A Tutorial on (mainly countable) Ordinals

Thomas Forster

July 27, 2025

Contents

Stuff to fit in

Look at p. 101.

Notice that there is a good notion of normal function from (as it might be) von Neumann ordinals to Russell-Whitehead ordinals. This reveals to us a rudimentary typing discipline on the language of ordinals arithmetic. Something to think about!

If we are thinking about fixed points for functions ordinals $\to$ ordinals then there can be only one type of ordinal: whatever typing discipline that we were trying to form in our minds collapses immediately.

What happens if we try and describe ordinals not using fixpoint machinery?

Suppose we think there are two kinds of ordinals: `pink` and `blue`. `pink` ordinals are arguments to functions and `blue` ordinals are values. Normal functions go from `pink` ordinals to `blue` ordinals. The *division algorithm for normal functions* respects this distinction. Indeed – and this is something i find quite exciting – it looks at first blush that we can state and prove the Cantor Normal Form theorem for ordinals below ϵ_0 while maintaining this distinction. Let's work through the proof and see how it goes. We are given a target ordinal β. It is `blue`. There is a largest `pink` ordinal α s.t. $\omega^\alpha \leq .$ α is `pink` (it's an argument to $\gamma \mapsto \omega^\gamma$ after all) and ω^α is `blue` – like β Then we apply the division algorithm to β using the function $n \mapsto \omega^\alpha \cdot n$. Hmmm, not so good. $\omega^\alpha \cdot n$ looks `blue`ish but then it seems that ω^α has to be `pink`.

But perhaps not, 'n' has to be `pink` certainly, but ω^α isn't an argument but a parameter to a function.

What can we save..?

It seems we get a typing system for variables ranging over ordinals.

If a variable never appears as a value to a function decorate it with 0.

If a variable appears as a value to a function with an agument decorated by n decorate it with $n + 1$.

If '$\alpha \leq \beta$' appears give the two variables the same decoration.

If '$\alpha = \beta$' appears give the two variables the same decoration.

If '$\alpha = \beta + \gamma$' or '$\alpha = \beta + \gamma$' or '$\alpha = \beta^\gamma$' appear then all three variables get the same decoration . . . or does 'α' get a decoration one higher than the other two.

We want CNF to be well-typed

Make a point about the Anselmian nature of ω_1.

Is it the case that a system of fundamental sequences for ordinals below Γ will give us a set of representatives of a special kind: for each $\gamma < \Gamma$ a wellordering of $\mathbb{N}$ of order type γ

It now seems to me to be easy to prove that if α and β are countable ordinals so is α^β. α^β is the order type of the set of all functions of finite support from B to A ordered somehow. (All we care about is the cardinality). But if B and A are both countable, the

set of all functions of finite support from one to the other is likewise countable. OK, but what happens if we want to show that it works for exponentiation defined recursively? Then we have to show that the two definitions are the the same. And i suspect that is quite hard.

Start here

Mistral Constrastin and Jason Grossman have emailed me to say that (an earlier version of) this document was 'trending' on Hacker News, which moved me to look again at the text that was visible. A glance at the page of acknowledgements prompts the sad thought that Harold Simmons has died since then, and the world has deteriorated in other ways too.... The .pdf is clearly in need of updating, there being topics that I now understand much better than I did then. And at least one correspondent said that a document by John Baez was superior. This is not to be borne – Baez is a *physicist* for heavan's sake. Only logicians understand ordinals – and far too few of them, one might add. Clearly it is again time for me to take up my **pen**!

This document doesn't contain any original research, by which i mean that i am not claiming any results here for my own. That's not to say that it isn't the result of hard work! Much of these details i had to work out for myself, despite the best efforts of friends to explain them to me. I often reflect on the sad fact that the only people who really understand how the wheel works are the poor buggers who reinvent it. I suppose my readers – despite my best efforts in turn – will end up having to reinvent the wheel themselves. That's life.

I am making this document freely available because it seems there is a call for a tutorial of this nature. It is definitely work in progress, and this unhappy status becomes increasingly clear from about chapter 7 ... tho' the appendices and chapter-of-discussion-answers are OK. And the earlier parts can be trusted: I even recommend them to my students! I intend to publish it one day, so i welcome feedback.

There are exercises in the body of the text and some of them (those marked with an asterisk) have discussion answers in chapter 13.

Acknowledgements

I can be quite sure that much of the material below was explained to me by patient friends and colleagues – to whom I undoubtedly owe a huge debt of gratitude. Sadly, the manner in which I internalised this material was such as to render its provenance unascertainable on subsequent regurgitation, so I cannot now be entirely sure what I learned from whom! (There is even the possibility – admittedly remote – that I actually managed to work some of this out for myself!) One thing I do know is that I have profited greatly from the patience and understanding of Adrian Mathias, Harold Simmons, Martin Hyland, Stanley Wainer, Jeroen van der Meeren, Michael Rathjen and Nathan Bowler at least, and it is a pleasure to be able to record my endebtedness to them – and my thanks – here. It is a pleasure also to be able to record my thanks to those of my students who, trawling though these notes in the expectation of gaining en-

lightenment thereby, discovered instead a rat's nest of errors which they were then kind enough to give me the opportunity of silently correcting. Increasingly, since ths document has cautiously entered the public domain, members of the public have supplied helpful comments, for which i am suitably grateful. Thank you, Nikita Fufaev...

Target Audience

Anyone who wants to know about ordinals. Graduate students in Logic will probably derive more benefit from it then their minders would like to admit, since it provides details that are often elided from treatments in the textbooks. People in neighbouring subject areas in Computer Science (who might be subscribers to *Hacker news*!) are certainly part of my target audience. On the whole the ordinals of interest to people in Computer Science are countable, and one can gain a mastery of them which is adequate for most purposes without having to go wading through any set theory.

Notation, Background, etc

Lowercase Greek letters are used to range over ordinals. The letter 'λ' – its use in λ-calculus notwithstanding – is always liable to be a variable ranging over *limit* ordinals in the way that in A-level analysis 'x' and 'y' are ordinate and abcissa, or input and output variables. With this in mind I shall refrain from using lambda notation, using the '$\mapsto$' notation instead.

I am going to assume that the reader knows a bit of first-year analysis: the rationals are countable, and dense in the reals (which are not countable); there is a real between any two rationals and a rational between any two reals. The set of naturals is of size $\aleph_0$; the continuum is of size $2^{\aleph_0}$. The **Continuum Hypothesis** is the proposition that $2^{\aleph_0} = \aleph_1$. Perhaps you do not yet know what $\aleph_1$ is but this will be explained to you on page 38.

I am going to assume that you know a bit of recursive function theory, though not very much, and only in the last few pages.

Chapter 1

The Emergence of Ordinals: Basics

Ordinals were the last acquisition by the Mathematical Zoo for the Number House, a donation by Cantor in the late 19th century. Like cardinals – but unlike naturals, integers, rationals, reals and complexes – ordinals can be infinite as well as finite (a feature they share with cardinals, and with Conway numbers) and therein lies much of their interest. In this document I shall explain where they come from, what they can do for you, and why (despite their being infinite) you (a mere finite being) need to worry about them.

I have taken great care to develop the theory of ordinals in a way that is not sensitive to set-theoretical assumptions. Nothing in what follows will depend in any way on ordinals being sets of any kind.

1.1 Cantor's Discovery of Ordinals

Ordinals were invented by Cantor to solve a problem in the theory of Fourier series. Although it's an interesting story I shall consider only those bits of it that are directly relevant.

X is a **set of uniqueness** if any periodic function that takes the value 0 on all arguments not in X has all Fourier coefficients zero.

A Fourier series whose every coefficient is zero is obviously the identically zero function. What about the converse? Cantor's first theorem said that if S is a Fourier series which converges to 0 everywhere then all coefficients are zero.

Obvious question: can we weaken the hypothesis by weakening 'everywhere' to 'except on a small set' in some sense of small? The answer is: yes, indeed we can. Think about the Fourier series for a square wave. That illustrates how a set of isolated points is a set of uniqueness.

> Quite how far one can weaken it is a question that doesn't have a nice answer. However Cantor was able to show that "something-or-other" can be closed-countable, and he did this by transfinite induction on the rank of closed sets. It turns out that

> the assumption of closedness is unneccessary, as was shown by an Englishman by the name of 'Young' by a completely different method.[1] But the trip up the blind alley at least gave us ordinals.

In the course of his investigations Cantor became interested in applying to an arbitrary closed set X of reals the operation that returns its **derived set**, or **derivative**: the set of all limit points of X. I think the point is that if the derivative of X is a set of uniqueness then so is X. Something like that. If X is closed its derived set is a subset of it. How often can one apply this operation to a closed set before one reaches either an empty set or a perfect closed set (which is a fixed point, being equal to its derived set)? The interesting point here is that, since this operation is monotone decreasing with respect to $\subseteq$, it makes sense to think of transfinite iteration: one can take intersections at limit stages and carry on deriving. So the answer to the question "How often?" might not be a natural number. What sort of number is it? The answer is that it will be an **ordinal**. Ordinals are the kind of number that measures the length of precisely this sort of process: transfinite, monotone, deterministic and discrete.

(We should see this in the context of a thought that the job of any flavour of number is *to measure something*. Cardinals measure *multiplicity*; the answer to "How many ..." is always a cardinal. Real numbers measure continuous (analogue) finite quantities.)

The idea that ordinals count the length of discrete transfinite processes should be taken seriously and can be taken further. There is an addition (concatenation) operation on processes, written '+' with overloading, but – apparently – no operation of multiplication of processes *by processes*. However there is a notion of multiplication of a process by an ordinal ("Do this α times"): a process multiplied on the right by an ordinal is another process.

Thus, if we let $\mathfrak{p}$ and $\mathfrak{s}$ be processes, and let α and β be ordinals then we have the following easy equations:

1. $\mathfrak{p} \cdot (\alpha + \beta) = \mathfrak{p} \cdot \alpha + \mathfrak{p} \cdot \beta$
2. $\mathfrak{s} \cdot (\alpha \cdot \beta) = (\mathfrak{s} \cdot \alpha) \cdot \beta$

and others like it. The effect is that processes form a module over the ordinals. In fact this could be an operational way of characterising the ordinals: as that-kind-of-number-such-that-processes-form-a-module-over-them[2]

Processes in our sense are discrete things (they have lengths that are ordinals after all) so we can interleave them. So we have to think about the lengths of interleavings of two processes.

> This turns out to be a thing called the *Hessenberg sum* which we will see in chapter 6, and gives us an inner product!
> I'm not sure how seriously this idea should be taken: certainly the mathematical community at large makes nothing of the possibility of thinking of the set of processes as something like a vector space over the ordinals.

[1] I stumbled upon the article in which Young proved this. It is in the same volume of the same journal as the article [15] by Hardy below!

[2] Pedants will delight in pointing out that modules are formed over *rings* and that the ordinals do not form a ring.

I have recently (re)discovered a typescript of Girard and Norman which says that things called *dilators* (which we may see later) behave like linear operators in vector spaces ... so presumably they had the same idea.

The Greeks never knew about ordinals. If they had, they might have seen a connection with Zeno's paradox of Achilles and the Tortoise. In that mind-game (More politely *thought-experiment*) one envisages an infinite sequence of stages where Achilles catches up to where the Tortoise has advanced to since the previous stage. This sequence is of course of length ω.

Even if all we know about ordinals is that they are the kind of number that enumerates the stages in processes like that of Cantor's we considered, we nevertheless know quite a lot about them. At any stage there is always in principle the possibility of a next stage, so the successor of an ordinal is an ordinal. But because the operation of taking-the-derived-set is monotone, there is a concept of a limit stage, so it must be that a supremum of a set of ordinals is an ordinal.

At this point I should really give a presentation of the ordinals as a recursive datatype. Unfortunately I am not in a position to do so, since assembling ing the precise specification turns out to be a fiddlier task than I had hoped, and it may well be that there is more than one way of doing it. I shall restrict myself to making some basic but (i hope) helpful observations, leaving the discussion of work-in-progress to an appendix.

1. The idea is that the Ordinals are like the Naturals with an extra constructor: `sup-of`, which is applied to sets of ordinals. This makes it a higher-order recursive datatype. Finite ordinals are in some sense the same things as natural numbers. Unless we have very strong type-theoretic scruples we just think of them as the same.

2. Since distinct sets of ordinals can have the same `sup` the `sup` constructor is not free, and this is the chief source of the trouble.

3. The reader should rehearse the way in which the declaration of $\mathbb{N}$ as a rectype gives rise to the engendering relation $<_{\mathbb{N}}$ and a proof that that engendering relation is a total order, and wellfounded. Make sure you understand that. Once you do, you will be able to see what a declaration of the ordinals should look like.

Ad (1) it's worth warning the reader not to confuse ordinals with nonstandard integers or with infinite Dedekind-finite cardinals. These three wild-and-woolly things that live in the desolate marches beyond $\mathbb{N}$ often sound similar to beginners, but they are all completely different things!

Infinite Dedekind finite cardinals (aka *Dedekind cardinals*) are cardinals not ordinals – they measure bulk, not order. Whether or not there are such things depend on whether or not countable choice holds. At all events there are no definable Dedekind cardinals, none you can name. So there is no way of reidentifing Dedekind cardinals across models, and there is no system of notation for them.

Nonstandard naturals are a pox brought to us by compactness. They're ordinals, beco's they are natural numbers and natural number are finite ordinals, but of course they are *nonstandard* ordinals. Like Dedekind-cardinals they are a product of a malfunction, and none of them can be definable. Again, there is no way of reidentifying them across models, and there is no system of notation for them.

In contrast, countable ordinals are not creatures of the night. Their relationship to natural numbers is that natural numbers are the finite things of this flavour. Unlike the Dedekind cardinals and nonstandard naturals, countable ordinals can be reidentified across models, and there are systems of notation for them. Indeed we will have quite a lot to say about notations for them in later sections.

1.2 Ordinals as Order Types

Ordinals are also the order types (aka isomorphism classes) of wellorderings, which are a special kind of total order.

Actually a *very* special kind of total order. Practically none of the total orders you will have encountered so far in your life, Dear Reader, will have been wellorderings. The integers, the reals, the rationals, interesting natural subsets of them, none of them are wellorderings. Almost certainly the only wellorderings you will have encountered are the finite wellorderings (every finite total ordering is a wellordering) and $\mathbb{N}$. Every now and then i encounter beginners who expect the order type of the reals to be ω_1; it isn't: the reals in their natural order are not a wellordering. No uncountable total order that you have seen is a wellorder. The natural numbers $\mathbb{N}$ in their usual ordering is the first nontrivial example of a wellordering.

The order type (isomorphism class, ordinal) of $\mathbb{N}$ in its usual order is always denoted 'ω'. 'ω' is of course the last letter of the Greek alphabet, and that ordinal comes after all the finite ordinals. However, for our purposes, it is a beginning rather than the end – a *point of departure* – co's we are interested in ordinals beyond ω.

What distinguishes ordinals from other linear order types is that they are the order types of *wellfounded* linear order types, aka wellorderings. We'd better get welfoundedness straight.

1.2.1 Wellfoundedness

Suppose we have a carrier set with a binary relation R on it, and we want to be able to infer

$$\forall x\, \psi(x)$$

from

$$(\forall x)((\forall y)(R(y,x) \rightarrow \psi(y)) \rightarrow \psi(x))$$

In words, we want to be able to infer that everything is ψ from the news that you are ψ as long as all your R-predecessors are ψ. y **is an R-predecessor of** x if $R(y,x)$. Notice that there is no "case $n = 0$" clause in this more general form of induction: the premiss we are going to use implies immediately that a thing with no R-predecessors must have ψ. The expression "$(\forall y)(R(y,x) \rightarrow \psi(y))$" is called the **induction hypothesis**. The first line says that if the induction hypothesis is satisfied, then x is ψ too. Finally, the inference we are trying to draw is this: **if** x has ψ whenever the induction hypothesis is satisfied, **then** everything has ψ. When can we do this? We must try to identify some condition on R that is equivalent to the assertion that this is a legitimate inference to draw in general (i.e., for any predicate ψ).

Why should anyone want to draw such an inference? The antecedent says "x is ψ as long as all the immediate R-predecessors of x are ψ", and there are plenty of situations where we wish to be able to argue in this way. Take $R(x, y)$ to be "x is a parent of y", and then the inference from "children of blue-eyed parents have blue eyes" to "everyone has blue eyes" is an instance of the rule schematised above. As it happens, this is a case where the relation R in question does *not* satisfy the necessary condition, for it is in fact the case that children of blue-eyed parents have blue eyes and yet not everyone is blue-eyed.

To find what the magic ingredient is, let us fix the relation R that we are interested in and suppose that the inference

$$\frac{(\forall y)(R(y,x) \to \psi(y)) \to \psi(x)}{(\forall x)(\psi(x))} \qquad R\text{-induction}$$

has failed for some choice ψ of predicate. Then we will see what this tells us about R. To say that R is well-founded all we have to do is stipulate that this failure (whatever it is) cannot happen for any choice of ψ.

Let ψ be some predicate for which the inference fails.

Then the top line is true and the bottom line is false. So $\{x : \neg\psi(x)\}$ is nonempty. Let us call this set A for short. Using the top line, let x be something with no R-predecessors. Then all R-predecessors of x are ψ (vacuously!) and therefore x is ψ too. This tells us that if y is something that is not ψ, *then there must be some y' such that $R(y', y)$ and y' is not ψ either.* If there were not, y would be ψ. This tells us that the collection A of things that are not ψ "has no R-least member" in the sense that everything in that collection has an R-predecessor in that collection. That is to say

$$(\forall x \in A)(\exists y \in A)(R(y, x))$$

To ensure that R-induction can be trusted it will suffice to impose on R the condition that $(\forall x \in A)(\exists y \in A)(R(y, x))$ never hold, for any nonempty $A \subseteq dom(R)$. Accordingly, we will attach great importance to the following condition on R:

DEFINITION 1 *R is* **well-founded** *iff for every nonempty subset A of $dom(R)$ we have* $(\exists x \in A)(\forall y \in A)(\neg R(y, x))$

(x is an "R-minimal" element of A.)

This definition comes with several health warnings: it is easy to misremember. The only reliable way to remember it correctly is to rerun in your mind the discussion we have gone through: well-foundedness is precisely the magic property one needs a relation R to have if one is to be able to do induction over R. No more and no less. The definition is not *memorable*, but it is *reconstructible*.

A second warning. It's easy to remember that wellfoundedness has a crucial minimal-element condition, but it's easy to remember it *wrong*. The condition is not that the domain of the relation has a minimal element; it's that *every nonempty subset* has a minimal element.

THEOREM 1 *Wellfounded induction: recursion on wellfounded relations*

Induction over a wellfounded relation is immediate. Justification of recursion requires a little thought.

Let $\langle X, R\rangle$ be a binary structure, with R wellfounded. Then the recursion

$$f(x) = G(x, \{f(x') : R(x', x)\})$$

has a unique solution as long as G is everywhere defined.

A niggle: why does G need to look at x? Why isn't it enough for it to look merely at $\{f(x') : R(x', x)\}$?

Answer: There might be two distinct things a and b s.t. $\{f(x) : R(x, a)\}$ and $\{f(x) : R(x, b)\}$ are the same set, and we want to keep open the possibility of f sending a and b to different things.

Fix f. We need the concept of the transitive closure of a relation. The transitive closure of R, written '$R*$' is the $\subseteq$-least transitive relation $\supseteq R$.

However the clever idea which is specific to this proof is the concept of an **attempt**. An attempt-at-x is a function f_x which is defined at x and at every y such that $R^*(y, x)$, and obeys the recursion wherever it is defined. That is to say, if f_x is defined for all z s.t. $R(z, y)$, and it is defined at y, then we must have $f_x(y) = G(y, \{f_x(z) : R(z, y)\})$.

The concept of *attempt* is the only clever part of this proof. All that remains to be done is to choose the right thing to prove by induction. We prove by R-induction on 'x' that (i) every x has an attempt-at-x and that (ii) all attempts-at-x agree at x and at all y such that $R^*(y, x)$. Everything has been set up to make that easy.

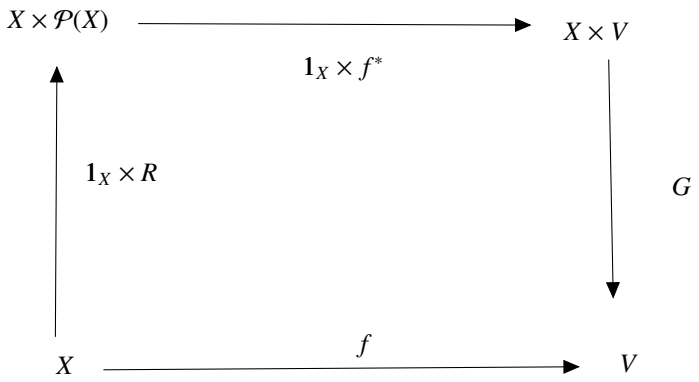
So: suppose the induction hypothesis holds for all y s.t. $R(y, x)$.

That is to say, for every y s.t. $R(y, x)$, there is f_y, an attempt-at-y, and all attempts-at-y agree on all y' s.t. $R^*(y', y)$.

Is there an attempt-at-x? Yes. We take the union of all the f_y for $R(y, x)$ and add the ordered pair that tells us to send x to $G(x, \{f_y(y) : R(y, x)\})$.

Then the function that we are declaring by this recursion is simply the function that, for each $x \in X$, sends it to whatever-it-is that all attempts-at-x want to send x to. This function is defined everywhere and it clearly obeys the recursion.

That is to say, for any set X with a wellfounded relation R on it, and every function $G : X \times V \to V$ there is a unique f making the following diagram commute.



DEFINITION 2 *Wellordering a wellfounded strict total order*

"every terminal segment has a least element" is equivalent. It's the "always an immediate next stage" condition.

COROLLARY 1 *Principle of induction for wellorderings*

COROLLARY 2 *Definition by recursion for wellorderings*

DEFINITION 3 *Ordinals are isomorphism types of wellorderings.*

There now follows a raft of things that you need to keep straight in your mind if you are to avoid going crazy. You don't need to know the proofs of these things but you need to internalise them co's they underpin everything.

THEOREM 2

1. *Every wellordering is rigid (no nonidentity automorphisms);*
2. *If there is an isomorphism between two wellorderings $\langle A, <_A\rangle$ and $\langle B, <_B\rangle$ then it is unique;*
3. *Given two wellorderings $\langle A, <_A\rangle$ and $\langle B, <_B\rangle$ one is isomorphic to a unique initial segment of the other.*

Proof:

1. The automorphism group of a total order is torsion-free: every nontrivial cycle looks like $\mathbb{Z}$. If τ is an automorphism of a wellordering consider $\{\tau^n(x) : n \in \mathbb{Z}\}$. What is its least element?
2. Suppose σ and τ were two distinct isomorphisms $\langle A, <_A\rangle \to \langle B, <_B\rangle$; then $\sigma \cdot \tau^{-1}$ would be a nontrivial automorphism of $\langle B, <_B\rangle$.

3. We define an isomorphism by recursion in the obvious way. It must exhaust either $\langle A, <_A\rangle$ or $\langle B, <_B\rangle$ and, by the earlier parts, it will be unique.

   To be slightly more formal about it, define $f : A \to B$ by the recursion $f(a) =: \sup\{f(a') : a' <_A a\}$ and $g : B \to A$ *mutatis mutandis*. We prove by wellfounded induction that $f \cdot g$ is the identity where it is defined. One of f and g must be total. If not, let a be the first thing not in the domain of f and b the first thing not in the domain of g. Then $\langle a, b\rangle$ should have been in f and $\langle b, a\rangle$ should have been in g.

DEFINITION 4 $\langle X, \leq_X\rangle$ **is an end-extension of** $\langle Y, \leq_Y\rangle$ *iff*

(i) $Y \subseteq X$,
(ii) $\leq_Y \subseteq \leq_X$, *and*
(iii) $(\forall y \in Y)(\forall x \in X)(x \leq y \to x \in Y)$.

Alternatively "$\langle Y, \leq_Y\rangle$ **is an initial segment of** $\langle X, \leq_X\rangle$*"*

"New stuff cannot be earlier than old stuff".

For the moment we use this only where $\langle Y, \leq_Y\rangle$ and $\langle X, \leq_X\rangle$ are wellorderings, but the idea is susceptible of generalisations to arbitrary posets. The concatenation of two tosets is an end-extension of the first toset, so addition of order types involves end-extension.

Every nonstandard model of PA is an end-extension of the standard model. We have an important notion of end-extension in set theory ("no new members of old sets") but we won't develop these ideas here.

LEMMA 1 *Every suborder of a wellorder is isomorphic to an initial segment of it.*

Proof:

The suborder inherits totality and wellfoundedness, and so is a wellorder. Apply theorem 2. ■

You might like to visualise this.... Suppose $\langle A, <_A\rangle$ injects isomorphically into $\langle B, <_B\rangle$. You do the "Othello" (falling discs) trick to the range of the injection to collapse it down to an initial segment of $\langle B, <_B\rangle$.

Notice that this is not true of arbitrary total orders. Not every subordering of $\mathbb{Z}$ is iso to an initial segment. There is in fact a converse to lemma 1 which you might like to prove.

EXERCISE 1 *If every subordering of a given toset is iso to an initial segment then the toset is a wellordering.*

In the light of this lemma we can define an order relation on ordinals:

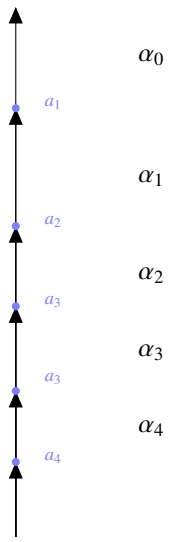
DEFINITION 5
$\alpha \leq_{On} \beta$ *if every wellordering of length* β *(every wellordering whose equivalence class is* β*) has an initial segment of length* α.

Equivalently
$\alpha \leq_{On} \beta$ *if every wellordering of length* α *can be injected in an order-preserving way into every wellordering of length* β.

The two ways you might define it are equivalent beco's of lemma 1.

Notice that this leaves open the question of how we define $\leq$ on arbitrary linear order types.

The following fact is crucial.



THEOREM 3 *$<_{On}$ is wellfounded.*

Proof: Let α be an ordinal. We will show that the ordinals below α are wellfounded under $<_{On}$. The long arrow represents a wellordering $\langle A, <_A\rangle$ of length $\alpha = \alpha_0$. If *per impossibile* there is a family $\{\alpha_i : i \in I\}$ of ordinals with no least member (and all of them $< \alpha$) then, for each $i \in I$, $\langle A, <_A\rangle$ has a (unique) proper initial segment of length α_i. For $i \in I$ let a_i be the supremum of that (unique) initial segment of $\langle A, <_A\rangle$ of length α_i. Then $\{a_i : i \in I\}$ is a subset of A with no $<_A$-least member. ■

I have drawn the picture as if the index set I were $\mathbb{N}$ and the sequence is strictly descending. We don't actually need this assumption but it does make the picture easier to draw. The assumption can be justified by appeal to a principle called DC: the principle of *dependent choice* of which more in section **??**.

This result is nontrivial: it's not always true that the family of isomorphism types of widgets has a widget structure. Think of the open and closed intervals $(0, 1)$ and $[0, 1]$ in the reals. This illustrates how linear order types without wellfoundedness are not a linear order; not even antisymmetrical indeed!

Beware! Some textbooks contain theorems with statements that sound like theorem 3 but are actually much weaker. A proof that the order relation on von Neumann ordinals is wellfounded is not a proof that $\langle On, <_{On}\rangle$ is wellfounded any more than a check that `UBUNTU` runs properly on my laptop means that it will run safely on yours. The fact that `UBUNTU` runs safely on my laptop is not a fact about the safety of `UBUNTU`

but a fact about the binary for my machine, and that says nothing about the binary for your machine.

The order relation $\leq$ on ordinals is a wellordering, so the wellordering of the ordinals below α has an ordinal. What is this ordinal? It obviously depends somehow on α. It turns out that it is fact exactly α. This fact is so cute that it has become the basis of the standard implementation of ordinal arithmetic into set theory. In this implementation (due to Von Neumann) each ordinal is simply taken to *be* the set of ordinals below it.

THEOREM 4 *Vital, central fact! (Cantor)*
Every ordinal is the order type of the set of ordinals below it in their natural order.
Equivalently:
The order type of an initial segment of the ordinals is the least ordinal not in it.

Proof:
On the assumption that ordinals are monomorphic you prove this by induction. ■

"Monomorphic"?

If, like me, you have type-theoretic scruples then there is something to worry about here. Put your type-theorist's hat on for the moment. Ordinals arise as isomorphism classes of wellorderings of stuff. Does the type of the ordinal that you get when you abstract away from the wellorderings depend on the type of the stuff that is being wellordered? *Prima facie* it might. Think about natural numbers and lists. Usually we take lists to be polymorphic: for each type α there is a type α-`list`. However once we apply the `length` constructor to objects of any of these types to get a natural number we get objects of only the one type: `int`. We don't get a polymorphic family α-`int`, and nobody would normally suggest that we should. However, if one were an extreme purist one feel like saying that, in principle, we should. For example: one might note that, strictly speaking, Euler's totient function (for example) is properly defined only for those `int`s that are `int`s of lists of `int`s, not on `int`s that are `int`s of lists of `wombat`s, for example. However this purism is obviously extreme, since it's pretty clear that all these types are isomorphic and we will happily make do with only one type of `int`s. This will enable us to minute that fact that, for any natural number n, the set $[0, n-1]$ of its predecessors is of length n. Rosser called this the **Axiom of Counting**. The axiom of counting (for $\mathbb{N}$ at any rate) is fine[3]; it is the extension of this observation to ordinals that is – ultimately – problematic. The problem it ultimately leads to is the **Burali-Forti paradox**.

COROLLARY 3 *(The Burali-Forti Paradox)* ☠☠
The collection On of all ordinals cannot be a set.

Proof:
By theorem 3 $\langle On, <_{on}\rangle$ is a wellordering. Since it is downward-closed, theorem 4 tells us that its order type must be the least ordinal not in it. The least ordinal that is not a ordinal? I don't need this! Beam me up, Scottie. ■

[3]There is virtue to be gained from thinking about how one might prove it!

The availability of theorem 4 relies on ordinals being monomorphic. The type-theoretic take on this is that at some point they have to stop being monomorphic lest we get the Burali-Forti paradox. At some point we have to start distinguishing between ordinals-from-(infinite)-lists-of-as and ordinals-from-(infinite)-lists-of-bs. However the point at which hygiene compels one to adopt this stronger typing machinery comes a long way beyond anything we are concerned with here. These dangers will remain innocuously over the horizon and we can quite safely take our ordinals to be monomorphic as we did our naturals, with the effect that we believe the analogue of the axiom of counting for countable ordinals.

