ordinals in ACL2

- Recall Definitional Principle requires termination proof
- What does that mean?
  - Exhibit a measure, a function from the formals to ordinals
  - s.t. the measure decreases on every recursive call
- (app x y) = (if (endp x) y (cons (car x) (app (cdr x) y)))
- What is an appropriate measure?
- (len x) = (if (endp x) 0 (+ 1 (len (cdr x)))) (len is in GZ)
- Proof obligations
  - (o-p (len x))
  - (implies (consp x) (o< (len (cdr x)) (len x)))
- Do we really need more than ω?
- Try all previous examples

Ordinals

- Start with 0, close under +1 *and unions*
- The smallest ordinal, 0, is really {}
- 1 = {0} is next, obtained by 0 + 1
- 2 = {0, 1} is next, and so on
- $0 \cup 1 \cup 2 \cup \cdots = \omega$ (naturals) is the first infinite ordinal
- Keep going: {0, 1, 2, ..., ω} = ω+1, ω+2, ..., ω+ω = ω·2, ω·2+1, ..., ω·3, ..., ω·ω = ω^2, ..., ω^3,..., ω^ω, ..., $\omega^{\omega^{\omega^{\cdots}}} = \varepsilon_0$
- ε_0 satisfies the equation $\alpha = \omega^\alpha$ (What is its size?)

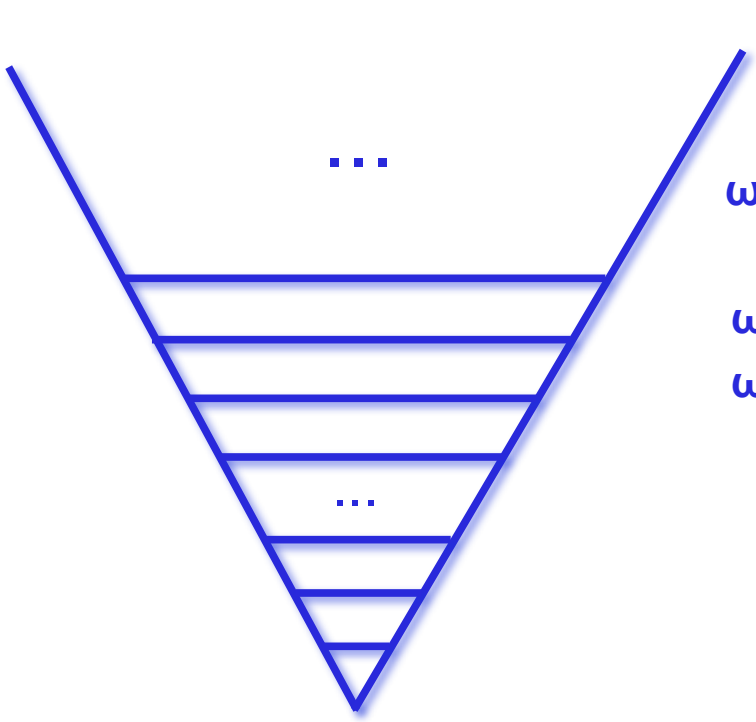
Some Questions

- Why stop at ε_0?
- Why not just say “well-founded”?
- Can we prove termination automatically?

Recursion and Induction

- When you prove termination, you get an induction scheme
- For example consider app, nat-ind
- The induction scheme for app is useful for proving theorems about app
  - The measured subset is important
  - Can be automated
  - Show app is associative
- But, the induction scheme can be used to prove theorems that don't mention app
- So, termination is a key enabling technology for theorem proving

Standard Model of Set Theory



$V_0 = \{\}$

$V_{\alpha+1} = \wp(V_\alpha)$

$V_\alpha = \bigcup_{\beta<\alpha} V_\beta$

$V = \bigcup_{\alpha\in On} V_\alpha$

What are Ordinals Good for?

- Relation to cardinal numbers
- Ordinals in proof theory
  - Gentzen used ε_0 to show Con(PA)
  - Consistency & strength of theories
  - Constructive proofs & ordinal notations (Church, Kleene)
- Computer Science
  - Termination proofs: partial vs total correctness
  - Term rewriting (well foundedness of tree orderings)
  - Reactive systems: liveness
  - *Any* termination argument can be embedded in ordinals
  - Can use ordinal arithmetic: methods for combining well founded relations