So concretising ordinals – thinking of them *as something* – is fraught with difficulty. For the moment here is a mental device that can help. Try thinking of cardinals just as sets, ordinary sets. Two sets are *identical-as-sets* iff they have the same members, but they are *identical-as-cardinals* iff there is merely a bijection between them. Similarly ordinals can be thought of simply as wellorderings; two wellorderings are identical-as-wellorderings if they wellorder the same things in the same way; they are *identical-as-ordinals* iff they are merely orderisomorphic.

In any case one can argue that corollary 3 goes deeper than set theory. That "fact" – that On turns out not to be a set – is an artefact of our decision to clothe this particular mathematical spirit in set-theoretic flesh. There is something deeply weird going on, and the weirdness is nothing specifically to do with set theory. If you try to understand it through other sensory modalities it will look different. As we have seen, if your first recourse is to type-theoretic intuitions then your insight will be that all ordinals are in principle polymorphic and that – altho' small ordinals can be thought of as monomorphic – all sufficiently large ordinals *have to* be thought of as polymorphic. Remember the Buddhist trope about the five blind men and the elephant: if you have only one teacher you will receive only one insight, and you will not get the full picture. I think it is fair to say that the Burali-Forti paradox is not generally understood, even by the *cognoscenti*. It's one of those things where you cannot trust the textbooks. Really.

1.3 Operations on ordinals defined "Synthetically"

Ordinals can be thought of as isomorphism classes of wellorderings. Thus some operations on wellorderings give rise to operations on ordinals.

Some of these operations are not peculiar to wellorderings. disjoint-union-followed-by-concatenation gives rise to addition; lexicographic product gives multiplication. And these operations distribute over one another in the way one expects. We can even define exponentiation! And all of these for *arbitrary* linear order types.

I'll supply the definition of exponentiation of order types for the sake of completeness here, tho' we are not going to use it – at least that's not my current intention!

Let $\langle A, <_A\rangle$ and $\langle B, <_B\rangle$ be orderings of length α and β respectively.

A function $f : A \to B$ is said to be "of "finite support" iff it sends all but finitely many of its arguments to $\bot_B$. '$\bot_B$'!? If B has a bottom element then $\bot_B$ is that element. If not, simply adjoin a new element below all the proper elements of B, and let *that* be $\bot_B$. If $\langle B, <_B\rangle$ is a wellordering then there will be a bottom element. (We are trying to

define exponentiation in sufficient generality so that it works for arbitrary linear order types, and of course not every linear order has a bottom element.)

If f and g are both of finite support then there will be a last argument x on which they disagree. We ordain that $f < g$ iff $f(x) <_B g(x)$. This is the "colex" ordering. Then we define β^α to be the order type of the set of functions $A \to B$ of finite support ordered colex.

I have to admit that it is less than entirely obvious that the colex ordering is transitive. You might like to attempt the exercise of providing a proof!

It is an elementary but extremely fiddly exercise to verify that exponentiation defined in this way interacts with multiplication in the way that it should. Mostly we will not make use of this definition, tho' we will need the fact that if A and B are both countable so is the set of functions $A \to B$ of finite support.

Warning! Ordinal exponentiation is not the same as cardinal exponentiation. ω is an ordinal and 2^ω is also an ordinal. $\aleph_0$ is a cardinal and so is $2^{\aleph_0}$. $2^{\aleph_0}$ is uncountable of course, but the ordinal 2^ω is countable. (It is in fact equal to ω.) There is a thoroughly reprehensible habit in some circles of abusing these notations – for example writing 'ω' when they mean '$\aleph_0$' – and this is a running source of confusion for beginners.

1.4 We can also define operations recursively

This is for when we thinking of ordinals as a recursive data type with 0, succ and sup.

DEFINITION 6

$\alpha + 0 := \alpha$;
$\alpha + \mathsf{succ}(\beta) := \mathsf{succ}(\alpha + \beta)$;
$\alpha + \mathsf{sup}(X) := \mathsf{sup}(\{\alpha + \beta : \beta \in X\})$.

$\alpha \cdot 0 := 0$;
$\alpha \cdot \mathsf{succ}(\beta) := (\alpha \cdot \beta) + \alpha$;
$\alpha \cdot \mathsf{sup}(X) := \mathsf{sup}(\{\alpha \cdot \beta : \beta \in X\})$.

$\alpha^0 := \mathsf{succ}(0)$;
$\alpha^{\mathsf{succ}(\beta)} := (\alpha^\beta) \cdot \alpha$;
$\alpha^{\mathsf{sup}(X)} := \mathsf{sup}(\{\alpha^\beta : \beta \in X\})$.

Given these definitions, it is clear that addition on the right, multiplication on the right and exponentiation on the right, namely, the functions $\alpha \mapsto (\beta + \alpha)$, $\alpha \mapsto \beta \cdot \alpha$ and $\alpha \mapsto (\beta^\alpha)$ are – for each fixed ordinal β – *continuous* in a "the value at the sup is the sup of the values" sense.

Remember which way round to write multiplication and addition. They are not commutative!!!

As well as addition and multiplication we are going to need ordinal **subtraction**. We desire a construct $\alpha - \beta$ which is defined whenever $\alpha \geq \beta$ and which obeys $\beta + (\alpha - \beta) = \alpha$.

in f"x notation

DEFINITION 7 *If $\beta \leq \alpha$ then whenever $\langle B, <_B\rangle$ belongs to β and $\langle A, <_A\rangle$ belongs to α, there is an isomorphism $\pi : \langle B, <_B\rangle$ to a unique initial segment of $\langle A, <_A\rangle$.*

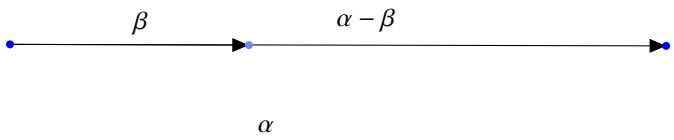
The truncation $\langle A \setminus \pi\text{"}B,\ <_A\restriction(A \setminus \pi\text{"}B)\rangle$ is our wellordering of length $\alpha - \beta$.

This definition ensures that $\beta + (\alpha - \beta) = \alpha$.

Observe however that for subtraction of β from α to be well-defined we need (i) an ordering of type α to have a unique initial segment of type β – or at the very least we need (ii) all the tail segments that remain after deletion of an initial segment of type β to be isomorphic. Thus we can subtract ω^* from $\omega^* + \omega$ to[4] obtain ω but to get subtraction of β from α to be defined for all $\beta \leq \alpha$ we need all initial segments of an ordering of type α to be pairwise nonisomorphic – or something quite like it – and there is not much hope of that unless α is an ordinal.

We will need ordinal subtraction for Cantor Normal Forms in section 4.1 – and ordinal notations generally.

Part 3 of theorem 2 reassures us that ordinal subtraction is uniquely defined.



We really do need wellfoundedness here. Let's introduce a bit of notation on the fly. For an ordinal α, α^* is α "turned upside down", so that – for example – ω^* is the order type of the negative integers, and $\omega^* + \omega$ is the order type of $\mathbb{Z}$. You'd think that $\omega^* - \omega^*$ would be 0, wouldn't you? But it can be any natural number. The set of negative integers has lots of initial segments of length ω^*.

We remark without proof that it is immediate from the definitions of addition and multiplication in terms of disjoint union and lexicographic product that both operations are associative, and that multiplication distributes over addition.

LEMMA 2

1. $(\forall\alpha)(\forall\beta)(\alpha \leq \alpha + \beta)$
2. $(\forall\alpha)(\forall\beta)(\beta \leq \alpha + \beta)$

Proof:

These two assertions are blindingly obvious if we think of α and β as isomorphism classes of total orders. However if we are thinking of ordinals as members of a recursive data type then these two assertions have to be proved by induction on that datatype. In definition 6 we define '+' by recursion. The challenge is to use that recursion to prove these two inequalities.

The two cases are different because addition on the left is different from addition on the right. Interestingly different, in fact. . . .

[4] see p 21 for definition of ω^*.

Case 1: $\alpha \leq \alpha + \beta$

For each α we prove by induction on β that $\alpha \leq \alpha + \beta$.

Case 2: $\beta \leq \alpha + \beta$

We prove by induction on β that $(\forall \alpha)(\beta \leq \alpha + \beta)$.

Clearly $(\forall \alpha)(0 \leq \alpha + 0)$

For the successor case, assume $(\forall \alpha)(\beta \leq \alpha + \beta)$. We want $(\forall \alpha)(\beta + 1 \leq \alpha + \beta + 1)$. But clearly $\beta \leq \alpha + \beta$ iff $\beta + 1 \leq \alpha + \beta + 1$.

For the limit case let $\lambda = \mathtt{sup} X$. Let α be arbitrary. We want $\lambda \leq \alpha + \lambda$.

$\alpha + \lambda = \alpha + \ \mathtt{sup} X$

$\alpha + \ \mathtt{sup} X = \mathtt{sup}\{\alpha + \beta : \beta \in X\}$

But now (by induction hypothesis) everything β in X is $\leq$ something (to wit: $\alpha + \beta$) in $\{\alpha + \beta : \beta \in X\}$ so $\mathtt{sup} X$ – which is λ – is $\leq \mathtt{sup}\{\alpha + \beta : \beta \in X\}$ – which is $\alpha + \lambda$. ■

Notice that for Case 1 we did a Δ_0 induction and for Case 2 we had to do a Π_1-induction. Addition on the right is easier to reason about than addition on the left!

We can extend this list of three definitions of functions $On \times On \rightarrow On$ further. Infinitely far in fact. (Readers may be familiar with the word *tetration*).

1.4.1 Doner-Tarski

Doner-Tarski [6] consider a hierarchy of functions defined so that:

DEFINITION 8

$f_0(\alpha, \gamma) =: \alpha + \gamma$;

check this! $f_{n+1}(\alpha, 0) =: \alpha$;[5]

$f_{n+1}(\alpha, \gamma + 1) = f_n(f_{n+1}(\alpha, \gamma), \alpha)$;

$f_{n+1}(\alpha, \lambda) =: \mathtt{sup}_{\gamma < \lambda} f_{n+1}(\alpha, \gamma)$;

$f_\lambda(\alpha, \beta) =: \mathtt{sup}_{\zeta < \lambda} f_\zeta(\alpha, \beta)$.

We are not going to be greatly concerned with functions beyond exponentiation. Generally people seem not to make much use of them. It may be worth reflecting on the fact that although – as we saw on p 19 seen – there is a "synthetic" definition of ordinal exponentiation (defining ordinal exponentiation in terms of an operation on the underlying wellorderings) this doesn't seem to be possible for operations higher up in the Doner-Tarski hierarchy. If you want to understand the Doner-Tarski operations you have to be thinking of ordinals as a recursive data type rather than as isomorphism classes of wellorderings.

[5] This is surely correct. $f_{n+1}(\alpha, 0)$ must be the result of doing f_n of something or other 0 times to α and this must be α. The consideration that causes me slight unease is that according to this line of thought $\alpha \cdot 0$ should be α not 0. So the function we call multiplication – $\alpha \cdot \beta$ is actually $f_1(\alpha, \beta + 1)$. Not that it matters. But one would have expected to see something about this in the literature.

EXERCISE 2

1. *Give examples to show that addition and multiplication on the left are not commutative.*

2. *Give an example to show that $\alpha \mapsto \alpha^2$ is not continuous.*

3. *Which of the following are true for all α, β and γ?*

   $(\alpha \cdot \beta)^\gamma = \alpha^\gamma \cdot \beta^\gamma$;
   $\gamma^{(\alpha+\beta)} = \gamma^\alpha \cdot \gamma^\beta$;
   $(\alpha + \beta) \cdot \gamma = \alpha \cdot \gamma + \beta \cdot \gamma$;
   $\gamma \cdot (\alpha + \beta) = \gamma \cdot \alpha + \gamma \cdot \beta$.

   Prove the true assertions and give counterexamples to the false assertions.

4. *Can you simplify $(\alpha\beta\gamma)^\omega$?*

The picture of ordinals as order-types of wellorderings also gives us slightly smoother – and more fundamental – motivations for the operations of addition, multiplication and exponentiation of ordinals that we have already seen. Addition corresponds to disjoint union (concatenation) and multiplication to colex order of the product. It is worth noting that because these definitions do not involve recursion we can invoke them in connection with linear order types that are not wellfounded: they work for arbitrary total order types. And the operations obey the distributivity laws that you expect.

EXERCISE 3 *Give a recursive definition of ordinal subtraction, and prove that your definition obeys $\beta + (\alpha - \beta) = \alpha$.*

There is one other fact about ordinals we will need which can be obtained only from the ordinals-as-isomorphism-classes-of-wellorderings view. Here we will be concerned specifically with countable ordinals. Recall that a countable ordinal α is the length of a wellordering of a countable set. So without loss of generality α is the length of a wellordering of $\mathbb{N}$. A wellordering of $\mathbb{N}$ can be coded as a set of ordered pairs of naturals, and ordered pairs of naturals can be coded as naturals. Wellorderings of $\mathbb{N}$ can therefore be coded as sets of naturals, which is to say as *reals*. This means that there is a surjection from the set of reals to the set of countable ordinals as follows: if a real codes a wellordering of $\mathbb{N}$, send it to its length, `else` 0. Notice that this does not obviously give us an injection from the set of countable ordinals into the reals: to do that we would have to choose, for each countable ordinal, a wellordering of the naturals of that length, and there is no obvious way to choose one. Notice that countable choice does not help here. We shall see more of this later.

So now we can do induction/recursion on ordinals.

DEFINITION 9 *A countable ordinal is the order type of a wellordering of $\mathbb{N}$.*

It's an immediate consequence of this definition, in conjunction with theorem 4, that an ordinal is countable iff there are countably many ordinals below it. This fact is too elementary to merit a label, but you need to internalise it. This absolutely must underpin your understanding of countable ordinals. Without it you would be entirely lost.

So there are *three* ways of thinking of countable ordinals:

(i) an ordinal with only countable many ordinals below it;
(ii) the order type of a wellordering of $\mathbb{N}$;
(iii) the order type of a wellordering of a countable set.

I find that students need to be warned about the possibility of confusion lurking in this form of words 'countable ordinal'. (If you are not planning to do any set theory you can ignore the rest of this paragraph.) It doesn't have the same semantics as 'countable set of reals' beco's 'countable ordinal' doesn't mean that the set that is that ordinal is countable. It may or may not be countable. If you are thinking of ordinals as von Neumann ordinals then, as a matter of fact, a countable ordinal is a countable set, but that's not what it *means*: it's pure coincidence. If you are using Scott's-trick ordinals then a countable ordinal is actually an uncountable set. So: do not attempt to add clause

We haven't discussed Scott's Tick

(iv) "is a countable set"

to the list above. It's an artefact of the von-Neumann implementation.

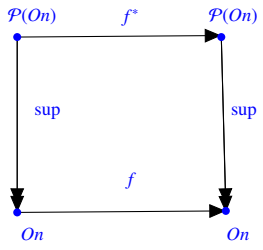
1.5 Normal Functions, fixed Points, and the Division Algorithm

DEFINITION 10 *Normal Functions*

A total function $f : On \to On$ is **normal** *if it is total, strictly increasing and continuous.*

The range of a normal function is a **clubset** *"closed unbounded set"*

"continuous"? In what topology? The order topology. *Continuous* means that the following diagram commutes.



"f^*" is a nonce notation for the function $X \mapsto f``X$. I don't expect to use it again.

Addition, multiplication and exponentiation on the Right are normal. In fact all the Doner-Tarski functions are normal "in their second argument" Not on the Left!

1.5.1 The Division Algorithm

The following lemma is absolutely central.

LEMMA 3 *The Division Algorithm for Normal Functions.*
If $f : On \to On$ is normal, and α is any ordinal, then there is a unique β such that

$$f(\beta) \leq \alpha < f(\beta + 1).$$

Proof:
The β we want is $\sup\{\gamma : f(\gamma) \leq \alpha\}$. What is $f(\beta)$? By normality it must be $\sup\{f(\gamma) : f(\gamma) \leq \alpha\}$, which is clearly $\leq \alpha$. So β is not merely the *supremum* of $\{\gamma : f(\gamma) \leq \alpha\}$, it is actually the *largest element* of $\{\gamma : f(\gamma) \leq \alpha\}$. But then $f(\beta + 1)$ must be strictly greater than α. ■

The division algorithm holds out the promise of building systems of notations for ordinals. You can think of it as saying "Give me a normal function f and a target α, i can give you a best attempt at representing α in terms of f and smaller ordinals". To make progress you can try subtracting $f(\beta)$ from α, where β was maximal s.t. $f(\beta) \leq \alpha$. You hope that $\alpha - f(\beta) < \alpha$, co's in that case you will have made some progress. We will elaborate this into a rigorous technique in section 4.1.

1.5.2 The Fixed Point Theorem

THEOREM 5 *Let $f : On \to On$ be a normal function and α any ordinal.*
Then $\sup\{f^n\alpha : n \in \mathbb{N}\}$ is
(i) a fixed point for f and
(ii) the least such fixed point above α.

Proof:
For (i) $\sup\{f^n\alpha : n \in \mathbb{N}\}$ is a fixed point for f because f is continuous.

For (ii) we prove by induction on 'n' that $f^n(\alpha) \leq$ the least f-fixed point above α.

Clearly true for $n = 0$.

For the induction suppose $f^n(\alpha) \leq \sup\{f^k\alpha : k \in \mathbb{N}\}$.

Then, by monotonicity of f, we have

$$f^{n+1}(\alpha) \leq f(\sup\{f^n\alpha : n \in \mathbb{N}\}) = \sup\{f^n\alpha : n \in \mathbb{N}\}.$$

■

This theorem is incredibly fruitful. The fact that every ordinal has a fixed point above it tells us that any normal function f has arbitrarily late fixed points. By normality of f we know that a limit of fixed points of f is another fixed point, so the function that enumerates those fixed points is itself normal. This function is sometimes called the *derivative* of f. This is elementary but incredibly important.

1.6 Some examples of ordinals that aren't too big

It would be nice to have natural examples of well-orderings of lengths other than ω. The fact that every ordinal is the order type of the ordinals below it means that for any ordinal there is a canonical wellordering of that length. Altho' this is an important fact it isn't much help to the beginner who is trying to get a sense of what particular individual ordinals look like – as it might be ω^2. Being told that ω^2 is the order type of the ordinals below ω^2 isn't much help. Fortunately ω^2 does have some natural manifestations: $\mathbb{N} \times \mathbb{N}$ ordered lexicographically is of length ω^2. And – in general – $\mathbb{N}^n$ ordered lexicographically, is of length ω^n. We can well-order the set of all finite lists of natural numbers to a longer length than this by a variant of the lexicographic ordering, but the definition is forgettable because of complications that have to do with deciding how to compare lists of different lengths. In some ways a simpler way to present these ordinals is through well-orderings of polynomials by dominance.

DEFINITION 11 *f* **dominates** *g if, for all sufficiently large n, $f(n) > g(n)$.*

Consider polynomials in one variable with coefficients in $\mathbb{N}$– Specifically the quadratics $x \mapsto (ax^2 + bx + c)$ – and order them by dominance. It is fairly clear that $x \mapsto (ax^2 + bx + c)$ is dominated by $x \mapsto (a'x^2 + b'x + c')$ iff $\langle a, b, c\rangle$ comes below $\langle a', b', c'\rangle$ in the lexicographic order of $\mathbb{N} \times \mathbb{N} \times \mathbb{N}$. So the set of quadratics, ordered by dominance, is of length ω^3. In fact, the analogue of this holds for polynomials of higher degree as well: the set of polynomials of degree n, ordered by dominance, is of length ω^{n+1}. One way of seeing this is to replace, in each polynomial, every occurrence of 'x' by 'ω'. Finally, the set $\mathbb{N}[x]$ of all polynomials (ordered by dominance) will be of order $\omega + \omega^2 + \omega^3 \cdots + \omega^n \cdots$. What is this ordinal? Since $1 + \omega = \omega$ it follows that $1 + \omega$ copies of anything is the same length as ω copies of whatever it was, so in particular $\omega^n + \omega^{n+1} = \omega^{n+1}$. Given this, the sum is simply the sup of all these ordinals, which – by definition – is ω^ω. There is another way of seeing this, given the synthetic definition of ordinal exponentiation using functions of finite support. It is not hard to see a polynomial in one variable with coefficients in $\mathbb{N}$ as a function $\mathbb{N} \to \mathbb{N}$ of finite support.

Let us call this family $\mathbb{N}[X]$ of polynomials in one variable *the set of polynomials of rank 1* (to give it a name). Now consider the set of polynomials in one variable with coefficients in $\mathbb{N}$ whose exponents are polynomials of rank 1. (I suppose one might notate this $\mathbb{N}[\mathbb{N}[X]]$!). An example would be

$$x^{x^3+x} + x^{200} + 137 \cdot x^3.$$

These will be the polynomials of rank 2. If you order these by dominance you obtain a wellorder of length ω^{ω^ω}. Similarly an example of a polynomial of rank 3 would be

$$x^{x^{x^3+x}+4x} + x^{x^{50}} + x^{200} + 137 \cdot x^3.$$

If we wellorder by dominance the set of all polynomials in one variable of finite rank we find it is of length

$$\omega^\omega + \omega^{\omega^\omega} + \omega^{\omega^{\omega^\omega}} \ldots$$

which is the first fixed point for $\alpha \mapsto \omega^\alpha$, otherwise known as ϵ_0. Of which more later!

> However if we consider the somewhat larger inductively defined family of expressions that contains all the above functions and is closed under exponentiation, so it contains things like
>
> $$(x^{x^{x^9+3}+x^{x^2}+x^2+5} + x^{x^5+10})^{(x^{x^{x^9+3}+x^{x^2}+x^2+5}+x^{1000})}$$
>
> then it is far from obvious that the set of [the functions denoted by] these expressions is totally ordered by dominance, let alone *well-ordered* by dominance, but as it happens it is. The order-type has not been computed, tho' some bounds are known. See [21], [7] and [18].

1.7 Some worked exercises

This is material that we use on our third year students at Cambridge.

EXERCISE 4

1. *Write down subsets of* $\mathbb{R}$ *of order types* $\omega + \omega$, ω^2 *and* ω^3 *in the inherited order.*
2. *Let* α, β *and* γ *be ordinals.*

   If $\alpha \leq \beta$, *must we have* $\alpha + \gamma \leq \beta + \gamma$?
   If $\alpha < \beta$, *must we have* $\alpha + \gamma < \beta + \gamma$?
3. *Show that the inductive and synthetic definitions of ordinal multiplication agree.*
4. *Is there a non-zero ordinal* α *with* $\alpha\omega = \alpha$? *What about* $\omega\alpha = \alpha$?
5. *Let* α, β, γ *be ordinals.*

   Must we have $(\alpha + \beta)\gamma = \alpha\gamma + \beta\gamma$?
   Must we have $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$?
6. *Find two totally ordered sets such that neither is isomorphic to a subset of the other. Can you find three such sets?*
7. *Let* α, β *and* γ *be ordinals.*

   Must we have $\alpha^{\beta+\gamma} = \alpha^\beta \cdot \alpha^\gamma$?
   Must we have $\alpha^{\beta^\gamma} = \alpha^{\beta \cdot \gamma}$?
   Must we have $(\alpha \cdot \beta)^\gamma = \alpha^\gamma \cdot \beta^\gamma$?

1.8 Cofinality

We will need the concept of the **cofinality** of an ordinal.

DEFINITION 12 *The cofinality* $cf(\alpha)$ *of an ordinal* α *is the least ordinal that is the length of an unbounded subset of a wellordering of length* α.

Thus the cofinality of a successor ordinal is obviously 1. It's an interesting function only when applied to *limit* ordinals. Clearly $cf(\omega) = \omega$; $cf(\omega + \omega) = \omega \ldots$.

Let's start with a few banalities to orient ourselves.

> Do not expect $\alpha \mapsto cf(\alpha)$ to be monotone. This will become clear later.
>
> Think about $cf(\alpha \cdot \beta)$ ("β copies of α"). Place a red dot on the first element of each copy of α. If β is limit the red dots are a cofinal sequence, so $cf(\alpha \cdot \beta) \leq \beta$. As long as β is limit of course. If it's successor then the cofinality is $cf(\alpha)$.
>
> Notice that cf is **idempotent**: $cf(cf(\alpha)) = cf(\alpha)$. This is because "is an unbounded subsequence of" is transitive.

One reason why the concept of cofinality is unappealing to many maths students is that it doesn't seem to be doing anything: it doesn't seem to help in drawing useful distinctions. Most people have never seen any wellordering that isn't of cofinality ω, so cofinality isn't something they ever needed to think about. Let's illustrate this.

THEOREM 6 *Every countable limit ordinal is of cofinality ω.*

Proof:

Let α be a countable limit ordinal. Then there is a worder $<_\alpha$ of $\mathbb{N}$ of order type α. We now define a cofinal subsequence of $\langle \mathbb{N}, <_\alpha \rangle$ of length ω. The first point is 0. Thereafter the $n+1$th point is the smallest natural number which is $>_\alpha$ the nth point.

Why is this sequence cofinal? Suppose it reaches a limit below α. Consider a natural number above this limit. It must be below something (say the nth) in the list of points we have identified, since this list contains arbitrarily large natural numbers. But then, at that stage n, it was a better candidate to be the nth point than the point we actually chose. ■

My colleague Imre Leader calls this construction *picking winners*; it's a good name and we should use it. *Picking winners* enables us to show that cofinalities are always initial ordinals, as we shall see below when we meet initial ordinals in section 3.2.

It is very important that this construction of a cofinal sequence for α needs an extra input, namely the wellordering $<_\alpha$ of $\mathbb{N}$. If we vary the choice of wellordering we get a different cofinal sequence.

What one wants to say at this point is that there is no way, given an ordinal α, of computing a cofinal sequence of ordinals below α of minimal order type. The obstructing to stating this properly is that it is not at all clear what it would be to be "given" an ordinal. If you are a complexity theorist reading this (and my target audience certainly includes complexity theorists!) then you would think of a presentation of an ordinal as a finite object, a *notation* for an ordinal, in some pre-agreed system of notation. If that is what we mean by a presentation of an ordinal then yes, indeed, we can compute a cofinal sequence of minimal length. But that isn't quite what we mean here, since ordinals are not *prima facie* finite objects[6]. Suppose i give you an ordinal in the form

[6] See appendix 10.1.5 for a discussion of *finite object*.

of a concrete set equipped with a wellordering of that length? Even that is not enough. (A lot of work will have gone into setting up a system of notation, and – anyway – a finitary system of notation will capture only countably many countable ordinals, and there are uncountably many of the buggers.) Suppose i give you an ordinal in the form of a von-neumann ordinal – which is a highly concrete object, a *set* – can you compute such a sequence? I can find such a sequence (for a countable von neumann ordinal) by *picking winners* but in order to pick winners i have to have an enumeration of the set. The problem then is that there is no way of computing an enumeration of a countable set from a wellordering of it, even when given the extra information that the set is countable. Let's set this up in lights:

REMARK 1

• *There is no algorithm which, on being given a set equipped with a wellordering, plus the news that the set is countable, will output an enumeration of the set.*

• *There is no algorithm which, on being given a set equipped with a wellordering, will output a cofinal subsequence of that wellordering of minimal length.*

It's as well to ensure that you are happy about these limitations *now* beco's they will matter when we come later to think about *fundamental sequences*.

(An aside on this subject for people who want to do a bit of Set Theory....
Let $\langle X, <_X \rangle$ be a wellordering, living in some model that believes it to be uncountable. (For example, $\langle X, <_X \rangle$ might be a von Neumann ordinal). In a bigger model it might become countable. If there were an engine that could take a wellordering of X and return an enumeration of X then clearly it couldn't do it just by looking inside X, because then the smaller model would also be able to count X. This is what lies behind the fact that *inter alia* you need AC to set up a system of fundamental sequences for all countable limit ordinals.)

Chapter 2

Rank Functions, and some Applications

Consider a computer system for storing sensitive information like people's credit information, or criminal records, and suchlike. It is clearly of interest to the subjects of these files to know who is retrieving this information (and when and why), and there do exist systems in which each file on an individual has a pointer to another file which contains a list of the the userids of people accessing the head file, and dates of those accesses. One can even imagine people wishing to know who has accessed *this* information, and maybe even a few steps further. A well-designed system would be able to allocate space for new and later members of this sequence of files as new reads by users made this necessary. These files naturally invite numerical subscripts. The system controllers might wish to know how many files had been generated by these reads, and know how rapidly new files were being generated, or what statistical relations existed between the number of reads at each level. This information would have to be stored in a file too, and the obvious subscript to give this file is ω. (It wouldn't be sensible to label it 'n', for n finite (even if large) because there is always in principle the possibility that we might generate more than n levels of data files.) Then we start all over again, with a file of userids and dates of people who have accessed the ωth file. Thus we can imagine a system where *even though there are only finitely many files* some of those files naturally have transfinite ordinals as subscripts[1].

DEFINITION 13 *If $\langle X, R\rangle$ and $\langle Y, S\rangle$ are two wellfounded binary structures then $f : X \to Y$ is* **parsimonious** *if, for all $x \in X$, $f(x)$ is an S-minimal y in Y such that $(\forall x'\, R\, x)(f(x')\, S\, y)$.*

[1] You might be thinking: "all we need for the labels is that they come from a dense ordering, like the rationals, so that we can always insert a new file if needed. So why can't we use the rationals? Yes, you can use the rationals. However, since at each stage there is no *least* rational that is suitable, your choice of rational conveys no information to any observer of your activities. You could have labelled your files 0, 1/2, 3/4, 7/8 ... 1. But you could equally well have labelled them with a sequence ending at 2. If you use ordinals then your choice of ω is forced. If you use ordinals then at each stage there is a least ordinal that is suitable, and that ordinal conveys information.

I think the ordinals are a terminal object in the category of wellfounded structures and parsimonious maps.

DEFINITION 14 Rank functions for wellfounded (binary) structures

If $\langle X, R\rangle$ is a wellfounded binary structure we define:

$$\rho(x) = \mathtt{sup}\{\rho(y) + 1 : R(y, x)\}.$$

(The intention is that $\rho(x)$ shall be the least ordinal bigger than all the $\rho(y)$ for y Related to x.)

XS

LEMMA 4 *Rank function is uniquely defined.*

Proof: By coroll 1.2.1. ■

The word 'least' in the above definition ensures that rank functions are parsimonious. Why do we want rank functions to be parsimonious? Because we want the rank of a structure to be a measure of its complexity. The more complicated a structure is, the bigger will be the *smallest* ordinal we can use to encompass its complexity.

> Sometimes we are interested in finding maps that are *not* parsimonious maps, maps that in contrast use as many ordinals as they can, subject to the constraint that the range of the map is an initial segment of the ordinals. The more ordinals we use to describe a structure, the more features we can highlight. This happens in WQO theory. But that's for another day.

So every wellfounded structure has a homomorphism onto an initial segment of *On*. There is a converse of sorts: If there is a homomorphism $h : X \to On$ defined on a binary structure $\langle X, R\rangle$ satisfying $x\,R\,y \to h(x) < h(y)$ then R is wellfounded. This can sometimes be a useful way of showing that a relation is wellfounded.

EXERCISE 5 *Let $\langle X, R\rangle$ be a wellfounded binary structure, with rank function ρ.*
Prove that

$$(\forall x \in X)(\forall \alpha < \rho(x))(\exists y \in X)(\rho(y) = \alpha).$$

You're obviously going to do this by induction; but is it by induction on R or on $<_{On}$?

The point of this exercise is to highlight the parsimonious nature of rank functions. If $\rho(x) = \alpha$ that's beco's all the ordinals below α have been used to decorate things that are below x in the sense of R. The range of a rank function is always an initial segment of *On*: no ordinal missed out – no holes!

Here is a live application of rank functions.

The game of **Sylver Coinage** (you can google it: there is stuff about it on the web, tho' i think it is first in *Winning Ways*[5]) is played between the mintmaster and the mintmaster's assistant. They take turns announcing a positive integer, which is to be the denomination of a new coin. There is a restriction that says that when your turn comes to announce a denomination, you may not announce a number that is a sum of numbers already announced. So for example, if the first two numbers announced are 10 and 15 you are not allowed to say 20 or 25 and so on, though you may say 5. 5

is a linear combination of 10 and 15 but it's not a sum of positive integer multiples of numbers already announced. The last player who is able to move loses.

One's first thought is that a play of this game might go on for ever, but interestingly this is not the case: all plays are finite. I use this as a take-home exercise for my first-year Compsci students (at least the better ones) beco's it's a good thing for them to think about. However we are in a hurry, so i shall cut to the chase. Here's why every play is finite.

Suppose it is your turn to move. What numbers are available to you? Anything that is not a sum of positive multiples of numbers already played. Here we need the key fact that *every sufficiently large multiple of the HCF of numbers already played is unavailable.* For example, suppose two numbers have been played so far, and they are 50 and 40. The HCF of 50 and 40 is 10. You can play 10, you can play 20, you can play 30, 60 or 70 or even 110, but every multiple of 10 from 150 onwards is of the form $40x + 50y$ with x and y positive integers. *There are only finitely many multiples of the HCF-of-the-numbers-already-played that are available to you.* So *either* (i) you play one of those numbers *or* (ii) you play something that is not a multiple of of 10. In case (i) you reduce by 1 the number of multiples-of-the-HCF-that-are-available, and in case (ii) you make smaller the HCF-of-numbers-so-far played. If you think about this for a bit you will convince yourself that every play must come to an end.

This suggests a parameter for describing a state of the game. The parameter is the ordered pair of (i) the HCF of the numbers played so far with (ii) the number of multiples of that HCF that are available. This parameter is important because whenever you make a move you *either* make the second component smaller while leaving the first unchanged, or you decrement the first component.

When you decrement the first component the second component might get bigger. For example, in the case we considered, where the first two numbers were 40 and 50, the first component is 10 and the second component is (i think, you may wish to check it) 6. If i now play – say – 75, the HCF drops to 5, but the number of multiples of the new HCF that is available is now much more than 6.

The set of these ordered pairs has a wellordering. Every descending sequence in this ordering is finite. That is why every play of this game must end.

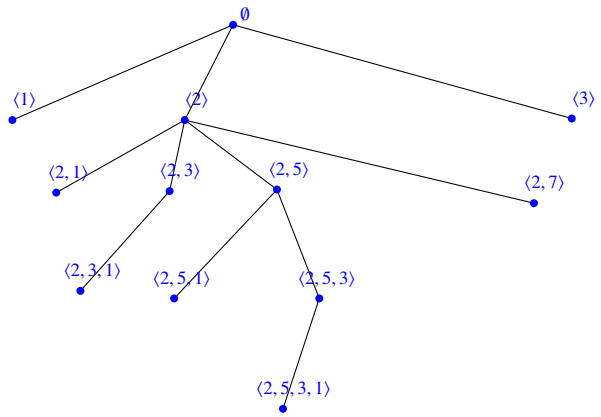
Can we straightforwardly identify a position in a play of this game with one of these ordered pairs? Depends what you are trying to do. Properly speaking a position in the game is a finite set of natural numbers, namely the set of numbers played so far. If all you know is the HCF of the numbers played so far you don't know which multiples of the HCF are available so it's best to think of the ordered pair not literally as a position in the game, but a parameter that contains most of the information that matters.

This wellordering is actually the "lexicographic ordering" on pairs of naturals. And, since it is a wellordering, it has a length. The length (you can check this) is ω^2. And not only that. Any position in this game can be thought of as an ordered pair, a thing in this wellordering, and this gives us a measure of the complexity of that position, which is the ordinal length of the set of positions that are below that position in the ordering. Let me illustrate, beco's this probably sounds a bit scary. Suppose the first two moves were 10 and 6, so we are in the position $\langle 2, 4\rangle$. 2 is the first component beco's 2 is the HCF of 6 and 10. Why 4 for the second component? Because there

are 4 multiples of the HCF that are available, namely 2, 4, 8 and 14. The positions that are below this are: any ordered pair whose first component is 1, plus the four pairs $\langle 2,3\rangle$, $\langle 2,2\rangle$, $\langle 2,1\rangle$ and $\langle 2,0\rangle$. This set of positions is wellordered by the lexicographic order and is of length $\omega + 4$. So the ordinal $\omega + 4$ is in some sense a measure of the complexity of the position $\langle 2,4\rangle$, in that it says something about the wealth (or dearth) of positions that can be reached from $\langle 2,4\rangle$. The pleasing part of this is that although the position $\langle 2,4\rangle$ is in some sense a well-behaved finite object, it points to an infinite set of possibilities, and this set of possibilities is indicated by an *infinite* ordinal.

Here is another slightly different treatment of the same game. We can think of a position in the game as a finite sequence of numbers, specifically the sequence of numbers played up to that point. So: let us consider the set of those finite sequences of numbers that can arise in the course of a play of this game. We put the empty set at the top of the page, and immediately below it all the singleton sequences $\langle 1\rangle$, $\langle 2\rangle$, $\langle 3\rangle$, and so on. We don't put anything below $\langle 1\rangle$, beco's that's an endpoint, beco's the game has ended. What goes below $\langle 2\rangle$? $\langle 2,1\rangle$ does, and that's also an endpoint. $\langle 2,3\rangle$ also goes below $\langle 2\rangle$, and $\langle 2,3\rangle$, is not an endpoint, tho' there is only one thing below it, namely $\langle 2,3,1\rangle$ (co's 1 is the only legal move in reply to $\langle 2,3\rangle$ and that's an endpoint). $\langle 2,3,4\rangle$ is not a legal move, so the next thing to the right of $\langle 2,3\rangle$ is $\langle 2,5\rangle$. In that position one can play 1, which takes one to the endpoint $\langle 2,5,1\rangle$, or 3 taking one to $\langle 2,5,3\rangle$. Then there is only one legal move – namely 1 – and it takes us to the endpoint $\langle 2,5,3,1\rangle$.

This is illustrated below.



So far, no ordinals. We can decorate this picture (remember, the whole picture is infinite, so i have drawn only an infinitesimal part of it) with ordinals as follows. Decorate the endpoints with 0. Thereafter recursively decorate each node with the least ordinal that is bigger than all the decorations on the nodes below it. Thus all the tuples with 1 as their last element get decorated with 0; $\langle 2,3\rangle$ and $\langle 2,5,3\rangle$ get decorated with 1; $\langle 2,5\rangle$ get decorated with 2. To see what $\langle 2,7\rangle$ gets decorated with one would have to draw the part of the picture below it... which i have omitted. I think it gets 3, and $\langle 2,9\rangle$ gets 4. In fact $\langle 2,2n+1\rangle$ gets n. Then $\langle 2\rangle$ gets ω!

This process of decorating-with-ordinals all the elements in a partial ordering in this way is a perfectly standard manœuvre, and the decorations are called *ranks*. It

works as long as all descending sequences eventually hit an endpoint.

OK, so what is there about the position $\langle 2 \rangle$ that justifies this infinite label? Any play from $\langle 2 \rangle$ is of only finite length of course. The point is that there is no finite bound on the length of plays from this position: you can spin it out for as long as you like. You have to pick an odd number of course, and if you pick $2n + 1$ the game can last for n further moves. Once you play your odd number the possible length of the subsequent play suddenly becomes finite. There is no response to 2 which leaves you in a position with the character that the position $\langle 2 \rangle$ has, namely that there is no finite bound on the length of feasible plays from that position.

Now consider the position $\langle 4 \rangle$. I can play an odd number, at which point the possible lengths of subsequent games suddenly gets a finite bound. However, if i play any number of the form $2n + 2$ i find the game in a position where the other player has infinitely many choices, just as he did in the position $\langle 2 \rangle$. Hence the larger rank.

There are other applications of rank functions which are more consequential, and we will see some in chapter 5. That was just a taster.

Chapter 3

Generalities about possibly uncountable ordinals

3.1 Hartogs' Lemma

ω is a *countable ordinal*. Observe that $\omega + 1$, ω^2 and lots of other ordinals are also countable. Are *all* ordinals perhaps countable . . . ? No!

The answer is 'no', and you might think that it is *obvious* that the answer is no. After all, $\mathbb{R}$ is uncountable, and – if we believe the axiom of choice – then we can wellorder $\mathbb{R}$ and no ordinal of such a wellordering can be countable. But we can give a more direct and informative proof without using AC.

THEOREM 7 *Hartogs' Lemma.*
For every set X there is a wellordered set Y s.t. $Y \not\hookrightarrow X$.

Proof:

We exhibit a uniform construction of such a Y.

Consider $\mathcal{P}(X \times X)$. This is the set of all binary relations on X. We define a map $f : \mathcal{P}(X \times X) \to On$. If $R \in \mathcal{P}(X \times X)$ is a wellordering we send it to its order type, its length; if it is not a wellordering we send it to 0. The range f"$(\mathcal{P}(X \times X))$ of f is the set Y that we want.

Y is naturally wellordered, being a set of ordinals, so what is its order-type in this ordering? Y is *downward-closed* so, by theorem 4 its order-type is the least ordinal not in Y. The ordinals in Y are precisely the ordinals of wellorderings of subsets of X. So the order type of Y is the least ordinal not the length of a wellordering of any subset of X. So Y is not the same size as any subset of X. *It's too big.*

■

A word is in order at this point about the *meaning* of Hartogs' lemma. Recall that ordinals are the kind of number that measures the lengths of discrete, deterministic transfinite processes. Suppose you are trying to construct something by a transfinite process. The tower of Babel, perhaps. The stages of your construction are indexed by

ordinals. In principle you might be worried that the process could be so complicated that there aren't enough ordinals for the process to complete. Hartogs' lemma lays this worry to rest. It doesn't guarantee that all discrete deterministic processes complete successfully, but it does tell you that if your process goes wrong it's not beco's you have run out of ordinals.

An aside about notation. The cardinality of the set Y that we obtain from X in the above proof is notated '$\aleph(|X|)$', but beware! That notation is for for the **cardinal** $|Y|$ of the Y thus obtained, *not* for the ordinal of the obvious wellordering of Y. This function is sometimes called 'Hartogs' aleph function'. Do not confuse this notation with the notation (which we will see later) that gives subscripts to alephs: $\aleph_0$ is not $\aleph(0)$! However we will not make much use of this notation here, and i mention it only for the sake of completeness.

It's natural to ask specifically what happens if we do the construction of theorem 7 in the particular case where $X = \mathbb{N}$. The answer is that we get the set of countable ordinals, a set that Cantor called the *second number class*. We need a name for the cardinal of this set: $\aleph_1$. The supremum of the second number class is the ordinal ω_1, the least uncountable ordinal..

It's worth spelling this out and thinking about it.

Start with the set $\mathbb{N}$ of natural numbers, the first number class. Its members are canonically ordered (wellordered indeed) by magnitude, to length ω, and there are $\aleph_0$ of them.

Now pick up your magic Hartogs' hammer. Consider the set of all wellorderings of subsets of $\mathbb{N}$, and take the quotient under orderisomorphism. The result is a set of ordinals. This set is the **second number class**. Its order type (which of course is the same as the first ordinal not in it, by thm 4) is called ω_1 and its cardinality is $\aleph_1$.

Of course you can repeat the trick, and obtain yet more ordinals, what one might (but doesn't) call the *third number class*, whose order type (and whose supremum) will be ω_2 and whose cardinality is $\aleph_2$.

And $\aleph_3$, $\aleph_4$, and so on . . . (!)

Do not panic if these last paragraphs look unintuitive. *You have almost certainly never seen a set of size $\aleph_1$ or $\aleph_2$ before.* I agree that it looks weird, but that's only beco's it is unfamiliar.

DEFINITION 15

(i) An aleph is the cardinality of an infinite wellordered set;
(ii) $\aleph(\alpha)$, for α a cardinal, is the least aleph $\not\leq \alpha$.

I know i said we wouldn't be doing any set theory here, but it may be worth pointing out – since people do worry about these things – that one can prove Hartogs' Lemma (lemma 7) *without* any use of the axiom scheme of replacement (as Hartogs in fact originally did, the axiom scheme of replacement not having been formulated at that stage).

It goes as follows.

Given X we seek a wellordered set Y with $|Y| \not\leq |X|$.

Consider $\mathcal{P}(X \times X)$ (use Wiener-Kuratowski ordered pairs if you want to be specific); throw away every subset that isn't a wellordering; quotient out what's left under isomorphism. The result is (a *concretisation* of) the set of ordinals of wellorderings of subsets of X – as it were equivalence-classes-local-to-X – and is the Y we desire.

This argument gives us an upper bound for $\aleph(|X|)$: $\aleph(\alpha) \leq 2^{2^{\alpha^2}}$. By modifying the construction you can obtain better bounds (such as $\aleph(\alpha) \leq^* 2^{\alpha^2}$ – where the asterisk means surjection) but we don't need them.

3.2 Initial Ordinals

For the moment write 'card(α)' for $|\{\beta : \beta <_{On} \alpha\}|$. (This 'card' notation is in the literature, but it is not in common use, and you do not need to know it). Then

DEFINITION 16
An ordering[1] *whose carrier set is of size κ is said to be κ-***like** *if every proper initial segment has size $< \kappa$.*

An ordinal α is **initial** *if it is the order-type of a κ-like wellordering:*

$$(\forall \beta <_{On} \alpha)(card(\beta) <_{card} card(\alpha)).$$

The set of orderings-whose-order-type-is-initial is a subset of On and is therefore wellordered in the inherited ordering.

We enumerate the initial ordinals as ω_0, ω_1, $\ldots \omega_\alpha \ldots$, and

We define $\aleph_\alpha$ to be $card(\omega_\alpha)$ which of course was $|\{\beta : \beta <_{On} \omega_\alpha\}|$.

Thus every finite ordinal is initial and (more to the point) ω is initial – while $\omega + \omega$ isn't.

The following should be evident:

- $\aleph_\alpha$ is also the αth aleph;
- $\aleph_{\alpha+1}$ is $\aleph(\aleph_\alpha)$;
- The alephs are wellordered by $<_{card}$.

Notice the overloading of '$\aleph$'. Most vexing!

This notation is legitimate because, if X is wellorderable, the Y that we obtain from the construction in the proof of theorem 7 is of minimal size $\not\leq |X|$. So, if $|X|$ is the αth $\aleph$, $|Y|$ is the $(\alpha+1)$-th aleph. Is this OK? Yes: each aleph corresponds to a unique initial ordinal, so – by theorem 3 – the alephs are wellordered by $<_{card}$, so we can enumerate them using ordinals.

[You can skip this next paragraph if you don't want to get embroiled in set theory]

We can use initial ordinals to implement alephs as sets. Every aleph corresponds to a unique initial ordinal, so we can implement an aleph as the corresponding (von Neumann) initial ordinal. If we are willing to adopt AC then every cardinal is an aleph,

[1] The definition works for all orderings, tho' here we will be concerned only with wellorderings.

and we have in fact thereby implemented all cardinals. Could we not have implemented cardinals by Scott's trick (if you know what that is)? Yes, if we have foundation, or even if we have the (weaker) assertion that every set is the same size as a wellfounded set. This route *via* von Neumann initial ordinals doesn't need either of these assumptions, but it does use AC.

However it is blindingly cute, and has become the industry standard.

DEFINITION 17 *If $\alpha = cf(\alpha)$ we say α is* **regular***; otherwise* **singular**.

This terminology comes from Topology (The ordinals can be given the order topology).

COROLLARY 4 *Every regular ordinal is initial.*

Proof:

Suppose $cf(\alpha) = \alpha$ and that $\langle A <_A \rangle$ is a wellordering of order type α. Now if α were not initial there would be a subset $A' \subset A$ which was an initial segment A' of $\langle A, <_A \rangle$ and a bijection $\pi : A \longleftrightarrow A'$ (not order-preserving!). We use π and "picking winners" to inject A' cofinally into A. But the image of A' under this embedding is of order type *less than* α, contradicting $cf(\alpha) = \alpha$.

■

REMARK 2 *Every countable limit ordinal λ is the sup of an ω-sequence $\langle \lambda_i : i < \omega \rangle$ of smaller ordinals.*

Proof:

The picture shows why every countable limit ordinal has cofinality ω. The long right-pointing arrow represents a countable ordinal manifested as a wellordering of naturals ($\mathbb{N}$ in a funny order). The (unbounded!) increasing sequence of natural numbers reading from the left are the numbers chosen as in the picking-winners recursion ... 1001 is the least natural number > 257 that is above 257 in both orders. The semicircle represesents where this increasing sequence of naturals comes to a halt, closes off. Are there any natural numbers in the region flagged by the question marks? Suppose there were – 347, say. OK, so what were doing declaring 1001 to be the 6th member of the sequence? We should have used 347!

■

DEFINITION 18
Such a sequence of smaller ordinals is a **fundamental sequence** *for λ.*

For many countable ordinals there is an obvious fundamental sequence: for ω the obvious fundamental sequence is the increasing sequence of finite ordinals, aka the identity function (tho' of course any increasing sequence of naturals will do). $\omega + \omega$ has the obvious fundamental sequence $\langle \omega + n : n < \omega \rangle$; for ω^2 we obviously reach for $\langle \omega \cdot n : n < \omega \rangle$, for ω^ω we want $\langle \omega^n : n < \omega \rangle$. For ϵ_0 we want the sequence ω, ω^ω, ω^{ω^ω}, $\omega^{\omega^{\omega^\omega}}$ .... However, in general there is no 'obvious' fundamental sequence for an arbitrary countable ordinal. This fact is not obvious, but it is one of the many consequences of remark 1

We will equivocate harmlessly between thinking of fundamental sequences as wellorderings and thinking of them as strictly increasing functions from $\mathbb{N}$ into the set of countable limit ordinals.[2]

We have seen that all countable limit ordinals have cofinality ω. Can a limit ordinal have any other cofinality? Might all limit ordinals have cofinality ω? It turns out that the answer is 'no' – at least if we have the axiom of choice.

REMARK 3 *(AC)*
$cf(\omega_1) = \omega_1$.

Proof:

Suppose not, and let $\langle X, < \rangle$ be a wellordering of length ω_1 with $x_1 < x_2 < x_3 \ldots < x_\beta < \alpha$ a cofinal subsequence of length α with α countable.. Then if we let $X_\beta =: \{x \in X : x_\beta \leq x < x_{\beta+1}\}$ then all the X_β are countable (ω_1 is the least uncountable ordinal after all) so $\{X_\beta : \beta < \alpha\}$ is a partition of the uncountable set X into countably many countable pieces. Countable choice tells us that a union of countably many countable sets is countable. So X would have to be countable, contradicting assumption. ■

(and yes, X here could be taken to be the second number class).

Quite what happens if we do not have AC is a complicated question which we cannot treat here.

EXERCISE 6 *Show that $\omega^{\omega_1} = \omega_1$.*
Is ω_1 the least ordinal α such that $\omega^\alpha = \alpha$?
[You may use standard facts about ordinal arithmetic.]

Something to think about ... every regular ordinal is initial ... is every initial ordinal regular...? Also ... the fixed point theorem 5 tells us that every normal function has arbitrarily late fixed points. However the proof given only supplies fixed points of cofinality ω. Might it be the case that every normal function has a regular fixed point...?

[2] There is an opening here for a little sermon whose burden is that our need to equivocate about this reveals that we haven't really got our data structures right (cf page 100).

3.3 $\aleph^2 = \aleph$

This section heading is a shorthand. We say a cardinal $|X|$ is *idempotent* if $|X| = |X \times X|$. Clearly if $|X| = |X \times X|$ then X is either empty or a singleton or is infinite. An aleph is the cardinal of an infinite wellordered set. The claim is that every aleph is idempotent. In the heading we are using the letter '$\aleph$' as a variable to range over alephs....

We start by noting that $\aleph = \aleph + \aleph$. (Well, what we will *actually* need is $\aleph + \aleph + \aleph = \aleph$, but never mind). Beginners might like to have this spelled out, and it holds because $2 \cdot \omega_\alpha = \omega_\alpha$. How so? Any order of limit order-type consists of lots of concatenated copies of $\mathbb{N}$, each of length ω. You can interleave two (or indeed three) worders of length ω to get a worder of length ω so you can do this for all the copies simultaneously.

We start by defining a function $\Im : On \to On$. Given an ordinal α, take a wellordering $\langle A, <_A \rangle$ of order type α, make disjoint copies of all its proper initial segments, and then concatenate the copies ... with longer things appended after shorter things.

The result is a wellordering and its order type is defined to be $\Im(\alpha)$. [This notation is not standard, and I am not going to use it outside this proof so i'm not numbering it]. Thus – for example – $\Im(\omega) = 1 + 2 + 3 + 4 + \ldots = \omega$.

[It occurs to me that you might be worried that an infinite wellordered sum of ordinals is not an ordinal, but it's quite easy to show that it is. Suppose i concatenate lots of (pairwise disjoint) wellorderings. Suppose there were a subset of the union with no least element. There must be a first summand that meets this bad subset. But then that summand wasn't a wellordering.

Another way of seeing it is to reflect that the sum – concatenation – of a host of wellorderings is the supremum of the partial sums. And we prove by induction on the partial sums that they are wellorderings. As long as the family of summands is wellordered of course!]

LEMMA 5

(i) $\Im : On \to On$ is a normal function;
(ii) Every initial ordinal is a value of $\Im$.

Proof:
(i) $\Im : On \to On$ evidently also has a recursive definition:

$\Im(\alpha + 1) = \Im(\alpha) + \alpha$ and
$\Im(\lambda) = \mathrm{Sup}\{\Im(\alpha) : \alpha < \lambda\}$ for λ limit.

... from which it is clear that $\Im$ is a normal function.

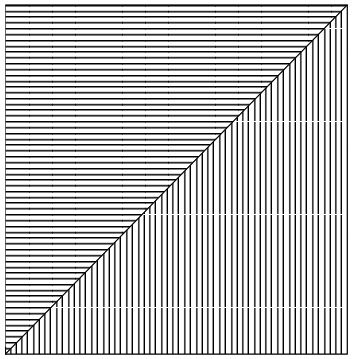
(ii)
Use the division algorithm for normal functions to show that there is a β s.t

$$\Im(\beta) \leq \omega_\alpha < \Im(\beta + 1).$$

If $\Im(\beta) < \omega_\alpha$ then we have $\omega_\alpha \leq \Im(\beta + 1) = \Im(\beta) + \beta$ which is impossible, since $\Im(\beta)$ and β both have cardinality below $\aleph_\alpha$. ■

We want to show that $(\aleph_\alpha)^2 = \aleph_\alpha$. Now $\aleph_\alpha$ is defined as the cardinal $|\{\beta : \beta < \omega_\alpha\}|$, which means that the canonical set of size $(\aleph_\alpha)^2$ is the cartesian product $\{\beta : \beta < \omega_\alpha\} \times \{\beta : \beta < \omega_\alpha\}$. We partition this last set into three pieces:

> (i) the [graph of] the identity relation restricted to $\{\beta : \beta < \alpha\}$, and
>
> (ii), (iii)
>
> the two triangles above-and-to-the-left, and below-and-to-the-right of the diagonal.



To be formal about it, we partition the cartesian product $\{\beta : \beta < \alpha\} \times \{\beta : \beta < \alpha\}$ into the three pieces $\{\langle\beta, \gamma\rangle : \beta < \gamma < \alpha\}$, $\{\langle\beta, \gamma\rangle : \beta = \gamma < \alpha\}$ and $\{\langle\beta, \gamma\rangle : \gamma < \beta < \alpha\}$.

It is clear that the third piece is of order type $\mathfrak{S}(\alpha)$ in the lexicographic order.

The idea is to show that these three pieces all have cardinality $\aleph_\alpha$. That's obvious for the second piece, the identity relation. Also there is an obvious bijection between the first and third piece ("flip your ordered pairs") so it will suffice to prove that the third piece ("the bottom-right triangle") has cardinality $\aleph_\alpha$.

Now we can prove

THEOREM 8 $(\forall\alpha)(\aleph_\alpha = (\aleph_\alpha)^2)$.

Proof:

By induction on α. The fact that it holds for $\alpha = 0$ you learnt in your first year.

Assume true for all alephs $< \aleph_\alpha$. By lemma 5, ω_α is a value of $\mathfrak{S}$; we want to show that it is actually a fixed point. Now ω_α is an initial ordinal, which is to say that for any $\beta < \omega_\alpha$, the cardinal $|\{\gamma : \gamma < \beta\}|$ is less than $\aleph_\alpha$, and (by induction hypthesis) is equal to its own square. Suppose ω_α were $\mathfrak{S}(\beta)$ for some $\beta < \omega_\alpha$. This would entail that the size of the cartesian product $\{\gamma : \gamma < \beta\} \times \{\gamma : \gamma < \beta\}$ is at least $\aleph_\alpha$, contradicting the induction. So ω_α is a fixed point of $\mathfrak{S}$. This means that the lower-right triangle of the cartesian product $\{\gamma : \gamma < \omega_\alpha\} \times \{\gamma : \gamma < \omega_\alpha\}$ – which can be wellordered to length $\mathfrak{S}(\omega_\alpha) = \omega_\alpha$ – is of cardinality $\aleph_\alpha$. It's clearly naturally isomorphic to the upper-left triangle (as remarked earlier) so the cartesian product is now a union of three sets each of size $\aleph_\alpha$, giving $(\aleph_\alpha)^2 = \aleph_\alpha + \aleph_\alpha + \aleph_\alpha = \aleph_\alpha$ as desired.

■

Thus if the axiom of choice holds (so every infinite cardinal is an aleph) then $\alpha = \alpha^2$ for all infinite cardinals. There is a converse, but since this is a pamphlet about ordinals not Set Theory I shall not prove it. We can also use theorem 8 to show that a lot of initial ordinals are regular.

THEOREM 9 *(uses AC)*
Every ordinal $\omega_{\alpha+1}$ is regular.

Proof:

If $\omega_{\alpha+1}$ is the sup of fewer than $\aleph_{\alpha+1}$ – which is to say the sup of no more than $\aleph_\alpha$ – smaller ordinals, then the set of ordinals below it (which is of size $\aleph_{\alpha+1}$) is a union of at most $\aleph_\alpha$ things each of size $\aleph_\alpha$ at most. We saw in an example sheet question[3] how to use AC to show that such a union is of size $(\aleph_\alpha)^2$ at most, and theorem 8 now tells us it is of size $\aleph_\alpha$ at most, which is impossible. ■

The obvious follow-up question is: if λ is limit can ω_λ be regular? It is if $\lambda = 0 \ldots$ The context in which to consider this question is the context of independence proofs, to which we turn later.

[3]Cambridge reference here

Chapter 4

Mainly concerning Countable Ordinals

4.1 Cantor's Normal Form Theorem

To prove Cantor's normal form theorem we will need to make frequent use of lemma 3, the division algorithm for normal function.

The way into Cantor Normal Forms is to think of that lemma as a rudimentary result of the kind "Given an ordinal β and a normal function f, $f(\alpha_0)$ is the best approximation to β from below that I can give using f." Cantor Normal form is an elaboration of this idea into a technique. Let us first minute a few normal functions to see what sort of things we can attack β with. For every $\alpha > 0$ the functions

$$\gamma \mapsto \alpha + \gamma; \qquad \gamma \mapsto \alpha \cdot \gamma; \qquad \gamma \mapsto \alpha^{\gamma}$$

are all normal, and each is obtained by iteration from the preceding one.

We are given β and we want to express it in terms of a given normal function. Let α be some random ordinal below β. Then $\gamma \mapsto \alpha^{\gamma}$ is a normal function and since $\alpha < \beta$ we know by lemma 3 that there is a largest γ such that $\alpha^{\gamma} \leq \beta$. Call this ordinal γ_0. Then $\alpha^{\gamma_0} \leq \beta$. If $\alpha^{\gamma_0} = \beta$ we stop there.

Now consider the case where $\alpha^{\gamma_0} < \beta$. By maximality of γ_0 we have

$$\alpha^{\gamma_0} < \beta < \alpha^{\gamma_0+1} = \alpha^{\gamma_0} \cdot \alpha \qquad (*)$$

We now attack β again, but this time not with the normal function $\gamma \mapsto \alpha^{\gamma}$ but the normal function $\theta \mapsto \alpha^{\gamma_0} \cdot \theta$. So by remark 3 there is a maximal θ such that $\alpha^{\gamma_0} \cdot \theta \leq \beta$. Call it θ_0. By (*) we must have $\theta_0 < \alpha$.

If $\alpha^{\gamma_0} \cdot \theta_0 = \beta$ we stop there, so suppose $\alpha^{\gamma_0} \cdot \theta_0 < \beta$, and in fact

$$\alpha^{\gamma_0} \cdot \theta_0 < \beta < \alpha^{\gamma_0} \cdot (\theta_0 + 1) = \alpha^{\gamma_0} \cdot \theta_0 + \alpha^{\gamma_0} \qquad (**)$$

by maximality of θ_0.

Now $\beta = \alpha^{\gamma_0} \cdot \theta_0 + \delta_0$ for some δ_0, and we know $\delta_0 < \alpha^{\gamma_0}$ because of (**).

What we have proved is that, given ordinals $\alpha < \beta$, we can express β as $\alpha^{\gamma_0} \cdot \theta_0 + \delta_0$ with γ_0 and θ_0 maximal. If $\delta_0 < \alpha$ we stop. However if $\delta_0 > \alpha$ we continue, by attacking δ_0 with the normal function $\gamma \mapsto \alpha^\gamma$.

What happens if we do this? We then have $\delta = \alpha^{\gamma_1} \cdot \theta_1 + \delta_1$, which is to say

$$\beta = \alpha^{\gamma_0} \cdot \theta_0 \ + \ \alpha^{\gamma_1} \cdot \theta_1 \ + \ \delta_1$$

One thing we can be sure of is that $\gamma_0 > \gamma_1$. This follows from the maximality of θ_0.

We now go back and repeat the process, this time with δ_1 and α rather than β and α.

Therefore, when we repeat the process we obtain:

$$\beta = \alpha^{\gamma_0} \cdot \theta_0 + \alpha^{\gamma_1} \cdot \theta_1 + \alpha^{\gamma_2} \cdot \theta_2 + \delta_3$$

and so on:

$$\beta = \alpha^{\gamma_0} \cdot \theta_0 + \alpha^{\gamma_1} \cdot \theta_1 + \alpha^{\gamma_2} \cdot \theta_2 + \ldots \alpha^{\gamma_n} \cdot \theta_n + \ldots$$

Now we do know that this process must terminate, because the sequence of ordinals $\{\gamma_0 > \gamma_1 > \gamma_2 > \ldots \gamma_n \ldots\}$ is a descending sequence of ordinals and must be finite, because $<_{On}$ is wellfounded.

So we have proved this:

THEOREM 10
For all $\alpha < \beta$ there are $\gamma_0 > \ldots > \gamma_n$ and $\theta_0 \ldots \theta_n$ with $\theta_i < \alpha$ for each i, such that

$$\beta = \alpha^{\gamma_0} \cdot \theta_0 \ + \ \alpha^{\gamma_1} \cdot \theta_1 \ + \ \alpha^{\gamma_2} \cdot \theta_2 \ + \ \ldots \alpha^{\gamma_n} \cdot \theta_n$$

■

[*HOLE We can also prove it by using only the first part of this proof, by extracting the largest power of α that is less than β and subtracting it – thereby obtaining something smaller – and appealing to induction. The point being that there is γ s.t. $\alpha^\gamma \leq \beta < \alpha^{\gamma+1}$, so the exponent of the largest power of α that is $< (\beta - \alpha^\gamma)$ is less than γ. So we claim that the CNF for β is $\alpha^\gamma +$ CNF for $\beta - \alpha^\gamma$, and – since $(\beta - \alpha^\gamma) < \beta$ – it has a CNF by induction hypothesis.*

In particular, if $\alpha = \omega$ all the θ_i are finite. Since every finite ordinal is a sum $1 + 1 + 1 + \ldots$ this means that every ordinal is a sum of a decreasing finite sequence of powers of ω.]

EXERCISE 7 *Use Cantor Normal Forms to show that every ordinal can be expressed as a sum of powers of 2.*

4.2 The Veblen Hierarchy

(*Veblen chores:*

Establish that every ordinal below Γ_0 has a normal form.

Establish that you can use those normal forms to equip all ordinals below Γ_0 with a

fundamental sequence
Establish that $\phi(\alpha, \beta)$ is ctbl if α and β are.

To find the normal form of θ find the last row that contains something below θ. θ then sits between the αth and the $\alpha + 1$th elements of that row. Record the αth. But the $\alpha + 1$th element is the sup of an ω-sequence starting at the αth (it's the next fixed point after all, and is acquired by iteration) so it lies between the nth and the $n + 1$th. Record n ...

)

Oswald Veblen came up with a system of notations for countable ordinals which takes Cantor Normal form as its point of departure. This happened really quite early on in the piece, and it is worth emphasising that the treatment of Veblen's happened at a time when there was an abstract theory of ordinals but before anyone had come up with a bundle of axioms for Set Theory. In fact Veblen's article and Zermelo's axioms appeared in the same year – 1908. The moral for us nowadays is that you can do a lot of ordinal arithmetic without actually doing any set theory.

Start with notations for 0, ω, $+$, $\cdot$ and exponentiation. The thought is that if we have a second-order constructor – `sup` – then we can reach all ordinals, but we are interested in first-order notations. Cantor Normal Form exploits those five bits of syntax and gives us notations for countably many ordinals, in fact an initial segment of the countable ordinals. How far does it take us? The first step ("look for the largest power of $\omega \leq$ your target) works for things that are not fixed points for $\alpha \mapsto \omega^\alpha$. Or rather, it works until we reach the least such fixed point. If we try it on things with such fixed points below them then the process of descent (as in: the computation of Cantor Normal Form) gets trapped at one of those fixed points. So we have to *do* something. We could add a constant term for this fixed point, and use that as the base for our exponentiation algorithm instead of ω. This new constant is written 'ϵ_0'.

The construction underlying the Cantor normal form theorem works for all ordinals, but we tend to reserve the expression for ordinals notated in this style where the base of the exponent is ω. This analysis is informative as long as the ordinal we are processing into normal form is less than the first fixed point for $\alpha \mapsto \omega^\alpha$, an ordinal that we commonly call 'ϵ_0'. If we apply the above algorithm to ϵ_0 we find that it has Cantor Normal form ω^{ϵ_0} which – admittedly – is true, but it is hardly informative, in the sense that it doesn't describe the target ordinal in terms of smaller ordinals. It will be helpful – in digesting the developments which are to come – to think of this as the CNF algorithm *crashing*. It is a deep and discouraging (or inspiring, depending on how you look at it) fact that any finitary system of notations for countable ordinals must crash; this is because a finitary system of notations can have only countably many wffs, and there are uncountably many countable ordinals queueing up to be notated. We need to embrace the fact that any system will crash, and try to form a picture of how the crashes happen: there is method in this madness.

CNF crashes at ϵ_0. Ok, so you pick yourself up, dust yourself off and start again building CNFs as tho' nothing had happened, the only difference being that this time you use ϵ_0 as the base of your exponentiation instead of ω.

That way you notate an ordinal α as a sum of terms of the form $(\epsilon_0)^{\beta_i} \cdot \gamma_i$ with $\gamma < \epsilon_0$ and $\beta_i < \alpha$. This works as long as $\alpha < {\epsilon_0}^\alpha$, so you go on until you reach an α

Rewrite this para

s.t. $\alpha = {\epsilon_0}^{\alpha}$. To the least such α we give the name ϵ_1. Whence cometh this notation? We've seen $\epsilon_0 \ldots$ The suspicious reader will have noticed that this ordinal ϵ_0 of which we discourse so airily has a notation with internal structure, specifically a numerical subscript, carrying the strong suggestion that there are other ϵ ordinals with names that have other subscripts – of which we have so far heard nothing.

> Connoisseurs of notation might notice that we have been writing 'ϵ_0' with a numerical *subscript*, rather than '$\epsilon(0)$' with the number as an *argument*, so that we think of ϵ as a function. Really we should think of ϵ as a function (tho' the notation will soon be superceded) so that $\epsilon(\alpha)$ is the αth fixed point for the (normal!) function $\beta \mapsto \omega^{\beta}$. Hang on to the fact that ϵ will be a normal function.

Thus we define ϵ_1 to be the first fixed point for $\beta \mapsto \omega^{\beta}$ above ϵ_0. However what will matter here is that it is also the smallest fixed point for $\beta \mapsto {\epsilon_0}^{\beta}$.

Let's quickly verify this.

$$ {\epsilon_0}^{\epsilon_1} = (\omega^{\epsilon_0})^{\epsilon_1} =^{(*)} \omega^{\epsilon_0 \cdot \epsilon_1} = \omega^{\epsilon_1} = \epsilon_1 $$

Might be an idea to check the equation marked with a (*). It's obviously true but it'll do no harm to write out a proof of the general case: $(\alpha^{\beta})^{\gamma} = \alpha^{\beta \cdot \gamma}$. (It would be a good currying exercise to do this for the synthetic definition.) And it might be an idea to check that analogous equations work for ϵ_2, ϵ_3 and so on.

$$ {\epsilon_\alpha}^{\epsilon_{\alpha+1}} = (\omega^{\epsilon_\alpha})^{\epsilon_{\alpha+1}} = \omega^{\epsilon_\alpha \cdot \epsilon_{\alpha+1}} = \omega^{\epsilon_{\alpha+1}} = \epsilon_{\alpha+1} $$

In fact, we can prove the more general

REMARK 4
For all α, $\epsilon_{\alpha+1}$ is the least fixed point for $\beta \mapsto (\epsilon_\alpha)^{\beta}$.

Proof:

First we check that it is, indeed, a fixed point.

$$ (\epsilon_\alpha)^{\epsilon_{\alpha+1}} = (\omega^{\epsilon_\alpha})^{\epsilon_{\alpha+1}} = \omega^{\epsilon_\alpha \cdot \epsilon_{\alpha+1}} = \omega^{\epsilon_{\alpha+1}} = \epsilon_{\alpha+1} $$

To show that it's the *least* we show that

$$ \epsilon_{\alpha+1} = \mathtt{sup}\{\epsilon_\alpha, {\epsilon_\alpha}^{\epsilon_\alpha}, {\epsilon_\alpha}^{{\epsilon_\alpha}^{\epsilon_\alpha}} \ldots\} $$

and then prove by induction on this sequence that all its members are $\leq_{On}$ the least fixed point.

■

Armed with this insight we can rethink CNF.

Bog standard CNF works for ordinals below ϵ_0. By using ϵ_0 as our base instead of ω we can notate ordinals below the least fixed point for $\alpha \mapsto {\epsilon_0}^{\alpha}$ which – as we have just seen – is ϵ_1. In doing so we have spiced up the syntactical base by adding the symbol 'ϵ_0'

By using ϵ_1 as our base instead of ω we can notate ordinals below the least fixed point for $\alpha \mapsto {\epsilon_1}^{\alpha}$ which – as we have just seen – is ϵ_2.

And so on!

Now we can notate ordinals below the least fixed-point ϵ-number, as follows. Suppose α is an ordinal less than the least fixed-point ϵ-number. Since the function ϵ that enumerates the ϵ numbers is normal there will be a largest ϵ-number below α. It will be ϵ_γ for some γ.

Now use ϵ_γ (which, remember, is the largest ϵ-number below α) as the base for your exponentiation in the version of CNF algorithm!

But how is this progress? It's progress as long as the trick launched by expressing α in terms of γ eventually terminates. We have given α a CNF description using a smaller ordinal ϵ_γ. This ϵ_γ is below the first fixed-point ϵ-number so $\gamma < \epsilon_\gamma$. And terminate it does, beco's the trick of giving α a CNF description using a smaller ordinal γ can be run again on the (smaller!) γ. So the process really does terminate.

In effect what this has done is to augment the notational apparatus with which we started (and which gave us Cantor Normal Form) by adding the function ϵ. As a result we have gone from a notation that worked for ordinals less than the first fixed point for $\alpha \mapsto \omega^\alpha$ to a notation that works for ordinals less than the first fixed point for $\alpha \mapsto \epsilon_\alpha$.

Now ask yourself: "where does this new system crash?". The answer is that it crashes at the first fixed-point for ϵ, the least α s.t. $\alpha = \epsilon(\alpha)$ – or $\alpha = \epsilon_\alpha$ if you prefer. Let us call this number κ_0. *It crashes at κ_0 in the sense that when we look for the largest ϵ-number $\leq \kappa_0$ we get... κ_0.*

Thus we are led to invent a function κ, that enumerates the fixed-point ϵ-numbers. I think there was a brief period in the development of this subject when these were called 'κ' numbers but it rapidly became obvious that we are going to have to go on forever inventing new notations in this way, so the best thing to do – rather than have lots of one-place functions – is to have a single two-place function, and this function symbol is 'ϕ'.

This move to having a two-place predicate instead of this indefinitely extensible family of one-place predicates is the key move in the erection of the Veblen hierarchy.

The derivation of a CNF for an ordinal relied heavily on the fact that $\alpha \mapsto \omega^\alpha$ is a normal function. If we are to use ϕ as a gadget for ordinal notation then we need $\alpha \mapsto \phi(\beta, \alpha)$ to be normal for every β. This may be hard work. A key fact in this connection is lemma 13 which states that the function that enumerates the fixed points of a normal function is itself normal. Anyway, once we've done that, how do we notate an ordinal α using ϕ? You look for the largest γ which is to the left of α in the row you are interested in, and get a CNF for α using γ as base for the exponent. Then all the ordinals that appear in the CNF are below α and you can notate them. So we need each row to be a clubset.

Something i felt it would be a good idea to write out a proper proof of is the fact that the least ordinal in the λth row of the Veblen diagram (λ limit) is the sup of the first ordinals in the rows above. It's elementary but it matters.

Let us write 'μ_α' for the least ordinal in the αth row. Fix λ limit, and consider $\{\mu_\alpha : \alpha < \lambda\}$ and then consider its sup. For $\beta < \lambda$ we reason as follows: $\sup(\{\mu_\alpha : \beta \leq \alpha < \lambda\}) = \sup(\{\mu_\alpha : \alpha < \lambda\})$, and each row is closed, so $\sup(\{\mu_\alpha : \alpha < \lambda\})$ belongs to every row, and is therefore in the λth row. Is that enuff to ensure that it is μ_λ? It bounds a whole lot of things all $\leq \mu_\lambda$ so it, too, is $\leq \mu_\lambda$. But it belongs to the λth row since it belongs to all higher rows, so it must genuinely *be* the least ordinal in that row.

So the function that enumerates the μ_α is normal and so has a fixed point. And on it goes.

The Veblen diagram

Top row is the stream of countable powers of ω. This is a clubset and the function that enumerates it is a normal function from the second number class into itself. Its order type is ω_1.

Thereafter we obtain the α + 1st row from the αth as the set of fixed points in the enumeration of the αth row.

At limits we take intersections. (At this point we really *really* need to think about diagonal intersections.)

"This is a clubset and the function that enumerates it is a normal function from the second number class into itself. Its order type is ω_1" – or at least we hope so! The quoted text is obviously to be desired, and we naturally aspire to prove it by induction on α.

Things we will need:

(i) The pointwise sup of a countable family of normal functions is normal.

(ii) Every row is unbounded. Ideally we also want: every row is of length ω_1

Actually (i) is not obvious. Such a sup is nondecreasing but might not be strictly increasing.

Chapter 5

Fundamental sequences and fast-growing functions

Fundamental sequences were introduced in definition 18 but no use was made of them there. The time has come to put them to work.

My point of departure here is an exercise that my friend and colleague Peter Johnstone used to give to the third-year logic students here at Cambridge: *prove that for every countable ordinal α there is a set of reals which is of order type α in the inherited order.*

There are [at least!] three ways of exhibiting a set of reals of order type α in the inherited order..

(i) Make α copies of $\mathbb{Q}$;
(ii) Embed α directly by picking a worder of $\mathbb{N}$ of length α and doing a "forth" construction.
(iii) A method using fundamental sequences which will explain below.

(i) runs as follows: Let α be an arbitrary countable linear order type (even! – it doesn't even have to be an ordinal). Concatenate α copies of $\langle \mathbb{Q}, 0\rangle$ (the rationals as an ordered set with a designated element.) This structure is a dense linear order with a family of designated constants forming a subset of order-type α. But the ordering formed by discarding the designated constants is a countable dense total order and is therefore isomorphic to the rationals. Therefore every countable linear order type embeds in the rationals. In particular, every countable ordinal embeds into the rationals and therefore into the reals.

More formally:

$\langle \mathbb{Q} \times \{\beta : \beta < \alpha\}\rangle$ ordered colex is a countable dense linear order and so there is an isomorphism $i : \langle \mathbb{Q} \times \{\beta : \beta < \alpha\}\rangle \longleftrightarrow \mathbb{Q}$ and now the function $\beta \mapsto i(\langle 0, \beta\rangle)$ injects $\{\beta : \beta < \alpha\}$ into $\mathbb{Q}$.

(ii) shares with (i) the feature that the construction does not require that α be an ordinal; any old countable linear order type will do. We will prove that if $\prec$ is any total order of $\mathbb{N}$ then $\langle \mathbb{N}, \prec\rangle$ can be isomorphically embedded into $\langle \mathbb{Q}, \leq_Q\rangle$. We construct

an embedding f by recursion on $\leq_{\mathbb{N}}$. Send 0 to 0; thereafter, when considering $n+1$, see how it is related by $\prec$ to the numbers $k \leq_{\mathbb{N}} n$. If it is above all those k then declare $f(n+1)$ to the the smallest whole number bigger than all the $f(k)$; If it is below all those k then declare $f(n+1)$ to the the negative integer with smallest absolute value $<_Q$ all the $f(k)$. If neither of these hold then it is $\prec$-sandwiched between two immediate neighbours $m \prec n+1 \prec m'$. Then we ordain that $f(n+1)$ = arithmetic mean of $f(m)$ and $f(m')$.

This embeds any countable linear order into $\mathbb{Q}$.

(iii) is the method using fundamental sequences. (Many students plump for this)

We will show how to construct, for arbitrarily large countable ordinals α, an order-preserving map f_α from the ordinals below α into $[0,\infty)$ – and i think we want the range of f_α to be unbounded whenever α is limit. Indeed we probably want the map to be continuous in the sense of the order topology on the ordinals. That is to say, if λ is a limit ordinal below α then $f_\alpha(\lambda)$ is the lub of f_α"$\{\beta : \beta < \lambda\}$. It's probably true that a nice enough construction will make this happen automatically, but it's something worth keeping an eye on.

The obvious candidate for f_ω is the ("casting") function that sends the ordinal number n to the real number n[1]. Thereafter we have two tricks we can use. If we have f_α we can construct $f_{\alpha\cdot\omega}$ by "squashing" the range of f_α down on $[0,1)$ by composing with $\frac{2}{\pi}\texttt{arctan}$ and then making copies to put in each interval $[n, n+1)$, and concatenating them. To be slightly less hand-wavy about it, let A_α be the range of f_α, then $f_{\alpha\cdot\omega}$ is the function that enumerates the points in

$$\bigcup_{n\in\mathbb{N}}(n + \frac{2}{\pi}\texttt{arctan}\text{"}A_\alpha)$$

(where the notation '$n + X$' of course denotes $\{n + x : x \in X\}$.) If α is an ordinal that cannot be reached by this method we find an increasing ω-sequence $\langle\alpha_n : n < \omega\rangle$ whose sup is α and compress the ranges of the f_{α_i} into the intervals $[i, i+1)$, thus:

$$\bigcup_{n\in\mathbb{N}}(n + \frac{2}{\pi}\texttt{arctan}\text{"}A_{\alpha_n})$$

Let us suppose that we have such a family $\langle f_\alpha : \alpha < \omega_1\rangle$. Fix a countable ordinal ζ and consider the ω_1-sequence $\langle f_\gamma(\zeta) : \gamma > \zeta\rangle$. It would be natural to expect this to be a non-increasing sequence of reals. After all, the more ordinals you squeeze into the domain of an f, the harder you have to press down on its values to fit all the arguments in. But you'd be wrong!

REMARK 5 *For each countable ordinal γ, the sequence $\langle f_\gamma(\zeta) : \gamma > \zeta\rangle$ is not monotone nonincreasing.*

Proof:

[1] I have the strong feeling that it's very important to **not** think of this function as the identity function. The real number 2 is not the same as the ordinal 2.

Suppose that

$$(\forall \gamma < \gamma' < \omega_1)(\forall \zeta < \omega_1)(f_\gamma(\zeta) \geq f_{\gamma'}(\zeta)). \tag{5.1}$$

Then, for each $\zeta < \omega_1$, the sequence $\langle f_\gamma(\zeta) : \gamma > \zeta \rangle$ of values given to ζ must be eventually constant. For if it is *not* eventually constant then it has $cf(\omega_1) = \omega_1$ decrements, and we would have a sequence of reals of length ω_1^* in the inherited order, and this is known to be impossible.

So there is an eventually constant value given to ζ, which we shall write '$f_\infty(\zeta)$'. But now we have $\alpha < \beta \rightarrow f_\infty(\alpha) < f_\infty(\beta)$. (We really do have '$<$' not merely '$\leq$' in the consequent: suppose $f_\infty(\alpha) = f_\infty(\beta)$ happened for some α and β; then for sufficiently large γ we would have $f_\gamma(\alpha) = f_\gamma(\beta)$ which is impossible because f_γ is injective). This means that f_∞ embeds the countable ordinals into $\mathbb{R}$ in an order-preserving way, and this is impossible for the same reasons.

So we conclude that the function $\langle \alpha, \beta \rangle \mapsto f_\alpha(\beta)$ is *not* reliably decreasing in its second argument.[2] ■[3]

So what can possibly have gone wrong? Surely any sensible allocation of maps to limit ordinals will be well-behaved in the sense that it obeys (5.1)? Let us step back a bit and introduce a new gadget, one which has been lurking in the background all along.

5.0.1 Fundamental sequences for ordinals below ϵ_0

Theorem 6 told us that every countable limit ordinal has cofinality ω. This is of course just the same as saying that every countable ordinal has a fundamental sequence.

I mentioned earlier (see definition 18 that for quite a lot of ordinals there is an "obvious" fundamental sequence for that ordinal. let's spell this out.

Fix an ordinal α and a wellordering of that length. Every $\beta < \alpha$ defines a terminal segment, and the lengths of these terminal segments decrease as β gets bigger, so there must be a least one. Clearly this 'tail' function $On \rightarrow On$ is idempotent and nonincreasing. What remains to be shown is that all its values are powers of ω. We do this by showing that if β is not a power of ω then $\text{tail}(\beta) < \beta$. If β is not a power of ω then it has a Cantor Normal Form $\omega^\gamma \cdot n + \delta$. If $\delta \neq 0$ then $\text{tail}(\beta) = \text{tail}(\delta) \leq \delta < \beta$. If $\delta = 0$ then $\text{tail}(\beta) = \text{tail}(\omega^\gamma) \leq \omega^\gamma < \omega^\gamma \cdot n = \beta$.

Next we characterise the "obvious" family of fundamental sequences for the ordinals below ϵ_0.

Every limit ordinal below ϵ_0 has a Cantor Normal Form $\gamma + \omega^\alpha$ for some α, where ω^α is its tail. (We might need to think of $\omega^\alpha \cdot n$ as $\omega^\alpha \cdot (n-1) + \omega^\alpha$ to secure this effect.) A fundamental sequence for $\gamma + \omega^\alpha$ can be obtained from a fundamental sequence $\langle \beta_n : n < \omega \rangle$ for ω^α, namely $\langle \gamma + \beta_n : n < \omega \rangle$ for ω^α. So to equip every limit ordinal $< \epsilon_0$ with a fundamental sequence it will suffice to to equip every ordinal $\omega^\alpha < \epsilon_0$ with a fundamental sequence.

[2] I suspect that the the sequence $\langle f_\gamma(\zeta) : \gamma > \zeta \rangle$ of values given to ζ describe a nonmeasurable set. I have seen no proof of this, tho'. We needed AC to build it so it might well be nonmeasurable.

[3] Is it the case that if we use a Schmidt-coherent family of fundamental sequences then bad behaviour of the f_ζs can be postponed as far as we like?

Now how do we allocate fundamental sequences to ordinals ω^α – that are powers of ω? If α has a fundamental sequence $\langle \alpha_n : n < \omega \rangle$ then $\langle \omega^{\alpha_n} : n < \omega \rangle$ will be a fundamental sequence for ω^α.

This preceding text defines a recursion which reduces the problem of finding a fundamental sequence for ω^α to that of finding such a sequence for α and – as long as there are no $\alpha = \omega^\alpha$ in the mix waiting to be encountered – will supply us with fundamental sequences for every limit ordinal, which is to say every limit ordinal below ϵ_0 – at least as long as we have one for ω. But the identity function on finite ordinals is the obvious fundamental sequence.[4] Had we taken a fancy to a different fundamental sequence for ω we would have ended up with a different family of fundamental sequences for ordinals below ϵ_0: the family is completely determined by what it does to finite ordinals.

DEFINITION 19
A **family** $\mathcal{F}$ *is a function sending each limit ordinal in some given initial segment of the second number class to a fundamental sequence for that ordinal.*

How do we obtain families of fundamental sequences? Suppose the order type of the limit ordinals below α is successor, so $\alpha = \beta + \omega$. In those circumstances the obvious choice for a fundamental sequence for α is $\langle \beta + n : n < \omega \rangle$. So far so good. Now suppose in contrast that the limit ordinals below α form a sequence of order type β for some limit ordinal $\beta < \alpha$. That is to say, there is a function g from $\{\zeta : \zeta < \beta\}$ to the set of limit ordinals below α. But if there is also a fundamental sequence f for β, then $g \cdot f$ will be a fundamental sequence for α.

This last step works as long as the order type of the set of limit ordinals below α is less than α. If it isn't then one has to do something slightly more clever. If we consider the ordinals that are fixed points for the function that enumerates the limit ordinals – which is the problematic case we have just identified – what might this clever thing be? The function that enumerates the limit ordinals is $\alpha \mapsto \omega \cdot \alpha$. Let's keep our feet on the ground for the moment by considering its first fixed point, which is ω^ω. A fixed point $\geq \alpha$ for a normal function f can be obtained as sup $\{f^n(\alpha) : n \in \mathbb{N}\}$. So ω^ω is immediately presented to us as the sup of $\{\omega^n : n \in \mathbb{N}\}$ and this gives us a fundamental sequence for ω^ω.

The hope is that there will always be some generalisation of this construction however far out we go. If F is a normal function $On \to On$ then whenever $\langle \beta_n : n \in \mathbb{N} \rangle$ is a fundamental sequence for β then $\langle F(\beta_n) : n \in \mathbb{N} \rangle$ is a fundamental sequence for $F(\beta)$. We will return to this later.

We have just seen how the construction of a fundamental sequence for β needs as input a bijection between $\mathbb{N}$ and the set of ordinals below β. In fact we can refine the proof of theorem 6 by exhibiting an algorithm that takes a bijection between $\mathbb{N}$ and the ordinals below β (or takes a wellordering of $\mathbb{N}$ of length β) and returns a family of fundamental sequences for limit ordinals below β. Similarly there is an algorithm that takes a family of fundamental sequences for the ordinals below β and returns a bjiecton between $\mathbb{N}$ and the set of ordinals below β. (Really one should say that this algorithm

[4] A sleeper for *dilators*.

accepts and outputs *notations* for these objects rather than the objects themselves. The notations are genuine finite objects and we can compute with them. A countable ordinal is not on the face of it a finite object: curiosity about how far one can go in thinking of countable ordinals as finite objects is the energy driving interest in the material in this tutorial.)

THEOREM 11
There is a natural map that takes a wellordering of $\mathbb{N}$ *of length* α *and returns a family of fundamental sequences for the limit ordinals below* α *– and vice versa.*

Proof:

This is a generalisation of theorem 6.

(i) *Left-to-right*

Suppose we have a wellordering $<_\alpha$ of the naturals to length α; let β be an arbitrary limit ordinal below α. We will find a sequence $\langle b_n : n \in \mathbb{N}\rangle$ of natural numbers which is of length ω according to $<_\alpha$, and whose sup in that order is the βth element of $\langle \mathbb{N}, <_\alpha\rangle$. We define b_0 to be the $<_{\mathbb{N}}$-least natural number in that unique initial segment of $\langle \mathbb{N}, <_\alpha\rangle$ that is of length β. Thereafter b_{n+1} is to be the $<_{\mathbb{N}}$-least natural number that belongs to that unique initial segment of $\langle \mathbb{N}, <_\alpha\rangle$ that is of length β and is $>_\alpha b_n$.

How do we know that the upper bound of this sequence is the βth element of $\langle \mathbb{N}, <_\alpha\rangle$? By construction the set $\{b_n : n \in \mathbb{N}\}$ is unbounded in $<_{\mathbb{N}}$. So if n is a natural number that lies above the $(\leq_\alpha)$-sup of $\{b_n : n \in \mathbb{N}\}$ but is still below the βth element then it is $<_{\mathbb{N}}$ terminally many of the b_n, and should have been chosen. Now we take β_n to be the length of the initial segment of $\langle \mathbb{N}, <_\alpha\rangle$ bounded by b_n.

Clearly we can do this simultaneously for all limit ordinals $\beta < \alpha$.

All i've exhibited so far is a natural construction of a fundamental sequence for α – not a family of fundamental sequences for all limits below β. However this is easy. For any $\gamma < \alpha$ consider the initial segment of $<_\alpha$ that is of length γ. This is a wellordering of a subset of $\mathbb{N}$ to length γ, and any infinite subset of $\mathbb{N}$ is naturally the same size as $\mathbb{N}$.

(ii) *Right-to-left*

We want to be able to construct a bijection between $\mathbb{N}$ and the ordinals below β on being given a family of fundamental sequences of limit ordinals below β.

The idea behind this proof is that the availability of fundamental sequences for limit ordinals below β enables us to give – in a uniform way – a finite description of any ordinal below β. Every infinite set of finite strings over a finite alphabet is demonstrably countable. Totally order the alphabet; then order the set of finite strings colex. It will be of length ω, as will any of its infinite subsets. So how do we get a finite notation for an arbitrary $\zeta < \beta$? Let $\{\beta_{0,n} : n \in \mathbb{N}\}$ be the fundamental sequence for β. Consider the first member of $\{\beta_{0,n} : n \in \mathbb{N}\}$ that is $\geq \zeta$. This is β_{0,n_0}, say. Record the n_0. `If` this β_n is actually equal to ζ `then HALT`, `else` step down from this ordinal to the last limit ordinal below it (which for the moment we will call 'α') and record the suffix 'i' such that it was $\beta_{0,i}$. (We don't need to record the decrement, and in any case if the fundamental sequence for α are sensible the α_i will be limit ordinals unless $\alpha = \omega \cdot (\gamma + n)$ for some $n < \omega$). Now let $\{\beta_{1,n} : n \in \mathbb{N}\}$ be the fundamental sequence for α. Consider the first member of $\{\beta_{1,n} : n \in \mathbb{N}\}$ that is $\geq \zeta$. `If` this $\beta_{1,n}$

is actually equal to ζ `then` record the n and `HALT`. `Else` step down from this ordinal to the last limit ordinal below it (which for the moment we will call 'α' as before) and record the suffix 'j' such that it was $\beta_{1,j}\ldots$(As before we do not need to record the decrement). Eventually we will find ourselves a finite distance above a point of a fundamental sequence and this time we do record the decrement.

I think this has become garbled and should be rewritten

By this procedure we build a sequence of natural numbers. This sequence is going to have to be finite if this construction is to be of any use to us. The reason why it will be finite is that the sequence of ordinals that were named 'α' at any stage of this process form a strictly descending sequence of ordinals and so must be finite.

So we have coded every ordinal below β by a finite string of symbols, and thence – using standard methods – by a natural number.

Perhaps we should explain how, with the help of this notation for ζ, we can navigate our way thither from 0. Given a sequence s for ζ we recover ζ as follows. First approximation is $\beta_{s(1)}$. Step down to the last limit ordinal below $\beta_{s(1)}$. Second approximation is the $s(2)$th member of the fundamental sequence for the last limit ordinal below $\beta_{s(1)}$. The last member of s (that is, $s(|S|)$) tells us what natural number to subtract from the approximation-in-hand.

To do this we think of the family as a set of ordered pairs $\langle s, s'\rangle$ of these finite sequences where (the ordinal notated by s) $<$ (the ordinal notated by s').

■

REMARK 6 *There is no definable family of fundamental sequences for all $\alpha < \omega_1$.*

Proof:

Let $\mathcal{F}$ be a family of fundamental sequences for all countable limit ordinals. We will show that $\mathcal{F}$ cannot be definable.

We define by recursion on the second number class a sequence $\langle W_\alpha : \alpha < \omega_1\rangle$ of wellorderings of $\mathbb{N}$ (so each is a subset of $\mathbb{N} \times \mathbb{N}$). We fix once for all a bijection $\mathbb{N} \times \mathbb{N} \longleftrightarrow \mathbb{N}$.

0 is easy; successor steps are easy; at a limit λ use the fundamental sequence $\mathcal{F}\lambda$, to get the codes $W_{\mathcal{F}\lambda n}$ you have already formed for each $\mathcal{F}\lambda n$ and then piece them all together one after the other to get a wellordering of $\mathbb{N} \times \mathbb{N}$. Use the bijection $\mathbb{N} \times \mathbb{N} \longleftrightarrow \mathbb{N}$ to turn this into a code for $\Sigma_{n\in\mathbb{N}}\mathcal{F}\lambda n$, which we will call λ'. Here we have to be careful, because the *sum* of a sequence of ordinals might be bigger than its *supremum*. What we want is a wellordering of $\mathbb{N}$ to the sup of this set of ordinals (which is λ) not its sum (which is λ'). Suppose $\lambda' > \lambda$. We delete from $\mathbb{N}$ those naturals that get sent to addresses after λ, and we delete ordered pairs containing them from the graph of the wellordering of $\mathbb{N}$ to length λ'. What's left is a wellordering of a proper subset $\mathbb{N}' \subset \mathbb{N}$ to length λ. But there is an obvious canonical bijection between $\mathbb{N}'$ and $\mathbb{N}$, and we can use it to copy the wellordering of $\mathbb{N}'$ over to a wellordering of $\mathbb{N}$ to length λ as desired. None of this uses any AC.

This shows that if we have a function $\mathcal{F}$ assigning a fundamental sequence to every countable limit ordinal, then we have a function assigning to each countable ordinal a wellordering of $\mathbb{N}\times\mathbb{N}$ of that length, and this new function can be defined in terms of $\mathcal{F}$. But (as we saw on page 23) any wellordering of $\mathbb{N}\times\mathbb{N}$ is coded by a real number so

the existence of the new function assigning a fundamental sequence to every countable ordinal implies $\aleph_1 \leq 2^{\aleph_0}$. It is known that this is independent of ZF.

This doesn't mean that there can be no family $\mathcal{F}$ of fundamental sequences for all countable limit ordinals, but it does mean that no such family can be definable; if it were, we would have an outright proof that $\aleph_1 \leq 2^{\aleph_0}$.

■

5.1 Fast-growing hierarchies

Our motive for considering fundamental sequences is that any family of fundamental sequences can be used to extend declarations of families of functions $\mathbb{N} \to \mathbb{N}$ into the transfinite in something like the following style.

The first person to spell out a fast-growing hierarchy seems to have been Hardy [15]. His idea was that if you could extend a fast-growing hierarchy out to all countable ordinals then you would have an injection of the second number class into the reals. As we have just seen, this hope is vain.

DEFINITION 20
Suppose $\mathcal{F}$ is a family in the sense of definition **??**. *Then we can declare*

$f_0^{\mathcal{F}}$ = *some function or other;*
$f_{\alpha+1}^{\mathcal{F}}$ =: *do something to* f_α*;*
$f_\lambda^{\mathcal{F}}(n) =: f_{(\mathcal{F}\ \lambda\ n)}(n)$.

(Typically we will omit the '$\mathcal{F}$' superscript).

> There is also the (apparently) minor detail that in the process of constructing the embeddings f_α from initial segments of the second number class into the reals we exploit representations of countable ordinals as *sums* of countably many smaller ordinals whereas in the definition of the fast-growing hierarchies we exploit fundamental sequences – which are representations of limit ordinals as *suprema* of ω-sequences of small ordinals. I don't think the difference matters, but one never knows.

Declarations in the style of definition 20 are typically used to generate families of functions where f_α dominates f_β whenever $\beta < \alpha$.

At successor stages this will be taken care of by the second clause and the purpose of the third clause is to ensure that f_λ dominates ("majorises") f_β with $\beta < \lambda$ for λ limit. Naturally one expects that if f_0 was strictly increasing then all the later f_α will be too – and that one will be able to prove this by transfinite induction. However to arrange for strict monotonicity of all the f_α it turns out one needs a condition on the family $\mathcal{F}$ of fundamental sequences which we will now investigate.

Stuff to fit in

Let $\mathcal{F}$ be a counted family of functions, equipped with $F : \mathbb{N} \to \mathcal{F}$. Then we can define a supremum f_∞ of $\mathcal{F}$ by

$$f_\infty(n) = sup\{(F\ j\ n) + 1 : j \leq n\}$$

We need this in the case where $\{\mathcal{F}\}$ is $\{f_\beta : \beta < \alpha\}$

5.1.1 Schmidt Coherence

Schmidt-coherent. Build a tree out of the predecessor relation. Fundamental sequences lie along branches of the tree. If $\alpha \leq_{\mathcal{F}} \beta$ then $f_\alpha(0) \leq f_\beta(0)$ and $(\forall n > 0)(f_\alpha(n) < f_\beta(n))$; if $\alpha \leq \beta$ then $(\forall^\infty n)(f_\alpha(n) < f_\beta(n))$.

Mark Ryten sez that Schmidt construx works only where $f_{\alpha+1}$ is pointwise bigger than f_α and guarantees pointwise domination over Schmidt relatives.

Is the set of tails of a Schmidt-coherent family of fundamental sequences itself Schmidt-coherent?

The idea is to prove by induction on α that f_α is monotone increasing and dominates all earlier f_β. Let's get the dominance out of the way first. Given the induction hypothesis we strive to prove that f_α dominates all earlier f_β. The successor case is obvious;...

Is the succ case really obvious? Pse check

For the limit case suppose f_{λ_i} is strictly increasing for each $i \in \mathbb{N}$ and that later fs dominate earlier fs.

It will suffice to show that f_λ dominates f_{λ_n} for sufficiently large n. So we want:

> for all sufficiently large n and all sufficiently large k[5], $f_\lambda(k) > f_{\lambda_n}(k)$

which is to say

> for all sufficiently large n and all sufficiently large k, $f_{\lambda_k}(k) > f_{\lambda_n}(k)$

One might think that this is simply a matter, for each n, of choosing k large enough. What is certainly true is the following:

> for all sufficiently large n and all sufficiently large k, and all sufficiently large k', $f_{\lambda_k}(k') > f_{\lambda_n}(k')$

But what is not by any means clear is that "sufficiently large k'" is covered by "bigger than k".

If f_λ is $n \mapsto f_{\lambda_n}(n)$ then it dominates every f_{λ_i}.

How about strict monotonicity? If f_α is strictly increasing so is $f_{\alpha+1}$. The hard case is that of limit ordinals. Let λ be limit and $\langle \lambda_n : n \in \mathbb{N} \rangle$ the fundamental sequence for it. We want

This needs to be thoroughly reworked

$$f_\lambda(n) < f_\lambda(n+1). \qquad \text{This holds iff}$$

$$f_{\lambda_n}(n) < f_{\lambda_{n+1}}(n+1). \qquad \text{Now we do at least have}$$

$$f_{\lambda_n}(n) < f_{\lambda_n}(n+1)$$

because f_{λ_n} is strictly increasing by induction hypothesis. So to complete the proof it will suffice to show

$$f_{\lambda_n}(n+1) < f_{\lambda_{n+1}}(n+1),$$

[5] Observe that these quantifiers do not commute

which by induction hypothesis is true for all sufficiently large n ($f_{\lambda_{n+1}}$ dominates f_{λ_n}). But we want it true for *all* n. That will follow if $(\forall\lambda\forall n)(\mathsf{succ}(\lambda_n, \lambda_{n+1}))$ where $\mathsf{succ}(\alpha,\beta)$ is:

$$\alpha < \beta \rightarrow (\forall m)(f_\alpha(m) < f_\beta(m)).$$

However when β is a limit we can be sure of the consequent of $\mathsf{succ}(\alpha,\beta)$ only for sufficiently large m. The construction of the f_αs ensures that $\mathsf{succ}(\alpha,\beta)$ holds if $\beta = \alpha + 1$ or if β is limit and $\alpha = \beta_0$. To be sure of $\mathsf{succ}(\alpha,\beta)$ when $\alpha < \beta$ are members of a fundamental sequence we need to specify that they are related by the transitive closure of the union of these two relations. A family of fundamental sequences satisfying this condition is **Schmidt-coherent**.

Formally:

DEFINITION 21 *Let the family $\mathcal{F} : \Delta \rightarrow \Delta^\omega$ be an assignment of fundamental sequences to an initial segment Δ of the second number class. Let $<_\mathcal{F}$ be the strict partial order which is the transitive closure of $\beta <_\mathcal{F} \beta + 1$ and $(\mathcal{F}\ \beta)\ 0 <_\mathcal{F} \beta$. (Schmidt [22] calls $<_\mathcal{F}$ the step-down relation of $\mathcal{F}$.)*

Then

$\mathcal{F}$ is **Schmidt-coherent** *iff*

$$(\forall\lambda \in \Delta)(\lambda \textit{ limit} \rightarrow (\forall n \in \mathbb{N})((\mathcal{F}\ \lambda\ n) <_\mathcal{F} (\mathcal{F}\ \lambda\ (n + 1)))).$$

(Schmidt calls these 'built-up' rather than 'coherent'.)

It is not hard to see that, for any $\mathcal{F}$, $<_\mathcal{F}$ is a wellfounded (upward-branching) tree and that all paths are of length ω. One steps down at limit ordinals λ by leaping downwards to $\mathcal{F}\ \lambda\ 0$ – the first member of the fundamental sequence for λ, aka λ_0. At successor steps one subtracts one. The way one steps down is uniquely determined by where one **is** not by where one **starts from**. This means that two descending paths that meet anywhere thereafter remain coincident.

Schmidt-coherence is equivalent to the condition that every fundamental sequence lies entirely within one branch of the tree.

EXERCISE 8 *Define the natural assignment of fundamental sequences to ordinals below ϵ_0 and check that it is Schmidt-coherent.*

Do the same for the ordinals below Γ_0.

This completes the proof of:

THEOREM 12 *(Schmidt [22] theorem 1)*

If $\mathcal{F}$ is a Schmidt-coherent family of fundamental sequences then every function in the fast growing hierarchy over $\mathcal{F}$ is monotone and strictly increasing.

Proof:

The definition of Schmidt-coherence was cooked up precisely to make this work.

■

LEMMA 6 *If $\mathcal{F}$ is Schmidt-coherent, λ is limit and $n \in \mathbb{N}$ then $\mathcal{F}^{\lambda,n}$, defined by*

$$\mathcal{F}^{\lambda,n}\ \lambda\ m =: \mathcal{F}\ \lambda\ (m+n);\ \ \mathcal{F}^{\lambda,n}\ \beta\ m = \mathcal{F}\ \beta\ m \text{ for other } \beta$$

... is also Schmidt-coherent.

Proof:

It will suffice to show that $\mathcal{F}\ \lambda\ 0 <_{\mathcal{F}^{\beta,n}} \lambda$. But – since $\mathcal{F}$ is Schmidt-coherent we have $\mathcal{F}\ \lambda\ 0 <_{\mathcal{F}} \lambda$. Hence – by the definition of $\mathcal{F}^{\beta,n}$ – we have $\mathcal{F}^{\beta,n}\ \lambda\ 0 <_{\mathcal{F}^{\beta,n}} \mathcal{F}^{\beta,n}\ \lambda\ n$. But this last ordinal is the $<_{\mathcal{F}^{\beta,n}}$-predecessor of λ, whence $\mathcal{F}\ \lambda\ 0 <_{\mathcal{F}} \mathcal{F}\ \lambda\ n <_{\mathcal{F}^{\beta,n}} \lambda$.

LEMMA 7 *Let $\mathcal{F}$ be a Schmidt-coherent system of fundamental sequences for Δ an initial segment of the second number class, and suppose $\alpha < \beta \in \Delta$. Then there is a system $\mathcal{F}^{(\alpha,\beta)}$ of fundamental sequences[6] for Δ such that*

1. *$\mathcal{F}^{(\alpha,\beta)}$ is Schmidt-coherent;*
2. *$\alpha <_{\mathcal{F}^{(\alpha,\beta)}} \beta$ and*
3. *for all $\delta \leq \alpha$ we have $\mathcal{F}^{(\alpha,\beta)}\delta = \mathcal{F}\delta$.*

Proof:

(lifted brazenly from Schmidt [22])
We define a sequence $\langle \gamma_n, \mathcal{F}_n \rangle$ as follows.
$\gamma_0 =: \beta$, $\mathcal{F}_0 =: \mathcal{F}$;
Thereafter

- if $\gamma_n = \alpha$ then $\gamma_{n+1} =: \alpha$ too, and $\mathcal{F}_{n+1} =: \mathcal{F}_n$;
- if $\gamma_n = \delta + 1 > \alpha$ then $\gamma_{n+1} =: \delta$ and $\mathcal{F}_{n+1} =: \mathcal{F}_n$;
- if $\gamma_n > \alpha$ and is a limit, and m is minimal such that $\mathcal{F}\gamma_n m \geq \alpha$ then $\gamma_{n+1} =: \mathcal{F}\gamma_n m$ and
- – if $\gamma \neq \gamma_n$ then $\mathcal{F}_{n+1}\gamma q =: \mathcal{F}_n \gamma q$, and
  – if $\gamma = \gamma_n$ then $\mathcal{F}_{n+1}\gamma q =: \mathcal{F}_n\gamma(q+m)$.

Using lemma 6 it is easy to show that

- $\mathcal{F}_n$ is Schmidt-coherent,
- $\gamma_n <_{\mathcal{F}_n} \beta$ or $\gamma_n = \beta$,
- $\mathcal{F}_n\delta = \mathcal{F}\delta$ for all $\delta < \alpha$,
- $\gamma_n \geq \alpha$.

Now $\langle \gamma_n : n < \omega \rangle$ is a nonincreasing sequence, so is eventually constant, so there is $n_0 \in \mathbb{N}$ such that $\gamma_{n_0} = \alpha$. Set $\mathcal{F}^{(\alpha,\beta)} =: \mathcal{F}_{n_0}$. ■

[6] This is my notation not hers, and i've put in the brackets to make it less likely that readers will confuse it with the "$\mathcal{F}^{\alpha,\beta}$"

LEMMA 8 *Let $\mathcal{F}$ be a Schmidt-coherent system of fundamental sequences for Δ an initial segment of the second number class, and let λ be the smallest limit ordinal not in Δ. Then there is a Schmidt-coherent system $\mathcal{F}'$ of fundamental sequences for $\Delta \cup \{\lambda\}$.*

Proof:

Let $\langle \lambda_n : n \in \mathbb{N} \rangle$ be a fundamental sequence for λ. We define a sequence $\langle \mathcal{F}_n : n \in \mathbb{N} \rangle$ by recursion as follows. $\mathcal{F}_0 =: \mathcal{F}$ and thereafter $\mathcal{F}_{n+1} =: (\mathcal{F}_n)^{(\lambda_n, \lambda_{n+1})}$ as in 7. Now – by that lemma (itemwise!) – for each $n \in \mathbb{N}$ we have

1. $\mathcal{F}_n$ is Schmidt-coherent;

2. $\lambda_n <_{\mathcal{F}_{n+1}} \lambda_{n+1}$;

3. $\mathcal{F}_n \delta = \mathcal{F}_{n+m} \delta$ for all $\delta \leq \lambda_n$ and $m \in \mathbb{N}$.

We can now set $\mathcal{F}'\beta$ to be

- $\langle \lambda_n : n \in \mathbb{N} \rangle$ if $\beta = \lambda$;
- $\mathcal{F}\beta$ if $\beta \leq \lambda_0$;
- $\mathcal{F}_{m+1}\beta$ if $\lambda_m < \beta \leq \lambda_{m+1}$.

$\mathcal{F}'$ obviously assigns fundamental sequences to everything in $\Delta \cup \{\lambda\}$.

■

THEOREM 13 *(Schmidt [22] theorem 2)*
Every proper initial segment of the second number class admits a Schmidt-coherent family of fundamental sequences.

Proof:

We prove by induction on 'α' that the countable ordinals strictly below α admit a Schmidt-coherent family.

The successor case is easy: if α is a successor of a successor, the assertion follows from the induction hypothesis; if α is the successor of a limit it follows from lemma 8 and the induction hypothesis.

So consider the case where α is limit.

Let $\langle \alpha_n : n \in \mathbb{N} \rangle$ be a fundamental sequence for α, and for each $n \in \mathbb{N}$ set $\sigma_n =: \Sigma_{m<n} \alpha_m$. Clearly $\alpha \leq \mathsf{sup}(\{\sigma_n : n \in \mathbb{N}\})$.

By the induction hypothesis for each $n \in \mathbb{N}$ there is a Schmidt-coherent family $\mathcal{F}_n$ for the ordinals below $\alpha_n + 1$. We now define a family $\mathcal{F}$ as follows:

$\mathcal{F}\gamma\, m =:$

- 0 if γ is zero or a successor;
- $\sigma_n + (\mathcal{F}(\gamma - \sigma_n)m)$ otherwise, where n is maximal so that $\sigma_n < \gamma$.

Now for all μ and ν such that $\sigma_n < \mu \leq \sigma_{n+1}$ and $\sigma_n < \nu \leq \sigma_{n+1}$ we have $\mu <_{\mathcal{F}} \mu \longleftrightarrow (\mu - \sigma_n) <_{\mathcal{F}_n} (\nu - \sigma_n)$. Hence if γ is a limit ordinal and $\sigma_n < \gamma \leq \sigma_{n+1}$ then $\gamma - \sigma_n$ is also a limit, and since $\mathcal{F}_n$ is Schmidt-coherent we have $\mathcal{F}(\gamma - \sigma_n)m <_{\mathcal{F}_n} \mathcal{F}(\gamma - \sigma_n)(m+1)$ for each $m \in \mathbb{N}$. Thus $\mathcal{F}\gamma m = \sigma_n + (\mathcal{F}(\gamma - \sigma_n)m) <_{\mathcal{F}} \sigma_n + (\mathcal{F}(\gamma - \sigma_n)(m+1)) = \mathcal{F}\gamma(m+1)$. So $\mathcal{F}$ is Schmidt-coherent.

■

Can we omit 'proper' from the statement of theorem 13? We proved it without any use of AC.

what is this Rose reference?

> Rose says that theorem 13 is best possible, and credits Bachmann: *Transfinite Zahlen* Springer, 1967. I'm sceptical about this because he also says that Schmidt, too, proves that it is best possible – and she doesn't!
>
> If it really is best possible, it's presumably because a Schmidt-coherent family for all countable ordinals would give us an embedding of ω_1 into the reals, or something like that. There can be long sequences ($\geq \omega_1$) of functions with each function dominating all earlier functions, but they don't increase as fast as Wainer-Buchholtz.

[two thoughts: To each ordinal κ associate the least ordinal α such that there is a β such that $\beta + \alpha = \kappa$. There can be only finitely many such α. Is this idempotent?

This suggests a topology on the ordinals: for each α, the set $\kappa + \alpha : \kappa \in On\}$ is basic open. Any ordinal can belong to only finitely many basic open sets]

5.2 Nathan on Schmidt-coherence

A *system of fundamental sequences* for a countable ordinal γ is a function assigning to each limit ordinal $\alpha < \gamma$ a sequence $\langle \alpha_n : n \in \mathbb{N} \rangle$ with supremum α. For such a system, we let $\preceq$ be the partial order generated from $\alpha \preceq \alpha + 1$ and $\alpha_0 \preceq \alpha$ over all α. We say the system is *Schmidt coherent* if for any $\alpha < \gamma$ and $n \in \mathbb{N}$ we have $\alpha_n \preceq \alpha_{n+1}$.

The following construction builds a Schmidt-coherent system of fundamental sequences for an ordinal γ from an enumeration of γ as $\{\alpha(n) : n \in \mathbb{N}\}$ such that $\alpha(0) = 0$. For any n with $\alpha(n)$ a limit, we choose n_0 such that $n_0 < n$ and $\alpha(n_0) < \alpha(n)$, and we choose it to maximise $\alpha(n_0)$ subject to these constraints (this is possible as there are only finitely many $m < n$). Then for any $i \geq 0$ we choose n_{i+1} to be minimal such that $\alpha(n_i) < \alpha(n_{i+1}) < \alpha(n)$. We assign to $\alpha(n)$ the sequence $(\alpha(n_i)|i \in \mathbb{N})$, which clearly has supremum $\alpha(n)$, so gives a fundamental sequence for $\alpha(n)$. We will now show that the system of fundamental sequences defined in this way is Schmidt-coherent.

Let $\preceq$ be defined as above. We define a further relation on the natural numbers by $m \lessdot n$ if $\alpha(m) < \alpha(n)$ and for all k with $\alpha(m) < \alpha(k) \leq \alpha(n)$ we have $k > m$.

For any n we define $p(n)$ to be 0 if $n = 0$, the m with $\alpha(n) = \alpha(m) + 1$ if $\alpha(n)$ is a successor and n_0 if $\alpha(n)$ is a limit. Thus $\alpha(p(n)) \preceq \alpha(n)$.

LEMMA 9 *If $m \lessdot n$ then either $m \lessdot p(n)$ or else $m = p(n)$.*

Proof:

We cannot have $\alpha(n) = 0$. If $\alpha(n)$ is a successor then it is clear that $\alpha(m) \leq \alpha(p(n)) < \alpha(n)$. if $\alpha(n)$ is a limit then we have $m < n$ and $\alpha(m) < \alpha(n)$ so that by the definition of n_0 we have $\alpha(m) \leq \alpha(n_0)$, so in this case we also have $\alpha(m) \leq \alpha(p(n)) < \alpha(n)$. Now the result follows from the definition of $\lessdot$. ■

LEMMA 10 *For any m and n with $m \lessdot n$ we have $m \leq n$.*

Proof:

Suppose not for a contradiction. For any i we have $p^i(n) \leq n$, so for no i can we have $p^i(n) = m$. Thus by Lemma 9 we have for every i that $m \lessdot p^i(n)$, and in particular $p^i(n) \neq 0$. Thus $(p^I(n)|n \in \mathbb{N})$ is an infinite strictly decreasing sequence of ordinals, which is the desired contradiction. ■

LEMMA 11 *For each n with $\alpha(n)$ a limit and each i we have $n_i \lessdot n_{i+1}$.*

Proof:

First we show this in the case $i = 0$. By the definition of n_1 we have $\alpha(n_0) < \alpha(n_1)$. Suppose for a contradiction that there is some $k \leq n_0$ with $\alpha(n_0) < \alpha(k) \leq \alpha(n_1)$. Then $k < n$ and $\alpha(k) < \alpha(n)$, so by the definition of n_0 we have $\alpha(k) \leq \alpha(n_0)$, contradicting our assumptions. Thus $n_0 \lessdot n_1$.

Next we deal with the case $i > 0$. By the definition of n_{i+1} we have $\alpha(n_i) < \alpha(n_{i+1})$. For any k with $\alpha(n_i) < \alpha(k) \leq \alpha(n_{i+1})$ we have $\alpha(n_{i-1} \leq \alpha(k)$ and so by the definition of n_i we have $n_i \leq k$, so $n_i < k$ as $n_i \neq k$. ■

It follows from the last two lemmas that if n is a limit then for any i we have $n_i \leq n_{i+1}$, so that the system is Schmidt coherent.

Is the Veblen ϕ function dominated by anything in the Doner-Tarski hierarchy?

enuff rec fn th to explain why low members of the hierarchies are prim rec.

$\square\kappa$ says that there is an assignment of fundamental sequences to all the ordinals between κ and κ^+ and that the sequences cohere

Define fundamental sequences and some fast-growing hierarchies. Prove that primitve rec fns come in at low levels.

The fact that dilators are uniquely determined by their action on $\mathbb{N}$ is surely crucial. Does this shed any light on the old question of whether or not $\mathrm{AxCount}_\leq$ implies the analogue for ctbl ordinals?

We've managed to get this far on generalities that do not depend on the precise declaration of the fast-growing hierarchy. The time has now come to be specific. Let $\mathcal{F}$ be a Schmidt-coherent family of fundamental sequences.

The following seems to be popular: (Buchholtz-Wainer[3] refer to it merely as 'the' fast-growing hierarchy!)

DEFINITION 22 *(Buchholtz-Wainer)*
The Fast-Growing Hierarchy

$f_0(x) =: x + 1$;
$f_{\alpha+1}(x) =: f_\alpha{}^{x+1}(x)$;
$f_\lambda(x) = f_{(\mathcal{F}\ \lambda\ x)}(x)$.

The fast-growing hierarchy with finite subscripts is the **Grzegorczyk** *hierarchy.*
The **Hardy Hierarchy** *([15]) is:*

$H_0(x) =: x + 1$;
$H_{\alpha+1}(x) =: H_\alpha(x + 1)$;
$H_\lambda(n) = H_{(\mathcal{F}\ \lambda\ n)}(n)$.

Just to reassure myself that i am in familiar surroundings i shall prove

REMARK 7 *For $\alpha < \omega$, f_α is primitive recursive.*

Proof:
Clearly true for $\alpha = 0$. Define `iter` g so that $\texttt{iter}(g, n) : m \mapsto (g^n(m))$ by means of the following declaration:

$$\texttt{iter}(f, 0)\ m =: m;\ \texttt{iter}(f, (n + 1))\ m =: f(\texttt{iter}(f, n)\ m)$$

we see that $\texttt{iter}(g, n)$ is primitive recursive as long as g is. Then
$f_{\alpha+1} : n \mapsto (\texttt{iter}(f_\alpha, n + 1)\ n)$
is primitive recursive as long as f_α is.

■

EXERCISE 9 *Determine f_0, f_1 and f_2.*

EXERCISE 10 *(Computer Science Tripos 1991:5:10)*
Ackermann's function is defined as follows:

$$A(0, y) =: y + 1;\ A(x + 1, 0) =: A(x, 1);\ A(x + 1, y + 1) =: A(x, A(x + 1, y))$$

For each n define
$a_n(y) =: A(n, y)$.
Prove $(\forall y)(\forall n \in \mathbb{N})(a_{n+1}(y) = a_n^{y+1}(1))$.

Notice that $a_0(x) = f_0(x) = x + 1$.
Then by induction on the recursive datatype of primitive recursive functions we prove that every primitive recursive function is dominated by all sufficiently late a_n.

THEOREM 14 *For every primitive recursive function $f(\vec{x}, n)$ there is a constant c_f such that*

$$(\forall n \forall \vec{x})(f(\vec{x}, n) < A(c_f, max(n, \vec{x})))$$

(In slang, every primitive recursive function is in O(Ackermann).)

EXERCISE 11 *Complete the proof.*

Notice that there cannot be a converse. This is because of the silly reason that there are slowly growing functions that are inverses of rapidly growing ones, and are therefore equally hard to compute. Try the computer science tripos question 1994 paper 5 question 11 (at `http://www.cl.cam.ac.uk/tripos/t-ComputationTheory.html`)

Then $A(n,n)$ diagonalises the a_n the way f_ω diagonalises the f_n. So $A(n,n)$ is "at the same level" as f_ω. In fact if f is primitive recursive, then the c_f of theorem 14 is precisely the level of the fast-growing hierarchy that f belongs to (I think!).

Chapter 6

Hessenberg Sum and Product

There is a wikipædia article that one could consult.

The Hessenberg sum arises from an attempt to give the ordinals the structure of an additive abelian semigroup with cancellation. If $\oplus$ is to have cancellation then $\alpha \oplus \beta$ had better be different from $\alpha \oplus \beta'$ for all β' and different from $\alpha' \oplus \beta$ for all α'. If we are to declare Hessenberg sum by recursion (as we will) it is of course enough to ensure that $\alpha \oplus \beta$ is the least thing distinct from $\alpha \oplus \beta'$ for all $\beta' < \beta$ and distinct from $\alpha' \oplus \beta$ for all $\alpha' < \alpha$.

Given that thought, the obvious first stab at a definition making addition-on-the-right injective declares $\alpha \oplus \beta$ to be the least ordinal above α that is not $\alpha \oplus \beta'$ for any $\beta' < \beta$. Since the set of ordinals for which $\alpha \oplus \beta$ is the least thing not in it is a subset of the set of ordinals for which $\alpha + \beta$ is the least thing not in it, it follows that $\alpha \oplus \beta \leq \alpha + \beta$.

Another way in (tho' i don't see how to tie this in with the foregoing) declares $\alpha \oplus \beta$ to be the largest ordinal that we can obtain by interleaving a worder of otype α with a worder of otype β. Notice that this definition enforces commutativity, which the other one doesn't – at least not obviously. What might this ordinal be? How about $\alpha + \beta$? We might be able to improve on that if β absorbs-on-the-left some terminal segment of α. So let's think of α as $\alpha_1 + (\alpha - \alpha_1)$ where α_1 is the shortest initial segment with the property that $\alpha - \alpha_1$ is absorbed by β. So we go for $\alpha_1 + \beta + (\alpha - \alpha_1) \ldots$? Is that what we want? It's certainly a step in the right direction. However there is the possibility that $\beta = \beta_1 + (\beta - \beta_1)$ where $\alpha - \alpha_1$ absorbs $\beta - \beta_1$ on the left, in which case we want to rearrange to get $\alpha_1 + \beta_1 + (\alpha - \alpha_1) + (\beta - \beta_1)$. But we might still not have reached our goal, beco's the $(\beta - \beta_1)$ bit we stuck on the end might absorb a terminal segment of the $(\alpha - \alpha_1)$ bit we stuck it on the end of. Key observation is that this cannot go on for ever beco's the sequence of subscripted αs (or βs) is decreasing. To get the connection with CNF we need to prove a theorem about absorbtion-on-the-left and powers of ω. But this is easy: γ absorbs-β-on-the-left iff $\gamma \geq \beta \cdot \omega$.

Some pictures here would be good!

We are now ready for the connection with Cantor Normal form, with its Leading Rôle for powers of ω. The point is that any power of ω absorbs all lower powers of ω on the left.

So: to obtain the Hessenberg sum of two ordinals, express them both in CNF, and

extract the two finite sets of terms used in those CNF. Order the union of those two sets in decreasing order, and add them up in that decreasing order. One ordinal might supply $\omega^\alpha \cdot \beta$ and the other might supply $\omega^\alpha \cdot \gamma$, so we have to do something with these terms – amalgamate them somehow – to get (i think) $\omega^\alpha \cdot (\beta \oplus \gamma)$. This makes this definition recursive.

Now think about Hessenberg natural product. As a first attempt think of making multiplication-on-the-right injective by defining $\alpha \otimes \beta$ to be the least ordinal above α that is not $\alpha \otimes \beta'$ for any $\beta' < \beta$. But we somehow have to take cognizance of the fact that multiplication distributes over addition. . . .

Copy in stuff from fundamentalsequence.tex or logicrave.tex

Have to show both are associative. Wikipædia asserts as much

Something to think about. Hessenberg maximal sum has this intimate relation with Cantor normal form, beco's of the rôle played by $\alpha \mapsto \omega^\alpha$ in both cases. Are there other binary operations related similarly to faster-growing normal functions and corresponding ordinal notations?

Chapter 7

Ordinals, Fast-growing Functions, Consistency and Totality Proofs

Stuff to fit in

Here is a potentially useful piece of armwaving.

7.0.1 Inductions over longer wellorderings are stronger

One thing that anyone who has heard of Con(PA) and ordinals will be able to recite is the fact that induction up to ϵ_0 is enough to prove Con(PA). Why induction up to ϵ_0 not ω? It always seems to be taken for granted that it's obvious that induction up to ϵ_0 (whatever that means!) is stronger than induction up to ω. I have never seen a satisfactory explanation in any textbook of what is going on, so what follows below is the result of my trying to explain this situation to myself[1].

Consider the scheme of R-induction we set out earlier:

$$\frac{(\forall y)(R(y,x) \to \psi(y)) \to \psi(x)}{(\forall x)(\psi(x))} \qquad R\text{-induction}$$

We are interested in calibrating the strength of the various versions of this scheme as R varies. Observe that any subset of (the graph of) a wellfounded relation is (the graph of) a wellfounded relation. In particular the empty relation is wellfounded.

What happens if we remove ordered pairs from R? How does that affect the strength of the principle of R-induction?

The assumption $R(x, y)$ on the top line becomes stronger so

[1] I suspect this is generally true, and that many textbooks and monographs arise from their authors' attempts to explain things to themselves.

the conditional $R(y,x) \to \psi(y)$) becomes weaker. Therefore

the condtional $(\forall y)(R(y,x) \to \psi(y)) \to \psi(x)$ becomes stronger, so

the inference thence to $(\forall x)(\psi(x))$ becomes weaker.

Consider in particular what the principle of R-induction tells us when R is the empty relation. It tells us nothing[2]!

For this to tell us *literally* that inductions over longer wellorderings are stronger than inductions over shorter wellorderings we would need graphs of longer wellorderings to be supersets of graphs of shorter wellorderings. That can't be true, beco's no superset of a wellordering of a set can be a wellordering – at least not of the same set. The graph of a wellordering of $\mathbb{N}$ to length ω^2 isn't literally a superset of the graph of $<_{\mathbb{N}}$ but it does *seem* to have more ordered pairs in the sense that in $<_{\mathbb{N}}$ every element has only finitely many predecessors whereas in any worder of $\mathbb{N}$ of otype ω^2 there are lots of elements with infinitely many predecessors – infinitely many in fact.

In this connection one can make the observation that if $f : X \hookrightarrow Y$ and $(\forall u, v \in X)(R(x,y) \longleftrightarrow S(f(x), f(y)))$ then $\langle X, R\rangle$ is wellfounded if $\langle Y, S\rangle$ is. This is in effect the burden of the following theorem.

THEOREM 15 *Suppose we have a principle of R-induction:*

$$\underline{(\forall x)((\forall y)(R(y,x) \to \psi(y)) \to \psi(x))}$$

$$(\forall x)(\psi(x))$$

R-induction

Suppose further that S is a relation with an injection $f : dom(S) \hookrightarrow dom(R)$ satisfying $(\forall x, y)(S(x,y) \longleftrightarrow R(f(x), f(y)))$.

Then we can infer a corresponding principle of S-induction:

$$\underline{(\forall x)((\forall y)(S(y,x) \to \psi(y)) \to \psi(x))}$$

$$(\forall x)(\psi(x))$$

S-induction

Proof:

Assume $(\forall x)((\forall y)(S(y,x) \to \psi(y)) \to \psi(x))$; we want to infer $\forall x \psi(x)$.

We want the instance of R-induction where the property being proved is "if x is a value of f then it's f of something that is ψ": $(\forall z)(x = f(z) \to \psi(z))$. Write this as $\psi^*(x)$ for short. So! is it the case that

$$(\forall x)((\forall y)(R(y,x) \to \psi^*(y)) \to \psi^*(x))?$$

[2]It tells us nothing – in the following sense. Take the statement of R-induction and replace all occurrences of '$R(x,y)$' by '$\bot$'. The resulting inference is logically valid, and we get it free.

Let x be arbitrary; we need to infer $\psi^*(x)$ from $(\forall y)(R(y,x) \to \psi^*(y))$. Well, assume $x = f(z)$, some z; we want to infer $\psi(z)$.

We have $(\forall y)(R(y, f(z)) \to \psi^*(y))$. So certainly, for all $f(w)$, we have

$R(f(w), f(z)) \to \psi^*(f(w))\ldots$ which is

$(\forall w)(S(w,z) \to \psi(w))$ which gives $\psi(z)$ by induction hypothesis.

■

Then there is the surjective-homomorphism case.

At some point use the *aperçu* about the destination of ω forming an ω_1-descending sequence in $\mathbb{R}$ as we pile more and more stuff on the end and press stuff down. It pops up! – and at places where coherence fails.

7.1 The Ordinal ϵ_0 and the Consistency of Peano Arithmetic

I will now sketch how to prove the consistency of Peano Arithmetic by transfinite induction. (I have lifted this from the *first* edition of [19]; this material was removed from some later editions but has reappeared in the 6th edition.) The proof goes back to [**?**].

We have a system of arithmetic in something like our natural deduction but in a language with $\vee$, $\neg$ and $\forall$ only. In addition to the obvious rules for $\vee$ and $\neg$ it has an ω-rule:

$$\frac{\Gamma \vdash F(0)\ \ \Gamma \vdash F(S(0))\ldots\Gamma \vdash F(S(S(0)))\ldots}{\Gamma \vdash (\forall n)(F(n))}$$

which serves as a kind of $\forall$-int rule. It also has a rule of "cut":

$$\frac{A \vee B \quad A \vee \neg B}{A}$$

The assumptions (the leaves of the proof-trees in this system) are true atomic sentences of the kind '$0 = 0$', '$0 \neq S(0)$' and suchlike (no variables!) The only terms allowed are numerals in the style $S \cdots S(0)$.

Proofs in this system can be seen as countable trees (each node [inference] might have a countable infinity of premisses). Clearly we are not going to be interested in proofs that have infinite paths – after all, any formula whatever can be supplied with a proof with an infinite path. We are interested only in proofs whose corresponding trees have no infinite paths. Such a proof can be decorated with ordinals in the standard manner from chapter **??**. How large a countable ordinal might one need to decorate a tree of a proof in this system? There are only countably many formulæ in the language of arithmetic so each node can have only countably many immediate predecessors, and

a sup of countably many countable ordinals is countable. This means that the rank of a proof must be countable[3].

This invites us to consider, for a countable limit ordinal α, the collection $T(\alpha)$ of those formulæ that have proofs whose trees have rank $< \alpha$, and where the proof has a cut of maximal degree. (The degree of a cut is the number of connectives and quantifiers in the cut formula). For suitable α, $T(\alpha)$ might be closed under the finitary rules of inference and thereby be a set deductively closed in the usual sense, to wit: a *theory*.[4]

Theories arising from countable ordinals in this sense have the potential to be very interesting ... particularly if they are consistent! Mendelson [19] says that $T(\omega_1)$ is the first-order theory of the standard model, and that $T(\epsilon_0)$ is Peano Arithmetic (or something very like it).

When do we know that such a theory is consistent? One way of detecting that a theory is consistent is to prove cut-elimination for it. This is because there is no cut-free proof of $\perp$.

This is roughly the point of departure for the analysis in [19]. The labellings of the trees that he uses there differ slightly from the rank function on a naked tree but the idea is the same. Decorate the proof tree by labelling endpoints with '0', and the rank of a node is the sup of rank + 1 of the nodes above it – unless the node corresponds to a structural rule, in which case the rank is the same as the rank of its predecessor.

It turns out that we can show that for all α, if we can do transfinite recursions of length 2^α, then for any proof in $T(\alpha)$ we can find a proof in $T(2^\alpha)$ with the same conclusion and lower cut rank.

Thus, by repeating this process we can show that, for every α and every proof in $T(\alpha)$ there is a cut-free proof in $T(\sup\{\alpha, 2^\alpha, 2^{2^\alpha} \ldots\})$ with the same conclusion.

EXERCISE 12 *ω is the first solution to the equation $\alpha = 2^\alpha$. What is the next solution?*

DEFINITION 23 *An ordinal α is an* epsilon number *iff it is a solution to $\alpha = \omega^\alpha$, or equivalently iff the ordinals below it are closed under exponentiation.*

Thus if α is an ϵ-number, written ϵ, then we find that $\epsilon = 2^\epsilon$, so that $\sup\{\alpha, 2^\alpha, 2^{2^\alpha} \ldots\} = \alpha$ so $T(\sup\{\alpha, 2^\alpha, 2^{2^\alpha} \ldots\}) = T(\alpha)$ and then induction/recursion up to ϵ enables us to show that any proof in $T(\epsilon)$ can have the cuts eliminated from it and become a proof still in $T(\epsilon)$! So we conclude that, for any ϵ-number ϵ, we can prove by transfinite induction on 'α' that

> if $\alpha < \epsilon$ then every formula that has a proof of rank $\leq \alpha$ has a cut-free proof of rank below ϵ.

In other words

REMARK 8 *For an ϵ-number ϵ, induction/recursion of length ϵ enables us to prove the consistency of $T(\epsilon)$.*

[3] There is enough structure around for us not to need countable choice to prove this.

[4] I shall equivocate between thinking of $T(\alpha)$ as a theory and thinking of it as a body of proofs.

Proof:

If α is an ϵ-number and we can induct as far as α (i.e., we have a wellordering of length α) then we can recursively eliminate cuts from proofs in $T(\alpha)$ while remaining inside $T(\alpha)$ thereby proving $T(\alpha)$ consistent.

To be more specific:

Let n be arbitrary (so we are doing a UG on 'n'). Let P be a proof of formula A with degree $n+1$; we prove by induction on 'α' that if P has rank α, then Transform(P) is a proof of formula A with degree n and ordinal 2^α"

At top level we are proving $\forall n$ something-or-other by UG on 'n'. At each n we do an induction on countable ordinals. This relies on "P' = transform(P)" containing no unrestricted quantifiers. That sounds believable-but-laborious-to-check.

What i don't really understand is why rank(P) = $\alpha \rightarrow$ rank(Transform(P)) $\leq 2^\alpha$ needs induction on α and doesn't just use UG. I'm definitely in the market for some intelligent tho'rts on that.

■

In particular, if we can induct as far as ϵ_0, then this will show that $T(\epsilon_0)$ is consistent. So: what do we know about this system $T(\epsilon_0)$ whose consistency we can prove if we can induct as far as ϵ_0? It turns out that $T(\epsilon_0)$ is at least Peano Arithmetic.

> (What had been worrying me here is that if the proof is infinite there may be no cut of greatest rank, so how can we prove that the process halts? The point is that all proofs that arise from embedding proofs of finitary arithmetic in this system are finitary and have finite cut degree.)

7.2 The Goodstein function

The Goodstein function, known as G (for obvious reasons) is an example of a function that is manifestly computable but very far-from-manifestly total. To discover what $G(x)$ is to be, we first express x as a sum of powers of 2, and then express the *exponents* as sums of powers of two, and so on recursively. Thus, if we do this to – say – 37, we get

$$32 + 4 + 1 =$$

$$\mathbf{2}^5 + \mathbf{2}^2 + 1 =$$

$$\mathbf{2}^{4+1} + \mathbf{2}^2 + 1 =$$

$$\mathbf{2}^{\mathbf{2}^2+1} + \mathbf{2}^2 + 1$$

This is the ϵ*xtended* base 2 representation of a number. I have written the '2's in **boldface** to remind us that this expression is in ϵxtended base 2.[5] Now replace all the

[5] there is a reason for the choice of a Greek font for the first letter of 'extended' It's the feed-line for a joke that will be revealed later.

2's by 3's and subtract 1. This gives us $\mathbf{3}^{\mathbf{3}^3+1} + \mathbf{3}^3$. The result is still in ϵxtended base 3. Now replace all '3's by '4's

$$4^{4^4+1} + 4^4$$

and subtract 1 to get

$$4^{4^4+1} + 4^4 - 1$$

But this is not in ϵxtended base 4 representation because of the minus sign, and we have to express $4^4 - 1$ as a sum of powers of 4 with a few 1's left over, thus

$$\mathbf{4}^{1+1+1} + \mathbf{4}^{1+1+1} + \mathbf{4}^{1+1+1} + \mathbf{4}^{1+1} + \mathbf{4}^{1+1} + \mathbf{4}^{1+1} + \mathbf{4} + 4 + 4 + 1 + 1 + 1$$

so the whole thing is

$$\mathbf{4}^{\mathbf{4}^{\mathbf{4}}+1} + \mathbf{4}^{1+1+1} + \mathbf{4}^{1+1+1} + \mathbf{4}^{1+1+1} + \mathbf{4}^{1+1} + \mathbf{4}^{1+1} + \mathbf{4}^{1+1} + \mathbf{4} + 4 + 4 + 1 + 1 + 1.$$

(The '$\mathbf{4}$'s are still in boldface to remind us that this number is being written in ϵxtended base $\mathbf{4}$.)

Then we can replace all '4's by '5's, subtract 1 and continue. How long can we continue doing this? These numbers seem to go on getting bigger and bigger!

However, if we try it on 2, the process stops: 2 becomes $3 - 1$ which in ϵxtended base 3 is $1 + 1$ becomes 1 becomes 0. If we try it on 3 we get $2^1 + 1$ becomes 3^1 becomes $4^1 - 1 = 1 + 1 + 1$ which will decay to 0 as before. We are now in a position to announce a definition:

> $G(x)$ **is the length of the sequence of terms generated in this way (if it is defined).**

Thus the Goodstein function is actually a cost function for the computable function $\mathbb{N} \to \{0\}$ defined by

```
INPUT n
    write n in ε-extended base 2
    i =: 3
REPEAT
    n =: replace 'i' with 'i + 1' in representation of n
    rewrite the result in ε-extended base i + 1 representation;
    i =: i + 1
    subtract 1
UNTIL
    n = 0
PRINT i
```

and this definition makes it clear that G is μ-recursive.

Thus $G(2) = 4$ and $G(3) = 5$. $G(4)$ is quite large but can be computed by hand. One might think that for at least some larger numbers the sequence goes on for ever; remarkably[6], this is not so: G is total computable.

[6] Try proving by induction on 'n' that $G(n)$ is defined; you will get nowhere.

THEOREM 16
If there is a wellordering of length ϵ_0 then $G(n)$ is defined for all $n \in \mathbb{N}$.

Proof

The key to the proof is to spot the trick that the conjuror is playing on you. Your attention is being directed to the apparently inexorably increasing sequence of numbers, so that you don't notice the thing that is actually decreasing.

Start with a number in ϵxtended base 2 representation. Consider the ordinal in Cantor Normal Form obtained from this expression by replacing every '2' by an 'ω'.[7] In our first example above (37), this would be $\omega^{\omega^{\omega}+1} + \omega^{\omega} + 1$, since the ϵxtended base 2 representation of 37 was $\mathbf{2}^{\mathbf{2}^{\mathbf{2}}+1} + \mathbf{2}^{\mathbf{2}} + 1$..

To every number in the sequence we are building (whose length will be $G(n)$) we will make correspond an ordinal in precisely this way – (That was why I wrote the base in **boldface** so that we can say:) – simply replace the boldface number by ω. Numerals not written in boldface are *not* replaced by 'ω'. Thus for each i the ith member of the sequence (on the left) will correspond to the ordinal to its right:[8]

$\mathbf{2}^{\mathbf{2}^{\mathbf{2}}+1} + \mathbf{2}^{\mathbf{2}} + 1$	$\omega^{\omega^{\omega}+1} + \omega^{\omega} + 1$
$\mathbf{3}^{\mathbf{3}^{\mathbf{3}}+1} + \mathbf{3}^{\mathbf{3}}$	$\omega^{\omega^{\omega}+1} + \omega^{\omega}$
$\mathbf{4}^{\mathbf{4}^{\mathbf{4}}+1} + 3\cdot\mathbf{4}^{3} + 3\cdot\mathbf{4}^{2} + 3\cdot\mathbf{4} + 3$	$\omega^{\omega^{\omega}+1} + \omega^{3}\cdot 3 + \omega^{2}\cdot 3 + \omega\cdot 3 + 3$
$\mathbf{5}^{\mathbf{5}^{\mathbf{5}}+1} + 3\cdot\mathbf{5}^{3} + 3\cdot\mathbf{5}^{2} + 3\cdot\mathbf{5} + 2$	$\omega^{\omega^{\omega}+1} + \omega^{3}\cdot 3 + \omega^{2}\cdot 3 + \omega\cdot 3 + 2$
$\mathbf{6}^{\mathbf{6}^{\mathbf{6}}+1} + 3\cdot\mathbf{6}^{3} + 3\cdot\mathbf{6}^{2} + 3\cdot\mathbf{6} + 1$	$\omega^{\omega^{\omega}+1} + \omega^{3}\cdot 3 + \omega^{2}\cdot 3 + \omega\cdot 3 + 1$
$\mathbf{7}^{\mathbf{7}^{\mathbf{7}}+1} + 3\cdot\mathbf{7}^{3} + 3\cdot\mathbf{7}^{2} + 3\cdot\mathbf{7}$	$\omega^{\omega^{\omega}+1} + \omega^{3}\cdot 3 + \omega^{2}\cdot 3 + \omega\cdot 3$
$\mathbf{8}^{\mathbf{8}^{\mathbf{8}}+1} + 3\cdot\mathbf{8}^{3} + 3\cdot\mathbf{8}^{2} + 2\cdot\mathbf{8} + 7$	$\omega^{\omega^{\omega}+1} + \omega^{3}\cdot 3 + \omega^{2}\cdot 3 + \omega\cdot 2 + 7$
$\vdots$	$\vdots$
$\mathbf{15}^{\mathbf{15}^{\mathbf{15}}+1} + 3\cdot\mathbf{15}^{3} + 3\cdot\mathbf{15}^{2} + 2\cdot\mathbf{15}$	$\omega^{\omega^{\omega}+1} + \omega^{3}\cdot 3 + \omega^{2}\cdot 3 + \omega\cdot 2$
$\mathbf{16}^{\mathbf{16}^{\mathbf{16}}+1} + 3\cdot\mathbf{16}^{3} + 3\cdot\mathbf{16}^{2} + \mathbf{16} + 15$	$\omega^{\omega^{\omega}+1} + \omega^{3}\cdot 3 + \omega^{2}\cdot 3 + \omega + 15$
$\vdots$	$\vdots$
$\vdots$	$\vdots$

So the length of the sequence we are building will be the same length as a particular decreasing sequence of ordinals. Why is it decreasing? The entries in the left-hand column keep increasing as long as there are boldface numerals around, because we increase each boldface numeral by one at each stage. In the short term, this more than compensates for the 1 that we keep subtracting. In contrast the entries on the right have ω instead of a boldface numeral, and we do not increase the ω, so there is nothing to counteract the slow attrition of subtraction of 1.

Any decreasing sequence of ordinals must be finite, so the original sequence of numbers was finite, so $G(n)$ is defined. In this case the ordinals we are using are all below ϵ_0, so it will suffice to have a wellordering of that length. ■

[7] For these purposes we take the Cantor Normal Form of an ordinal to be the wordy, verbose version that does not allow multiplication by naturals, so that an ordinal is a sum of powers of ω.

[8] I have reverted to the style of Cantor normal form that allows multiplication by naturals in order to save space!

Once you understand the proof of theorem 16 you can see immediately that from the same assumption used above – namely that the set of ordinals below ϵ_0 is available to us, along with its ordering, and the information that that ordering is wellfounded – we can prove not only the totality of G but also the totality of any function computed like G but with the tweak that we are not required to decrement *every single time* we increase the base, as long as we promise, when we find ourselves at a nonzero number, to decrement at some point. Consider what one might call the *Nondeterministic Goodstein Function* where at each stage in the computation of $G(n)$ one makes a random choice about whether to decrement or not. Clearly an analysis analogous to the analysis above will establish that any nonterminating computation of the Nondeterministic Goodstein function has only finitely many decrements. Let us minute this fact.

REMARK 9 *If there is a wellordering of length ϵ_0 then the nondeterministic $G(n)$ is defined for all $n \in \mathbb{N}$.*

Why the odd title?

Goodstein's paper was entitled "On the Restricted Ordinal Theorem"; "The restricted ordinal theorem" was the name current at that time for the allegation usually expressed nowadays by the form of words "the ordinals below ϵ_0 are wellordered". This is loose talk: ϵ_0 is an ordinal, and for any ordinal α the ordinals below α are wellordered: that's a complete triviality and cannot be used to prove anything. The bit that does the work is the assumption that *there is a wellordering of length α*. For consider how the proof would procede in a formal system: for each input to G we define a decreasing function from $\mathbb{N}$ to the ordinals below ϵ_0, and we need the range of that function to be a set, so we need that collection to be a set, and we need the ordering on it to be a wellordering. One might suspect that Goodstein's purpose in devising this rather odd function was to exhibit a computable total function whose totality is not demonstrable in Peano arithmetic, precisely because the totality relies on an induction that is not available in PA. However[9] the reason is more likely to do with the view – current around that time – that ϵ_0 was the supremum of those ordinals that had a finite description. It can't be that simple beco's the Veblen hierarchy was known at that stage, so it may instead be something to do with the fact that the ordinals below ϵ_0 are closed under $+$, $\times$ and exponentiation, and that those three operations are the only operations in the Doner-Tarski sequence that correspond to actual operations on wellorderings. In case you didn't know, α^β is the order type of the set of functions $B \to A$ which are 0 at all but finitely many places, ordered colex – where $\mathrm{otp}(\langle A, <_A\rangle) = \alpha$ and $\mathrm{otp}(\langle B, <_B\rangle) = \beta$. The next operation – f_s, the "tower of exponents" – has no concrete representation of this kind. This is because it grows faster than $n \mapsto \beth_k(n)$ for any $k \in \mathbb{N}$, so we cannot find any expression $R(x, y)$ in the language of set theory such that $|y| = |f_3(x, x)|$. Actually it's not the next one after exponentiation that explodes the type hierarchy but a slightly later one.

Worth spelling out in some detail

I do not know if this consideration is explicit in the literature of the 1930's and 40's . . . it could be worth checking.

[9] Thank you Stan Wainer!

Stan Wainer says that the significance of Goodstein's assault on ϵ_0 was that it was believed by many at the time to be a prime candidate for the rôle of first non-finitary ordinal. I wondered aloud if that might be connected to the fact that it is the least transfinite ordinal s.t. the set of its predecessors is closed under the three operations (+, $\times$ and *exp*) which correspond to concrete binary operations on wellorderings. The next Doner-Tarski operation doesn't correspond to any binary operation on wellorderings.

Interestingly those three operations correspond to *homogeneous* operations on wellorderings. OOps no. The first two do, but *exp* doesn't unless one has IO. [spell this out] This is beco's there is no type-lowering ordered pair.

a Conversation with Randall about type-level definitions of ordinal exponentiation

A key fact is that if we have a type-level pair then there is a definable global function f (for the moment) s.t. if $\mathcal{A} = \langle A, <_A \rangle$ is a wellordering then $f(\mathcal{A})$ is a bijection between A and $A \times A$. *Mutatis mutandis* if pairing is not type-level. This function is exploited in the proof that $\aleph = \aleph^2$. The uniform nature of this bijection is essential to the avoidance of choice.

[presumably we need A to be infinite; better spell this out.]

Let $\alpha = \text{otype}(\mathcal{A})$ and $\beta = \text{otype}(\mathcal{B})$. We seek a worder of otype β^α. The idea is to use f to design a wellordering whose carrier set is $A \times B$ and whose order type is β^α.

Now the carrier set of the obvious worder of otype β^α is the set of functions of finite support from A to B. Such functions are finite objects, and can be thought of as finite subsets of $B \times A$. Now the set of finite subsets of $B \times A$ is (definably) in 1-1 bijection with $B \times A$. Now by judicious use of Cantor-Bernstein there will be a bijection between $B \times A$ and the set of functions of finite support from A to B. Then we can copy onto $A \times B$ the order (which we have not yet, as it happens, mentioned) that lives on the set of functions of finite support from A to B.

Now! What about the next operation after exponentiation?

And one needs to find something sensible to say about why the next operation $\hat{}\,\hat{}$ in Doner-Tarski does not have a synthetic definition. I think the first tho'rt will be that the number of levels needed to house/express $n \hat{}\,\hat{}\, m$ is not a constant given by $\hat{}\,\hat{}$ but increases with m. So this operation is certainly not anything that lives inside $\mathcal{P}^k(M \sqcup N)$ for any finite k.

Have i got this definition right...?

$$\alpha \hat{}\,\hat{}\, 0 = 1; \quad \alpha \hat{}\,\hat{}\, (\beta + 1) = \alpha^{(\alpha \hat{}\,\hat{}\, \beta)}$$

Let's check.... One has to be more careful than with + and $\times$, beco's (unlike them) *exp* is not commutative, so $\alpha^{(\alpha \hat{}\,\hat{}\, \beta)}$ is not the same as $(\alpha \hat{}\,\hat{}\, \beta)^\alpha$ and we'd better use the correct one. On the first account we have

$$\alpha \hat{}\,\hat{}\, 1 = \alpha^{(\alpha \hat{}\,\hat{}\, 0)} = \alpha^1 = \alpha$$
$$\alpha \hat{}\,\hat{}\, 2 = \alpha^{(\alpha \hat{}\,\hat{}\, 1)} = \alpha^\alpha$$
$$\alpha \hat{}\,\hat{}\, 3 = \alpha^{(\alpha \hat{}\,\hat{}\, 2)} = \alpha^{\alpha^\alpha}$$

This matches "tetration" (a word i have only just learnt!) on $\mathbb{N}$, so we're looking good.

On the second account we get

$\alpha\hat{}\hat{}0 = \alpha$ (to kick things off, α instead of 1)

$\alpha\hat{}\hat{}1 = (\alpha\hat{}\hat{}0)^\alpha = \alpha^\alpha$

$\alpha\hat{}\hat{}2 = (\alpha\hat{}\hat{}1)^\alpha = (\alpha^\alpha)^\alpha = \alpha^{(\alpha^2)}$

The first definition makes $\alpha\hat{}\hat{}\omega$ equal to a tower of αs of height ω, and then $\alpha\hat{}\hat{}(\omega + 1)$ is α to the power of that tower, giving $\alpha\hat{}\hat{}\omega = \alpha\hat{}\hat{}(\omega + 1)$, and that contradicts the requirement that every DT function be strictly increasing. So we want the second definition. What worries me about this is that it conflicts with the definition of "tetration" on $\mathbb{N}$. This needs to be investigated.

We do need to think about after-exponentiation. $\alpha\hat{}\hat{}\beta = \gamma$ gets translated into the language $\mathcal{L}(\in$, pairing, unpairing). But since $\alpha\hat{}\hat{}\beta$ has no synthetic definition the translation is going to involve a recursion with quantifiers over sets of wellorderings. One should really spell this out properly... and that's the kind of thing i can no longer do, what with my multiple-infarct dementia. But let's try anyway.

$\alpha\hat{}\hat{}\beta = \gamma$ is going to be some three-place relation with '$\langle A, <_A\rangle$', '$\langle B, <_B\rangle$' and '$\langle C, <_C\rangle$' occupying the three slots. Every set that contains a triple

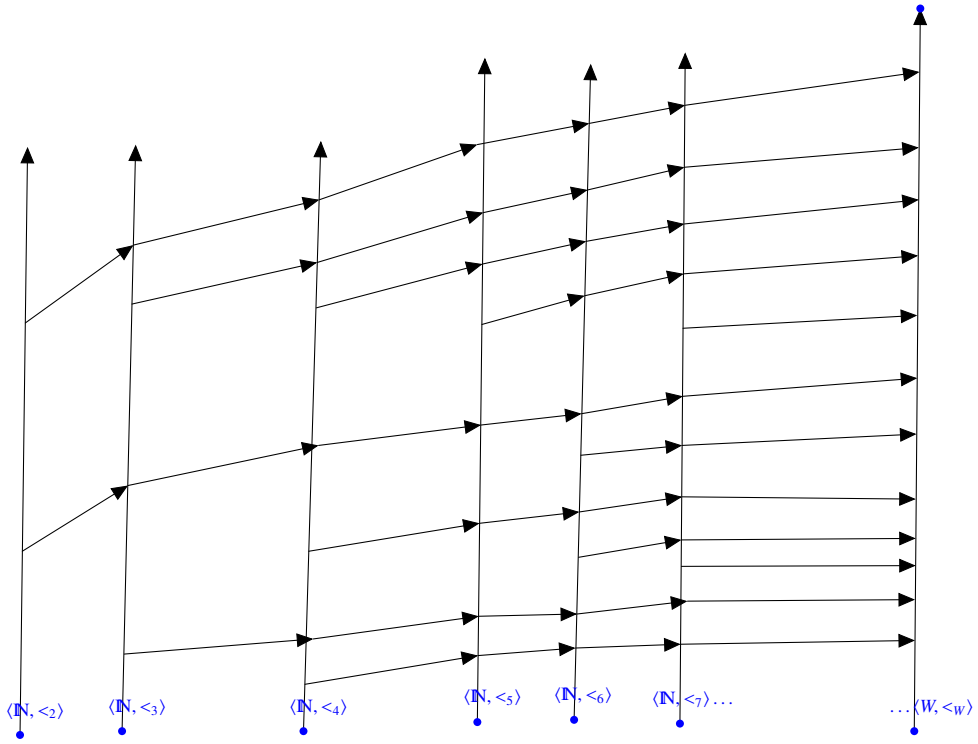
$\langle\langle A, <_A\rangle, \langle B, <_B\rangle, \langle C', <_{C'}\rangle\rangle$ with $\langle C', <_{C'}\rangle \simeq \langle C', <_{C'}\rangle$

that is closed under something or other contains a triple of suitable zero objects.

We'd better complete Goodstein's [putative] project by showing a converse to 9, namely that if the nondeterministic Goodstein function is total then PA is consistent.

REMARK 10 *There is a definable total ordering of* $\mathbb{N}$ *with the property that it is of length* ϵ_0 *if every nonterminating run of the nondeterministic Goodstein function has only finitely many decrements.*

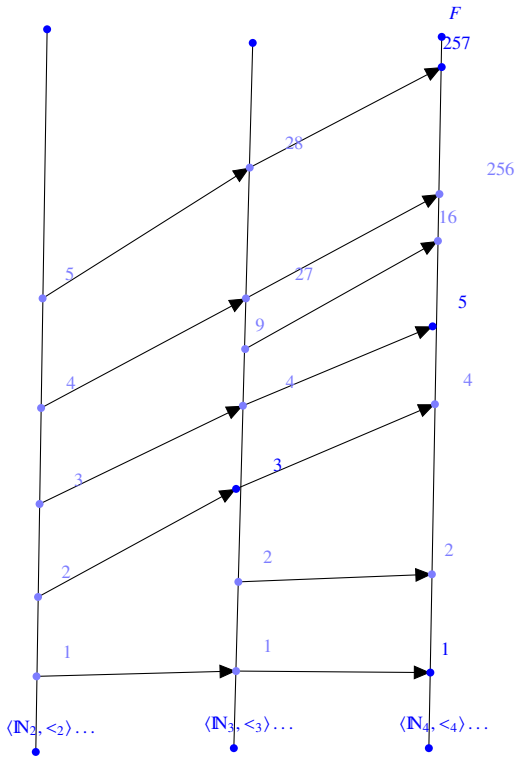
Proof:



We construct the total order as a direct limit. In fact it will be not merely definable but also actually decidable. And we can exhibit it without the assumption that the nondeterministic Goodstein functions is total; we don't need that assumption until we attempt to prove that the ordering is a *well*ordering.

Let $\langle\langle \mathbb{N}_n, <_n\rangle : 2 \leq n < \omega\rangle$ be a family of copies of $\langle \mathbb{N}, <_{\mathbb{N}}\rangle$. Define, for each $2 \leq n < \omega$, an injective homomorphism $i_n : \mathbb{N}_n \hookrightarrow \mathbb{N}_{n+1}$ as follows. Given $y \in \mathbb{N}_n$, think of it as written in ϵxtended base n. Then replace every 'n' by '$n + 1$'; this number is to be our value of $i_n(y)$. Now consider the direct limit ("colimit") of this system, which we will call $\langle W, \leq_w\rangle$. Every element of the direct limit $\langle W, <_W\rangle$ is an ω-sequence of natural numbers. Indeed any such sequence is a *computable* function, and thus a natural number, so W is clearly countable. (Actually – assuming countable choice – a direct limit of countably many countable structures is always countable, but never mind). However we will continue to think of elements of W as functions.

Thus, as *per* the slightly more detailed figure that follows, i_2 sends 1 to 1, sends 2 to 3, sends 3 (= 2 + 1) to 4 (= 3 + 1), sends 4 (= 2^2) to 27 (= 3^3), sends 5 (= 2^2 + 1) to 28 (= 3^3 + 1) and so on. Similarly i_3 sends 1 to 1, 2 (= 1 + 1) to 2, sends 3 to 4, sends 4 to 5, sends 9 (= 3^{1+1}) to 16 . . .



Each member of W is a function from a terminal segment of $\mathbb{N}$, typically a *proper* terminal segment. Consider $\mathbb{N}_3$ for example. The only numbers in $\mathbb{N}_3$ that are in the range of i_2 are sums of distinct powers of 3 (since they arise by replacing '2' by '3' in the ϵxtended base 2 representation of something). The sequence that is to become the finite ordinal n in $\langle W, <_W\rangle$ is a sequence that starts at $\mathbb{N}_{n+1}$.

If $<_W$ is illfounded there will be a descending ω-sequence. (We do not need DC for this, since the carrier set is wellordered, being a subset of $\mathbb{N}$.)

Suppose $f_i : i < \omega$ is a descending sequence in $\langle W, <_W\rangle$. Every f_i, being a member of W, is an ω-sequence, and it starts at $\mathbb{N}_i$ for some i. Without loss of generality we can pass to a subsequence of f so that the sequence of is s.t. members of the sequence start at $\mathbb{N}_i$ form an increasing sequence. Recall that we are thinking of the f_i as functions on terminal proper segments of $\mathbb{N}$, so that $f_i(n)$ is not defined if f_i first appears at $\mathbb{N}_j$ with $j > i$. Given this family $f_i : i < \omega$ consider the evaluation sequence g for the modified G function (so that $g(n) \in \mathbb{N}_n$ for all n) defined as follows. Set $g(0)$ to be some natural large enough to ensure that $g(j) > f_1(j)$, where $\mathbb{N}_j$ is the copy of $\mathbb{N}$ where f_1 first appears. The idea is that g decrements only when a new f_i appears. That is to say, $g(n+1) =: i_n(g(n))$ unless $\mathbb{N}_{n+1}$ is one of those copies of $\mathbb{N}$ at which a new f_j starts, in which case $g(n+1) =: i_n(g(n)) - 1$.

It may well be that, for all f_n, it happens that for sufficiently large values of m we have $g(m) <_m f_n(m)$, but the values of m for which this first happens increase

monotonically with n. This means that any function f in W that lies entirely $<_W$-below all the f_i must lie $<_W$-below g. But, by assumption on g, f now must be the zero element of W.

Finally we have to check that the order type of $<_W$ is indeed ϵ_0. To do this, we have to find, for any ordinal $\alpha < \epsilon_0$, a sequence which is a member of W to which it corresponds. Every ordinal $\alpha < \epsilon_0$ has a Cantor normal form $\mathfrak{C}(\alpha)$, which is a finite string of characters, so there is an upper bound a on the natural numbers that appear in $\mathfrak{C}(\alpha)$. The ω-sequence that will correspond to α starts in $\mathbb{N}_a$.

■

Recall at this point the results of chapter **??**, (for example theorem **??**) where we saw how natural assertions that certain functions are total can turn out to be unprovable. What remark 10 gives us is a specific function whose totality implies the consistency of PA.

It seems pretty obvious that the Goodstein function is monotone increasing. However we have to open a can of worms if we want to prove it. This introduces a new topic.

7.3 Hierarchies of fast-growing functions

Need the concept of *predecessor* function; $P_n(\alpha)$

Look at the picture on page 75. P_n is the function you need if you are to obtain the $n+1$th ordinal in the right-hand column from the nth ordinal in the right-hand column: P_n of the nth ordinal in the right-hand column is the $n+1$th ordinal in the right-hand column. To be precise:

$P_n(0) := 0;$
$P_n(\alpha + 1) := \alpha;$
$P_n(\lambda) := P_n(\lambda_n).$

...where λ_n is the nth member of the fundamental sequence for λ. Fundamental sequences (see for example Q 10 on Professor Leader's second example sheet from Part II Logic and Set Theory in 2015) go back to Hardy [15], an article rediscovered by Kreisel, Löb and Wainer. 'P' for *p*redecessor. We need another auxilliary function:

$H_0(n) := n;$
$H_\alpha(n) := H_{P_n(\alpha)}(n+1);$
$H_\lambda(n) := H_{\lambda_n}(n).$

and a function ord: $\mathbb{N} \times \mathbb{N} \to \omega_1$ defined so that $\mathrm{ord}(n, m)$ is the ordinal you obtain by writing m in ϵxtended base n and then replacing all the 'n's by 'ω'.

We'd better check that if we replace H_0 by any strictly increasing function $f : \mathbb{N} \to \mathbb{N}$ with $(\exists k \in \mathbb{N})(\forall n \in \mathbb{N})(f(n) < n \cdot k)$ then we get the same dominance behaviour. This could make an exercise.

The significance of H is as follows:

Evaluate $H_{\mathrm{ord}(k,2)}(2)$. First step gives $H_{P_2(\mathrm{ord}(k,2))}(3)$; then we get, successively:

$H_{P_3(P_2(\mathrm{ord}(k,2)))}(4)$;
$H_{P_4(P_3(P_2(\mathrm{ord}(k,2))))}(5)$;
$H_{P_5(P_4(P_3(P_2(\mathrm{ord}(k,2)))))}(6)$;

$\vdots$

and this continues until we reach an n such that $P_n(P_{n-1}(\ldots(\mathrm{ord}(k,2))(n+1)\ldots)) = 0$, at which point we return the answer $n+1$. The 'n' works like a kind of `count` variable that records the length of the evaluation sequence so far. Thus $H_{\mathrm{ord}(k,2)}(2)$ is the length of the descending sequence of ordinals in the right-hand column, starting with $\mathrm{ord}(k,2)$, which is to say, it is $G(k)$. Hang on to this fact: it's useful!

$$G(k) = H_{\mathrm{ord}(k,2)}(2).$$

REMARK 11 *If G is total, so too is H_α for every $\alpha < \epsilon_0$.*

Proof:
We prove by induction on $\mathbb{N}$ that $(\forall \alpha < \epsilon_0)(H_\alpha(n)\!\downarrow)$.

Assume G is total. That is to say $H_\alpha(2)\!\downarrow$, for all $\alpha < \epsilon_0$. That takes care of the base case, $n = 2$.

Induction step: Suppose true for all $\alpha < \epsilon_0$ that $H_\alpha(n)\!\downarrow$; we will show by UG on 'α' that the same goes for $n+1$. Let α be arbitrary. We want $H_\alpha(n+1)\!\downarrow$. But $H_\alpha(n+1) = H_{\alpha+1}(n)$ and the RHS is defined by induction hypothesis on 'n'. ■

This is clear enough, but it involves reasoning explicitly about ordinals. What are the chances of reproducing this proof (or anything like it) in a theory of natural numbers? Well, instead of ordinals-below-ϵ_0, we can reason about (gnumbers of) *character strings for* ordinals-below-ϵ_0. It is simple enough to define a set of natural numbers that are codes for ordinals-below-ϵ_0, and it is clear that this set will be decidable. We can even define an order $<'$ on the codes which (seen from outside) orders them like the ordinals below ϵ_0. The tricky part is justifying induction on $<'$. That is to say, the challenge is to prove all instances of

$$(\forall n)[(\forall m <' n)(\phi(m)) \to \phi(n)] \to (\forall n)(\phi(n))$$

How might we prove this? One naturally expects to use induction of some sort. The only kind of induction that we have straightforwardly available is mathematical induction. It is true that transfinite induction over $\mathbb{N}^2$ can be simulated by a nested induction ("inner loop") as in the second proof of totality of Ackermann (theorem **??**) but that technique offers hope only for ordinals below ω^ω.

We cannot in fact do this in Peano Arithmetic, and the reason is that transfinite induction up to ϵ_0 enables us to prove the consistency of Peano Arithmetic.

The Hardy hierarchy is a hierarchy of functions $\mathbb{N} \to \mathbb{N}$ each one dominating all previous ones. There is also ...

DEFINITION 24 *The Fast-Growing hierarchy.*

$F_0(x) := x + 1$;
$F_{\alpha+1}(x) := F_\alpha{}^{x+1}(x)$;
$F_\lambda(x) = F_{(\mathcal{F}\ \lambda\ x)}(x)$.

(I shall use capital 'F' rather than lower-case 'f' to forestall confusion with the Doner-Tarski hierarchy from p. 22.) The fast-growing hierarchy with *finite* subscripts is the **Grzegorczyk** hierarchy from [**?**].[10]

It turns out that

REMARK 12 $(\forall\alpha)(F_\alpha = H_{\omega^\alpha})$

EXERCISE 13 *(*)*

Think of the fast-growing hierarchy as a function F from the second number class to Baire space, $\mathbb{N}^\mathbb{N}$. *Both these spaces have natural topologies: the second number class has the order topology and* $\mathbb{N}^\mathbb{N}$ *can be thought of as the product (with the product topology) of countably many copies of* $\mathbb{N}$ *(with the discrete topology).*

Is F continuous with respect to these topologies?

There is an obvious possibility of proving by induction on the ordinal subscript that every H_α is total. What one has to think about is the formal system in which such a proof might be couched.

Just to reassure myself that I am in familiar surroundings I shall prove

REMARK 13 *For* $\alpha < \omega$, F_α *is primitive recursive.*

Proof:

Clearly true for $\alpha = 0$. Define `iter` g so that $\texttt{iter}(g, n) : m \mapsto (g^n(m))$ by means of the following declaration:

$$\texttt{iter}(f, 0)\ m := m;\ \texttt{iter}(f, (n + 1))\ m := f(\texttt{iter}(f, n)\ m)$$

we see that $\texttt{iter}(g, n)$ is primitive recursive as long as g is. Then

$$F_{\alpha+1} : n \mapsto \texttt{iter}(F_\alpha, n + 1)\ n$$

is primitive recursive as long as F_α is.

■

Indeed there is even a converse: we can show – by analogy with the proof that the Ackermann function dominates all primitive recursive functions – that every primitive recursive function is dominated by an F_n with $n < \omega$.

EXERCISE 14 *Complete this proof sketch from Stan Wainer.*

[10] I want a medal for spelling this name correctly. Craig McKay (my first Logic teacher) told me that Grzegorczyk was usually known in the West as 'G' – not because he was a spymaster but merely in order to sidestep the challenge to which I have just risen.

> *"For the primitive recursive bounding, you can show that if $f(0,a) = g(a)$ and $f(x+1,a) = h(x,a,f(x,a))$ where both g and h are assumed to be bounded by F_n, then $f(x,a) < F_n(F_n(F_n \ldots (F_n(a+x)\ldots)$ with $x+1$ iterates of F_n (or something like this). Then you get $< F_nF_nF_n...F_nF_n$ (max($\{x,a\}$)) with one extra iterate, since $F_n(b) > 2b$ for $n > 0$.*
>
> *Since $F_{n+1}(x) = F_n$ iterated $x+1$ times on x, this yields $f(x,a) < F_{n+1}(max\{x,a\}) < F_\omega(max\{x,a\})$ for $max\{x,a\} > n$. F_ω is a version of Ackermann, as can be shown fairly easily by comparison with the original."*

The Goodstein function is roughly F_{ϵ_0}. The modified version where you use base 2 not ϵxtended base 2 (so you leave the exponents alone) corresponds to F_{ω^ω}.

7.3.1 Good behaviour of the F_α, and the Schmidt conditions

We would like to establish that every F_α is strictly increasing and F_α dominates F_β whenever $\alpha > \beta$. However this is actually quite tricky, and the attempt to secure it gives rise to very subtle conditions on fundamental sequences. It turns out that – for ordinals below ϵ_0 – all the conditions one needs are in fact satisfied by the "obvious" system of fundamental sequences.

Might it be a good idea to think of a family of fundamental sequences as a three-place relation on the ordinals?

EXERCISE 15 *For α an ordinal, let α' be the least ordinal that is the length of a terminal segment of a wellordering of length α. Prove that α' is always a power of ω.*

EXERCISE 16 *(*)*

1. *Characterise the "obvious" system of fundamental sequences for ordinals below ϵ_0.*
2. *Establish that, using those fundamental sequences, F_α is strictly increasing and F_α dominates F_β whenever $\beta < \alpha < \epsilon_0$.*

This will lead us to the Schmidt conditions from [22].

7.3.2 Schmidt-coherence

Now we return to the endeavour of showing that a sequence of functions defined in the style of definition **??** will be monotone increasing with each function dominating all earlier ones. The idea is to prove by induction on α that f_α is monotone increasing and dominates all earlier f_β. Given the induction hypothesis it's easy to prove that f_α dominates all earlier f_β. Suppose f_{α_i} is strictly increasing for each $i \in \mathbb{N}$ and later fs dominate earlier fs. If f_α is $\lambda n.f_{\alpha_n}(n)$ then it dominates every α_i. Why isn't strict monotonicity obvious too? If f_α is strictly increasing so is $f_{\alpha+1}$. The hard case is that of limit ordinals.

We want

$f_\lambda\ n < f_\lambda(n+1)$. This holds iff

$f_{\lambda_n}\ n < f_{\lambda_{n+1}}(n+1)$. But

$f_{\lambda_n}\ n < f_{\lambda_n}(n+1)$

because f_{λ_n} is strictly increasing by induction hypothesis. Then to complete the proof it will suffice to show

$$f_{\lambda_n}\ (n+1) < f_{\lambda_{n+1}}(n+1)$$

which will follow if $(\forall\lambda\forall n)(S(\lambda_n, \lambda_{n+1}))$ where $S(\alpha,\beta)$ is:

$$\alpha < \beta \to (\forall m)(f_\alpha\ m < f_\beta\ m).$$

Now this clearly isn't going to happen: otherwise what could $f_\omega(0)$ possibly be? Duh! What one can ask for is that $f_{\lambda_{n+1}}$ has overtaken f_{λ_n} by the time argument $n+1$ comes along. This we can bring about by controlling our choices of λ_n.

The construction of the f_αs ensures that $S(\alpha,\beta)$ holds if $\beta = \alpha + 1$ or if β is limit and $\alpha = \beta_0$. To be sure of $S(\alpha,\beta)$ when $\alpha < \beta$ are members of a fundamental sequence we need to specify that they are related by the transitive closure of the union of these two relations. A family of fundamental sequences satisfying this condition is **Schmidt-coherent**.

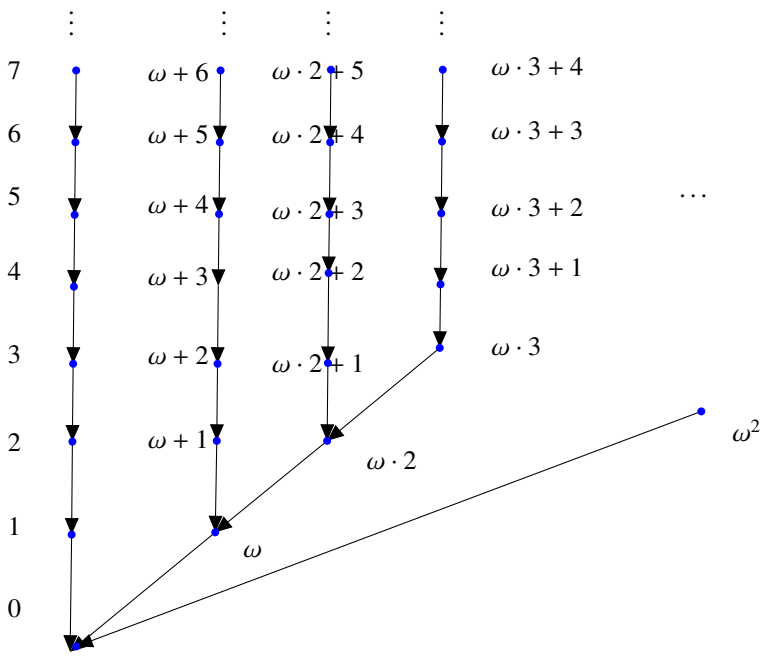
Formally:

DEFINITION 25 *Let $\mathcal{F} : \Delta \to \Delta^\omega$ be an assignment of fundamental sequences to an initial segment Δ of the second number class.*

Define the **step-down** *function $f : \Delta \to \Delta$ by*

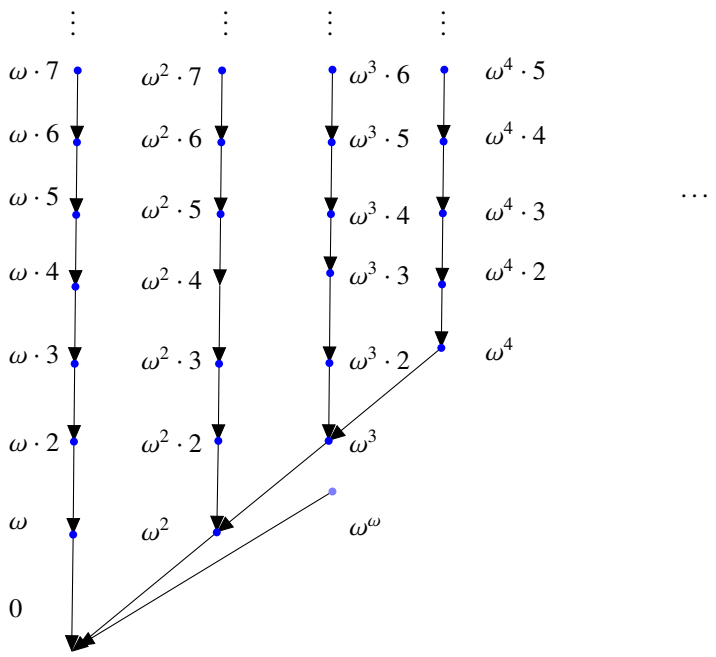
$$\texttt{if}\ \beta = \alpha + 1\ \texttt{then}\ \alpha\ \texttt{else}\ \mathcal{F}\beta\ 0$$

and $f(0)$ is of course undefined.



We can think of f as a digraph, in which all paths lead to 0. If we do this then we can see that it is actually a tree, and a tree with no infinite descending paths. Any digraph like that is of course also the graph of a transitive relation, and if we reverse the arrows we obtain the Hasse diagram of a wellfounded (strict) partial order.

If we zoom out a bit and show only the branches consisting entirely of limit ordinals we get



[Is every wellfounded partial order on a set an intersection of two wellorderings of that set?]

This order is written $<_{\mathcal{F}}$ by Schmidt [22] – who calls it the step-down relation *of $\mathcal{F}$.*

Then

$\mathcal{F}$ is **Schmidt-coherent** *iff*

$$(\forall \lambda \in \Delta)(\lambda \textit{ limit} \rightarrow (\forall n \in \mathbb{N})((\mathcal{F}\ \lambda\ n) <_{\mathcal{F}} (\mathcal{F}\ \lambda\ (n+1)))).$$

Equivalently: every fundamental sequence lies entirely within one branch of the tree.

The first picture is $<_{\mathcal{F}}$ restricted to ordinals below ω^2. The ordinals in this picture are a fundamental sequence for the first ordinal not so far seen, which is ω^2, so we put ω^2 on the end of a new sprout coming off 0, to its right. We can now put in the ordinals below ω^ω, as in the second picture.

Is there an identifiable wellfounded tree such that a family of fundamental sequences is just a decoration of this tree? branches thru' the tree are limit ordinals. This give a topology on the limit ordinals. Is this the same as the order topology?

EXERCISE 17 *In exercise 16 you defined the natural assignment of fundamental sequences to ordinals below ϵ_0: check that it is Schmidt-coherent.*

Now define a natural assignment of fundamental sequences to the ordinals below Γ_0, and check that that, too, is Schmidt-coherent.

We are now in a position to prove

THEOREM 17 *(Schmidt, [22] theorem 1)*
Consider the conditions:

(a) F_0 *is strictly monotonic;*
(b) if F_α *is strictly monotonic so is* $F_{\alpha+1}$*, and* $F_\alpha(0) \leq F_{\alpha+1}(0)$*, and* $F_\alpha(x) \leq F_{\alpha+1}(x)$*;*
(c) $F_\lambda(n) = F_{\lambda_n}(n)$ *when* λ *is limit.*

If the system $\mathcal{F}$ *defined on the initial segment* Δ *satisfies conditions (a), (b) and (c) and is Schmidt-coherent then, for each* $\alpha \in \Delta$*,*

(i) F_α *is strictly monotonic, and*
(ii) if α *is a limit ordinal then*

$F_{\alpha_n}(0) < F_{\alpha_{n+1}}(0)$
and
$F_{\alpha_n}(x) \leq F_{\alpha_{n+1}}(x)$.

Proof:
We show by transfinite induction on α that, for each $\alpha \in \Delta$,
(i) holds and
(iii) $\beta <_{\mathcal{F}} \alpha \rightarrow F_\beta(0) \leq F_\alpha(0); \beta <_{\mathcal{F}} \alpha \rightarrow F_\beta(x) < F_\alpha(x)$
[(ii) follows from (iii) because $\mathcal{F}$ is Schmidt-coherent.]

The case $\alpha = 0$ is easy.

Suppose $\alpha = \gamma + 1$: By induction hypothesis, (i) holds for γ; hence, by (b), it also holds for α.

By (b), (iii) holds if $\beta = \gamma$; but $\beta <_{\mathcal{F}} \alpha$ iff $\beta = \gamma \vee \beta \leq_{\mathcal{F}} \gamma$; hence, by (iii) of the induction hypothesis, (iii) holds for all $\beta <_{\mathcal{F}} \alpha$.

α a limit ordinal:
For each $x \in \mathbb{N}$ $F_\alpha(x) = F_{\alpha_x}(x) \leq F_{\alpha_{x+1}}(x)$ by (iii) of the induction hypothesis
$< F_{\alpha_{x+1}}(x+1)$ by (i) of the induction hypothesis
$= F_\alpha(x+1)$.

Hence (i) holds. Moreover, if $0 < x < \omega$, $F_{\alpha_0}(x) < F_{\alpha_x}(x) = F_\alpha(x)$, by (iii) of the induction hypothesis, since $\mathcal{F}$ is Schmidt-coherent; but $\beta <_{\mathcal{F}} \alpha \longleftrightarrow \beta = \alpha_0 \vee \beta <_{\mathcal{F}} \alpha_0$; hence – by (iii) of the induction hypothesis – $\beta <_{\mathcal{F}} \alpha \rightarrow F_\beta(x) < F_\alpha(x)$.

Also, $\beta <_{\mathcal{F}} \alpha \rightarrow \beta <_{\mathcal{F}} \alpha_0 \vee \beta = \alpha_0$ which implies $F_\beta(0) \leq F_{\alpha_0}(0) = F_\alpha(0)$, by (iii) of the induction hypothesis.

Thus (iii) holds for a.

■

The following is from [22], but the proof is due to Nathan Bowler.

THEOREM 18 *For every proper initial segment Δ of the second number class there is a [are uncountably many, in fact] Schmidt-coherent system of fundamental sequences for the limit ordinals in Δ.*

Proof:

Let f be a bijection $\mathbb{N} \longleftrightarrow \{\beta : \beta < \alpha\}$ for some countable ordinal α, satisfying $f(0) = 0$. Suppose that $f(k)$ is a limit ordinal. We define a sequence $\langle s^k_n : n \in \mathbb{N}\rangle$ as follows

- s^k_0 is that element of $\{i < k : f(i) < f(k)\}$ on which the value of f is maximal.
- s^k_{n+1} is the minimal element of $\{i \in \mathbb{N} : f(s^k_n) < f(i) < f(k)\}$.

It follows that

(a) $s^k_0 < k$;
(b) For any i with $f(s^k_0) < f(i) < f(k)$, we have $i > k$;
(c) For any $n \in \mathbb{N}$ and any i with $f(s^k_n) < f(i) < f(k)$, we have $i > s^k_n$;
(d) The sequence $\langle f(s^k_n) : n \in \mathbb{N}\rangle$ is strictly increasing with limit $f(k)$.

(d) says that $\langle f(s^k_n) : n \in \mathbb{N}\rangle$ is a fundamental sequence for $f(k)$. We take these sequences as the elements of our system of fundamental sequences for the limit ordinals below α. Let σ be the corresponding step-down function, and define $\delta : \mathbb{N} \to \mathbb{N}$ so that $\sigma \cdot f = f \cdot \delta$. Thus when $k \in \mathbb{N}$ is such that $f(k)$ is limit we have $\delta(k) = s^k_0$. We must show that, for any limit ordinal $\beta < \alpha$ and any γ in the fundamental sequence for β, the sequence $\langle \sigma^n(\gamma) : n \in \mathbb{N}\rangle$ run through all lower members of that fundamental sequence. To establish this, it will suffice to prove the following

LEMMA 12 *Let k be such that $f(k)$ is a limit ordinal, let $n \in \mathbb{N}$ and $i \in \mathbb{N}$ be such that $f(s^k_n) < f(i) < f(k)$. Then $\delta(s^k_n) \leq \sigma(f(i))$.*

Proof:

This is immediate if $f(i)$ is successor, so suppose it is limit. So $\sigma(f(i)) = f(\delta(i)) = f(s^i_0)$. By (c) above we have $s^k_n < i$, and by assumption we have $f(s^k_n) < f(i)$, so by definition of s^i_0 we have $f(s^k_n) \leq f(s^i_0) = \sigma(f(i))$. ■

REMARK 14 *There is no definable family of fundamental sequences for all $\alpha < \omega_1$.*

Some duplication

Proof:

Suppose $\mathcal{F}$ were such a family. We then define by recursion on ω_1 a sequence $\langle W_\alpha : \alpha < \omega_1\rangle$ of wellorderings of $\mathbb{N}$ (so each is a subset of $\mathbb{N}\times\mathbb{N}$). 0 is easy, successor steps are easy; at a limit λ use the fundamental sequence $\mathcal{F}\lambda$, to get the codes $W_{\mathcal{F}\lambda n}$ you have already formed for each $\mathcal{F}\lambda n$ and then piece them all together one after the other to get a wellordering of $\mathbb{N} \times \mathbb{N}$. Use a bijection $\mathbb{N} \times \mathbb{N} \longleftrightarrow \mathbb{N}$ to turn this into a code for $\Sigma_{n\in\mathbb{N}}\mathcal{F}\lambda n$ – which may have overshot the mark, so take the right initial segment and you have a code for λ. (The *sum* of a sequence of ordinals might be bigger than its sup). None of this uses any AC.

This shows that if we have a function assigning a fundamental sequence to every countable ordinal, then we have a function assigning to each countable ordinal a wellordering of $\mathbb{N}\times\mathbb{N}$. But any wellordering of $\mathbb{N}\times\mathbb{N}$ is coded by a real number so this implies $\aleph_1 \leq 2^{\aleph_0}$. It is known that this is independent of ZF. ■

(I think that when (in [15]) Hardy introduced the Hardy Hierarchy – of which more later – he was trying to solve the continuum problem)

Suppose there is a function $g : \mathbb{N} \to \mathbb{N}$ that dominates all f_α. Then, for each $n \in \mathbb{N}$, let $h(n)$ be the sup of the αs such that g has permanently overtaken f_α by stage n. h is clearly nondecreasing. For every α there is $n \in \mathbb{N}$ s.t. $h(n) \geq \alpha$, so h is unbounded below ω_1, and is an ω-sequence of countable ordinals whose sup is ω_1, contradicting countable choice.

This shows that if we assume countable choice (or merely that ω_1 is regular) then there cannot be a Schmidt-coherent system of fundamental sequences for the whole of the second number class.

> Rose says that theorem 13 is best possible, and credits [**?**] I'm sceptical about this because he also says that Schmidt, too, proves that it is best possible – and she doesn't!
>
> If it really is best possible, it's presumably because a Schmidt-coherent family for all countable ordinals would give us an embedding of ω_1 into the reals, or something like that. There can be long sequences ($\geq \omega_1$) of functions with each function dominating all earlier functions, but they don't increase as fast as Wainer-Buchholtz.

Chapter 8

Fast-growing Functions and Complex Analysis

8.1 Why is there (apparently) no connection between fast-growing functions $\mathbb{N} \to \mathbb{N}$ and Complex Analysis?

For any countable ordinal we can find a system of fundamental sequences for limit ordinals below it. With the help of AC we can find a system of fundamental sequences for *all* countable ordinals. Any such system for an initial segment of the second number class puts flesh on the definition of the functions in the Hardy hierarchy (or any of the other hierarchies for that matter – this is only an illustration), so that we have an actual sequence of fast-growing functions. Every bounded set of countable ordinals can be injected into the reals in a more-or-less smooth way (again, we need choice if we want to embed the *whole* of the second number class) so we can think of the *entire* Hardy hierarchy as a *single* function $H : X \times \mathbb{N} \to \mathbb{N}$ for some $X \subseteq \mathbb{R}$. [Do not forget that there are two nontrivial inputs to this:
(i) the choice of a family of fundamental sequences and
(ii) the choice of an injection from the second number class into the reals]
There are surely things that can be said about what $X \subseteq \mathbb{R}$ must look like as a subset of $\mathbb{R}$ which could have some bearing on what follows, but i can't think of anything offhand. What H looks like will presumably depend sensitively on the choices made under headings (i) and (ii).

Clearly both the domain and the range of H can be naturally thought of as subsets of the complexes, so we can think of H as the restriction of a function from the complexes to the complexes – and probably in lots of ways. (This is where the nature of X might matter).

Are any of these ways analytic? And might they be informative? I'm making a fuss about the use of AC in this context beco's the arbitrariness of the choices we make might deny us the smoothness needed to make the extension of H to the complexes

analytic.

It is also possible to think of H as a function from the second number class to Baire space. The second number class has the order topology, and Baire space has the product topology. It's a relatively simple exercise to show that H is not continuous. I append a proof at the end of this file.

8.2 Finding analytic interpolants

REMARK 15 *Every H_α has an analytic continuation to a function $\mathbb{C} \to \mathbb{C}$ with a power series all of whose coefficients are real.*

Proof:

If H_α is to be continued to an analytic function on some simply connected $X \supseteq \mathbb{N}$ then X might as well be the whole of $\mathbb{C}$, in which case we will have a power series

$$\sum_{n\in\mathbb{N}}(\frac{z^n}{a(n)} + i \cdot \frac{z^n}{b(n)})$$

for such an analytic continuation, where the $a(n)$ and the $b(n)$ are all real. The existence of such an analytic continuation is assured by Pringsheim interpolation. We can rearrange to

$$\sum_{n\in\mathbb{N}} \frac{z^n}{a(n)} + \sum_{n\in\mathbb{N}} i \cdot \frac{z^n}{b(n)}.$$

Then $\sum_{n\in\mathbb{N}} i \cdot \frac{z^n}{b(n)}$ must be zero for $z \in \mathbb{N}$, so the power series $\sum_{n\in\mathbb{N}} \frac{z^n}{a(n)}$ is an analytic continuation of H_α with all coefficients in $\mathbb{R}$. ∎

There is this theorem of Carlson's [4] that says if $f : \mathbb{C} \to \mathbb{C}$ is analytic and dominated by an exponential function, and f"$\mathbb{N} = \{0\}$ then f is identically zero. This means that if $H_\alpha : \mathbb{N} \to \mathbb{N}$ has two analytic continuations f and g with $|f(n) - g(n)|$ bounded by an exponential then $f = g$. This sounds like a choice principle: being-within-an-exponential-bound-of-each-other is an equivalence relation. Each equivalence class contains precisely one analytic function!

If H_α is to be entire then we need $n \mapsto a(n)$ to dominate $z \mapsto z^n$ for every $n \in \mathbb{N}$. (I mean *dominate* in the sense that $\frac{z^n}{a(n)}$ tends to 0 fast enough for $\sum_{n\in\mathbb{N}} \frac{z^n}{a(n)}$ to converge.)

The exponential function of course in this sense dominates $z \mapsto z^n$ for every $n \in \mathbb{N}$, but there are plenty of functions dominated by the exponential function that still dominate $z \mapsto z^n$ for every $n \in \mathbb{N}$. Observe that, for each countable ordinal α, the sequence of coefficients of a power-series for H_α would be such a function; observe, too, that the more slowly the function $n \mapsto a(n)$ grows the faster the function $z \mapsto \sum_{n\in\mathbb{N}} \frac{z^n}{a(n)}$

grows. Thus the endeavour to find power series for each H_α commits us, at the very least, to finding – for each countable α, a descending α-sequence of such functions, all dominated by the exponential function, each dominating all later functions, and all of them dominating $z \mapsto z^n$ for all $n \in \mathbb{N}$. The crucial point here is that there can be no such descending ω_1-sequence (at least if each sequence of coefficients is eventually monotone) beco's we can't embed the second number class into $\mathbb{R}$. It would be nice to be able to exhibit a sequence of functions such that the corresponding power series all take naturals to naturals.

8.2.1 Diagonalisation

There is a diagonalisation step at limit ordinals in the definition of the Hardy hierarchy. It would be nice if there were a simple-minded (diagonal!) construction of the sequence of coefficients in the power series for H_λ.

This domination is an immediate echo of the definition of the Hardy hierarchy. We certainly desire that if, for each $k \in \mathbb{N}$, $n \mapsto a(k,n)$ dominates $z \mapsto z^n$ for every $n \in \mathbb{N}$, then $n \mapsto a(n,n)$ dominates $z \mapsto z^n$ for every $n \in \mathbb{N}$. We would clearly need, for each $k \in \mathbb{N}$, that the coefficients $(a(k,n))^{-1}$ to be monotone increasing. TWK thinks that if you want a power series where the coefficients are monotone decreasing then you may be asking too much.

He says one should look for a series where almost all coefficients are zero. [why?]

Consider, for example the power series for $z \mapsto 3^z$: the nth coefficient is $(\log(3))^n/n!$. *This* sequence is not monotone decreasing: the coefficient of z is less than the coefficient of z^2. Perhaps we mean *eventually* strictly decreasing.

However there is no reason to suppose that the diagonal power series $\sum_{n\in\mathbb{N}} \frac{z^n}{a(n,n)}$ takes values in $\mathbb{N}$ for arguments in $\mathbb{N}$ even if $\sum_{n\in\mathbb{N}} \frac{z^n}{a(k,n)}$ takes values in $\mathbb{N}$ for arguments in $\mathbb{N}$, for every $k \in \mathbb{N}$. There is also an echo of the Schmidt conditions from [22], in that we want the diagonal sequence $n \mapsto a(n,n)$ to be monotone increasing whenever the sequence $n \mapsto a(k,n)$ is monotone increasing for each k.

TWK makes the point that there are various diagonal arguments in connection with convergent series, but one usually gets to choose which element of the nth series one picks, subject to the constraint that the choices get later and later. Of course when one diagonalises over the Hardy functions to get one with a limit subscript it oughtn't to matter *how* one diagonalises (tho', annoyingly, it does).

Another thing: Pringsheim tells us that if we extend the Hardy hierarchy over all countable ordinals we will have power series for every one. This means that there is no way of making all those series *nice* beco's we cannot embed the second number class into $\mathbb{R}$ in an order-preserving way.

I think if the $a(n)$ are monotone increasing then the function

$$z \mapsto \sum_{n\in\mathbb{N}} \frac{z^n}{a(n)}$$

has no zeroes. The exponential function has no zeroes! So zeroes start appearing at the stage where the $\vec{a}$ cease to be monotone.

8.3 Afterthoughts

Think of the fast-growing hierarchy as a function F from the second number class to Baire space, $\mathbb{N}^{\mathbb{N}}$. Both these spaces have natural topologies: the second number class has the order topology and $\mathbb{N}^{\mathbb{N}}$ can be thought of as the product (with the product topology) of countably many copies of $\mathbb{N}$ (with the discrete topology).

Is F continuous with respect to these topologies?

Answer: No! (Thanks to Jonathan Holmes)

Suppose that F is continuous on some open interval I containing a limit ordinal λ. There is $\alpha \in I$ with $\alpha = \mu + \omega$ for some limit μ (possibly $\mu = 0$), and α may or may not be λ.

Choose a large enough so that $f_\mu(n) > n$ for all $n > a$. (*)

Let $U = \{g \in \mathbb{N}^{\mathbb{N}} : g(a) = f_\alpha(a)\}$.

U is open, so F^{-1}"U is open, and so contains an open interval J around α. Choose $\beta \in J$ with $\alpha > \beta > \mu$. $f_\beta(a) = f_\alpha(a)$ by assumption that $\beta \in J$.

Noting that $\beta = m + 1$ for some m, have $f_{\beta+1}(a) = f_\beta^m(a)$ where $m \notin \{0, 1\}$.

But $f_\beta^m(a) > f_\beta(a)$ since $f_\beta(a) = f_\mu^{(m-1)!}(a)$, $f_{\beta+1}(a) = f_\mu^{m!}(a)$, and – by (*) – the sequence $\langle f_\mu^k(a) : k \in \mathbb{N}\rangle$ is strictly increasing.

■

So the challenge is: given a strictly decreasing sequence $1/b(n)$ of coefficients of an everywhere absolutely convergent power series for $B(z)$ find a strictly decreasing sequence $1/a(n)$ (which will be the coefficients of a power series for $A(z)$) such that

(i) $B(z) < A(z)$ for all suff large naturals z and

(ii) $\sum_{n\in\mathbb{N}} z^n/a(n)$ is absolutely convergent everywhere

How do we get such an a?

We have to do this in such a way that when we diagonalise we get another sequence of coefficients of an absolutely convergent power series.

Deep Breath

What i now think is going on is this. If we want an ω_1-sequence of ever faster-growing fast-growing functions then without serious loss of generality we can think of them as $\mathbb{R} \to \mathbb{R}$ rather than $\mathbb{N} \to \mathbb{N}$, and as power series with real coefficients. For each such power series think of the sequence of denominators. This should be an increasing sequence (should it?) but the faster-growing the function the more slow-growing the sequence of denominators.

There are two things to think about

(i) What does the operation we do to the fast growing function to get the next fast-growing function do to the sequence of denominators? If we try anything like $f_{\alpha+1}(n) = f_\alpha(n^2)$ then the new power series has lots of zero coefficients

(ii) At limit stages when we define F_λ we have to use a fundamental sequence someohow. Presumably we do something similar to the seqence of sequences of coefficients

Anyway, after a while it ceases to be possible to ensure that the fast-growing functions are strictly increasing *and* that the denominators in the coefficients are strictly increasing. At that point you find that the fast growing-functions have zeroes somewhere in the complex plane.

8.4 Consistency strength measured by ordinals: a quotation from Quine

> Any not conspicuously deficient set theory can of course prove the existence of transfinite numbers without end, but this does not mean getting them all. What is so characteristic of the transfinite is that we then go on iterating the iteration, iterating the iteration of the iterations, and so on, until somehow our apparatus buckles; and the least transfinite number after the buckling of the apparatus is how strong the apparatus was.
>
> W.V.Quine: [20] pp 323-4

Maybe we should say something here about how the endeavour to achieve a complete consistent system of arithmetic by transfinitely adding Gödel sentences comes unstuck. Quite where it comes unstuck will presumably depend on the strength of the original system. For PA it comes unstuck at ϵ_0?

Chapter 9

Recursive Ordinals and wellorderings

Next a little lemma we shall need later.

A countable ordinal is an ordinal that is the length of a wellordering of $\mathbb{N}$ or of a subset of $\mathbb{N}$– it makes no difference. Cantor called the set of countable ordinals the *Second Number Class* (the first number class is $\mathbb{N}$). A *recursive* ordinal is an ordinal that is the length of a *recursive* [= decidable] wellordering of $\mathbb{N}$ or of a *recursive* [decidable] wellordering of a decidable subset of $\mathbb{N}$– it makes no difference: either way it's a wellordering whose graph (set of ordered pairs of natural numbers) is a recursive (= decidable) set. A decidable relation on a decidable infinite subset of $\mathbb{N}$ is isomorphic to a decidable relation on the whole of $\mathbb{N}$ because the function enumerating the decidable subset is itself decidable. (This was exercise **??** on p. **??**.)

There is a simple cardinality argument to the effect that not every countable ordinal is recursive. Rosser's extended axiom of counting (explain) tells us that the length of the wellordering of all the countable ordinals has uncountable length, so there are uncountably many (in fact precisely $\aleph_1$) countable ordinals. However the set of recursive ordinals is a surjective image of the set of all machines, and that set is countable. Clearly every recursive ordinal is countable, so there must be countable ordinals that are not recursive.

Is this really the right point to insert recursive ordinals?

DEFINITION 26
The sup of the recursive ordinals is the **Church-Kleene** ω_1*, aka* ω_1^{CK}.

A standard application of countable choice tells us that every countable set of countable ordinals is bounded below ω_1, so we know that ω_1^{CK} is actually a countable ordinal. But we can do much better than that, and without using the axiom of choice.

REMARK 16
The family of recursive ordinals is a proper initial segment of the second number class.

Proof:

Suppose $<_R$ is a wellordering of $\mathbb{N}$ whose graph is a decidable subset of $\mathbb{N} \times \mathbb{N}$. That is to say that the length of $<_R$ is a recursive ordinal. Now consider any ordinal α less than the length of R. This is the length of a proper initial segment of $<_R$ – the length of $<_R \restriction \{m \in \mathbb{N} : m <_R n\}$ for some n, say – and this initial segment of $<_R$ is a decidable subset of $\mathbb{N} \times \mathbb{N}$ (it has the number n as a parameter) and its length is therefore a recursive ordinal. ■

This means that ω_1^{CK} is not merely the sup of the recursive ordinals but the least *non*recursive ordinal – and this is indeed how it is usually defined.

REMARK 17 *Every recursive limit ordinal has cofinality ω – recursively. That is to say: whenever R is a decidable binary relation on $\mathbb{N}$ that wellorders $\mathbb{N}$ to a length that is a limit ordinal there is a decidable $X \subseteq \mathbb{N}$ s.t. $otp(R \restriction X) = \omega$.*

Proof: Recycle the usual "picking winners" proof that countable limit ordinals have cofinality ω. It works in this context. We enumerate the members of X in increasing order $x_0, x_1 \ldots$. We set $x_0 := 0$. Thereafter x_{n+1} is the least natural number x such that $\langle x_n, x\rangle \in R$. There is always such an x and it is always decidable for any candidate whether or not the candidate passes. This ensures that X is a semidecidable set which can be enumerated in increasing order, and this makes it decidable (by exercise **??**). ■

Observe that this proof is effective: there is a computable function which, on being given the gnumber of a characteristic function of a wellordering of $\mathbb{N}$, returns the gnumber of the characteristic function of an unbounded subset of length ω.

EXERCISE 18

*The class of recursive ordinals is closed under the Doner-Tarski function f_α (see definition **??** p. **??**) for every recursive ordinal α.*[1]

Is there a sense in which one can say that ω_1^{CK} is not recursively of cofinality ω? We need to think a bit about what this might mean. Suppose we have a wellordering R of $\mathbb{N}$ of length ω_1^{CK}. It's not a decidable set of ordered pairs. Now suppose this worder R had a cofinal subsequence of length ω that was decidable. This chops up $\langle \mathbb{N}, R\rangle$ into ω segments $\{r_n : n \in \mathbb{N}\}$ where, for each n, $r_n \subseteq \mathbb{N}$ and $R \restriction r_n$ is a worder of length less than ω_1^{CK}. This doesn't mean that $R \restriction r_n$ is a decidable set of ordered pairs, but it does at least mean that there is a decidable wellordering of $\mathbb{N}$ to that length. Since there are only countably many decidable worders of that length and they are naturally wordered by their gnumbers pick the first one, and concatenate them all. Altho' this process clearly gives us a worder of length ω_1^{CK} what i am now (on writing this down) less than 100% confident is that the worder we get is decidable. The more i think about this the less convinced i am.

[1] Come to think of it i'm not really entirely happy about this ... but Stan says it's obvious so it must be OK

> Stanley,
> I think i may have answered my own question (This always happens once one sticks one's head above the parapet and asks a stupid question - but that's what friends are for.)
> Can there be a worder of $\mathbb{N}$ of length ω_1^{CK} every initial segment of which is decidable? Suppose we have a a wellordering $<<$ of the Naturals of length ω_1^{CK} s.t. every proper initial segment of it is a recursive wellordering of some subset of $\mathbb{N}$. That subset will of course be decidable. Suppose further that there is a computable total function that, on being given n, returns a function f_n that when it is given a pair $\{x, y\}$ of naturals both $<< n$, tells us which is $<<$-first, and is undefined otherwise.
> This further condition makes $<<$ decidable. For suppose we want to know which of x and y is $<<$-earlier. We just zigzag across the f_n until we get an answer. Sooner or later we will calculate $f_n(\{x, y\})$ for some $n >> max\{x, y\}$ and since $<<$ is a total order we know we will get an answer. Also it doesn't matter which f_n is the first to halt, because they all agree.
> But i suppose there might be a wellordering $<<$ of the Naturals of length ω_1^{CK} s.t. every proper initial segment of it is a recursive wellordering of some subset of $\mathbb{N}$, but without the extra condition.
>
> Hiya Thomas!
> I'm pretty sure $<<$ cannot be decidable - your function f is only defined on n, $< x, y >$ provided x and y are both $<< n$. And anyway, you can't have a decidable well-ordering of length ω_1^{CK}. You seem to be looking for a path through Kleene's O such that every initial segment is a decidable (or even r.e.) well-order of a subset of $\mathbb{N}$. Of course such paths do exist but they're fairly complex. There are Π_1^1 ones, but any subrecursive hierarchy defined along them has to be incomplete (i.e. misses out some recursive function). And you can define such complete paths, but they can only be recursive in the set O itself. These are old results of Feferman (TAMS around 1962). Maybe I'm missing the point ..... am I?
> 'Best,
> Stan.

Thus ω_1^{CK} is *huge*. This is contrast to the corresponding ordinal for automatic structures: the least ordinal not the ordertype of an automatic wellordering is ω^ω, see [**?**]

Something to be alert to. Do not confuse the concept of a recursive ordinal with the concept of a *recursive pseudowellordering* of $\mathbb{N}$. This would be a decidable binary relation R on $\mathbb{N}$ which is a total order with the property that every decidable subset of $\mathbb{N}$ has an R-least member.

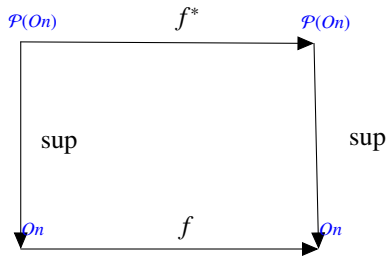
Here's another proof (Nathan Bowler) Consider an arbitrary initial segment of length β of a decidable total order of $\mathbb{N}$. It has a sup, n, say. Then the set of things below n is a decidable subset of $\mathbb{N}$, since the graph of the order relation is decidable. So throw away all ordered pairs that do not have both components in this initial segment. There is a recursive bijection between this initial segment and $\mathbb{N}$. Pull back to obtain a decidable worder of length β.

When reasoning inside a formal system of arithmetic care is needed in approaching the concept of recursive ordinal. It's one thing to have a definable binary relation on $\mathbb{N}$, it is quite another to have a proof that this definable binary relation is a wellorder. Come to think of it, how on earth can a system of first-order arithmetic (such as Peano Arithmetic) *ever* prove that a binary relation is wellfounded? After all, to show that a relation is wellfounded one has to be able to reason about all the subsets of its domain, and a first-order theory cannot reason about arbitrary subsets. The answer is that whenever T (being a first order theory of arithmetic) proves that a relation R on $\mathbb{N}$ is

a wellorder what is going on is that T proves all instances of R-recursion that can be expressed in the language of T.

9.1 Normal functions

Brief chat here about the order topology.
Need a picture
Surely some duplication??



As usual, a set is closed iff it contains all its limit points.

DEFINITION 27

A **clubset** *is a* **CL***osed and* **U***n***B***ounded set, or, alternatively, the range of a total continuous function.*

A **normal** *function f is*
(i) continuous: $f(\mathtt{sup}(A)) = \mathtt{sup}(f\text{“}A)$; and
(ii) strictly increasing: $\alpha < \beta \rightarrow f(\alpha) < f(\beta)$.

A clubset might be the range of lots of distinct continuous functions (repetitions are allowed, after all), but it is the range of only one *normal* function, to wit: the function that enumerates it. This bijection between the class of clubsets and the class of normal functions will be very useful to us. At times it will almost feel as if we have a datatype whose members can be thought of as clubsets and as normal functions at will. (cf page 41)

Clearly the derived set of a clubset is club.

It is easy to show that every normal function has a fixed point. If f is normal, then $\mathtt{sup}\{f^n\alpha : n \in \mathbb{N}\}$ is the least fixed point for f above α. In fact:

LEMMA 13 *The function enumerating the set of fixed points of a normal function is also normal.*

Proof:

This needs only the observation that if f is continuous then the sup of any set of fixed points for f is also fixed. ■

Notice that we can now define, in a completely straightforward way, a transfinite sequence of normal functions from the second number class into itself – or, indeed, from the class of all ordinals into itself. Let C_0 be the set of limit ordinals in the second number class, and $C_{\alpha+1}$ be the limit points of C_α. We say $C_{\alpha+1}$ is the **derived set** [from] C_α. Take intersections at limits. The sequence of C_αs is the sequence of derived sets. Now let f_α be the function that enumerates C_α. C_α is club so f_α is normal.

(It might be an idea to think about what these functions actually are.)

If f is a a normal function then for any ordinal α we can define a function f^α as follows:

$f^0(\beta) =? \ldots 1$, presumably

$$f^1(\beta) = f(\beta)$$

$$f^{\alpha+1}(\beta) = f(f^\alpha(\beta))$$

$$f^\lambda(\beta) = \sup\{f^\zeta(\beta) : \zeta < \lambda\}$$

Must check that f^α is normal if f is.

NB sez: if f = succ then $f^\omega(\omega) = \omega$ so f^ω is not strictly increasing and isn't normal; tf sez: this is because succ is not normal! $\mathtt{succ}^\alpha(\beta)$ is trying very hard to be $\beta + \alpha$

There is another way of defining unary functions from ordinals to ordinals that gives us – I was about to say *functions that are more rapidly increasing*. That wouldn't be quite correct: every function that is given by the second method is also given by the first method, but the first method takes longer to reach it.

The second method defines C_0 to be the set of limit ordinals in the second number class as before. We take intersections at limits as before. As before f_α will be the normal function that enumerates C_α. However now $C_{\alpha+1}$ is defined to be the set of fixed points of the normal function f_α that enumerates C_α.

(Notice that although the first method could have started with $C_0 =:$ second number class, the second method can't.)

We should think a bit here about what this new series of increasing functions look like.

There is a difference between these two ways of getting fast-growing functions that may strike a chord with people used to type disciplines. In the first case we can think of the ordinals that are arguments and the ordinals that are values as being two different types: green ordinals and blue ordinals.

In both cases we are indexing, by the ordinals, a family of ever-shrinking subsets of the ordinals. (We identify each skinny subset with the function that enumerates it). In both caes we take intersections at limits. In the first case the next set after A is the collection of limit points of A: we define a function from ordinals to sets of reals. $f(\alpha + 1)$ is the set of limit points of $f(\alpha)$. Nothing in this first construction compels us to think of the shrinking sets as shrinking sets *of ordinals*. Indeed in Cantor's original setting the derived sets are all sets of *reals* not sets of ordinals.

The difference between the first and second methods lies in the successor step. In the first construction the derived set at each stage is constrained to be a subset of the set it was derived from, so its members are objects of the same flavour that were found in that set, and that is the only constraint on their nature. However the second method exploits fixed points, so the functions it speaks of must have its arguments and its values of the same type. That means that the derived set must be a set of ordinals.

The first method is strongly typed and produces functions that don't grow very fast. The second method produces fast-growing functions much more efficiently but is less strongly typed. What we are seeing here is another instance of the way in which relaxation of typing disciplines makes for greater strength.

9.1.1 Cantor Normal Form using $\omega \uparrow\uparrow \alpha$

One obvious generalisation of CNF replaces the base ω by a different base. We exploited earlier the fact that ordinals above ϵ_0 but below ϵ_1 can be notated by a CNF with base ϵ_0. How else can we generalise?

Something that has always puzzled me is why the discovery that Cantor Normal form sometimes gives uninformative answers (think: ϵ_0) did not prompt the reflection that one should use the normal function after exponentiation as the gadget for a system of ordinal notations. After all, CNF uses exponentiation to base ω as a normal function that drives a "division algorithm", so why not just use the next normal function in the Doner-Tarski hierarchy? (Every normal function supports a division algorithm). Let's try this and see what happens; perhaps we shall learn from this exercise why Veblen and co^y escalated the struggle to notate ordinals by using this new gadget of enumerating fixed points rather than do what seems the obvious thing.

The next Doner-Tarski operation beyond exponentiation is declared by

$\beta \uparrow\uparrow 0 = \beta$;
$\beta \uparrow\uparrow (\alpha + 1) = (\beta \uparrow\uparrow \alpha)^\beta$;
taking sups at limits.

Thus $x \uparrow\uparrow 1 = x^x$; $x \uparrow\uparrow 2 = (x^x)^x = x^{x^2}$; $x \uparrow\uparrow 3 = (x^{x^2})^x = x^{x^3}$; and presumably $x \uparrow\uparrow n = x^{x^n}$ for $n \in \mathbb{N}$.

And, when $\beta = \omega$.

$\omega \uparrow\uparrow 0 = \omega$;
$\omega \uparrow\uparrow (\alpha + 1) = (\omega \uparrow\uparrow \alpha)^\omega$;
taking sups at limits.

It's worth noting that if you get it the other way round, so that the successor step is

$$\omega \uparrow\uparrow (\alpha + 1) = \omega^{(\omega \uparrow\uparrow \alpha)}$$

– which looks more natural – you find that $\omega \uparrow\uparrow \omega = \epsilon_0$ and $\omega \uparrow\uparrow (\omega+1) = \omega^{\omega\uparrow\uparrow\omega} = \omega^{\epsilon_0} = \epsilon_0$ so $\beta \mapsto \omega \uparrow\uparrow \beta$ grinds to a shuddering halt, and is not strictly increasing, let alone normal.

Then when we do the CNF thing we get.... Give me an ordinal α. Let β_0 be maximal such that

$$\omega \uparrow\uparrow \beta_0 \ \leq\ \alpha \ <\ \omega \uparrow\uparrow (\beta_0 + 1) = (\omega \uparrow\uparrow \beta_0)^\omega.$$

Now let n_0 be maximal such that...

$$(\omega \uparrow\uparrow \beta_0)^{n_0} \ \leq\ \alpha \ <\ (\omega \uparrow\uparrow \beta_0)^{n_0+1} \ =\ (\omega \uparrow\uparrow \beta_0)^{n_0} \cdot (\omega \uparrow\uparrow \beta_0)$$

Now let β_1 be maximal such that...

$$(\omega \uparrow\uparrow \beta_0)^{n_0} \cdot (\omega \uparrow\uparrow \beta_1) \leq \alpha < (\omega \uparrow\uparrow \beta_0)^{n_0} \cdot (\omega \uparrow\uparrow (\beta_1 + 1)) = (\omega \uparrow\uparrow \beta_0)^{n_0} \cdot (\omega \uparrow\uparrow \beta_1)^{\omega}$$

Then we find n_1 s.t.

$$(\omega \uparrow\uparrow \beta_0)^{n_0} \cdot (\omega \uparrow\uparrow \beta_1)^{n_1} \leq \alpha < (\omega \uparrow\uparrow \beta_0)^{n_0} \cdot (\omega \uparrow\uparrow (\beta_1 + 1)) = (\omega \uparrow\uparrow \beta_0)^{n_0} \cdot (\omega \uparrow\uparrow \beta)^{n_1 + 1}$$

The next question is: why do people not do this analysis? What is the least fixed point $\alpha = \omega \uparrow\uparrow \alpha$?

$$\omega \uparrow\uparrow 1 = \omega^{\omega}$$

$$\omega \uparrow\uparrow 2 = (\omega \uparrow\uparrow 1)^{\omega} = (\omega^{\omega})^{\omega} = \omega^{\omega^2}$$

$$\omega \uparrow\uparrow 3 = (\omega \uparrow\uparrow 2)^{\omega} = (\omega^{\omega^2})^{\omega} = \omega^{\omega^3}$$

So presumably

$$\omega \uparrow\uparrow \omega = \omega^{\omega^{\omega}}$$

and

$$\omega \uparrow\uparrow (\omega + 1) = (\omega^{\omega^{\omega}})^{\omega} = \omega^{\omega^{\omega} + 1}$$

so it's looking as if the least fixed point $\alpha = \omega \uparrow\uparrow \alpha$ is ϵ_0. If that's the case then that might help to explain why Veblen and co^y went straight to the device of enumerating fixed points. What rather bothers me is that the literature nowhere seems to explain why the tradition took the step it did. If the reason why it moved straight to Veblen ϕs is that using $\uparrow\uparrow$, $\uparrow\uparrow\uparrow$ and do on does nothing for us, then why was this never spelled out?

Want to show that every function in the DT hierarchy is normal in its second argument

`http://www.math.ucsb.edu/~doner/articles/`.

Chapter 10

Appendices

10.1 Appendix 1: Prologue on Countability

This can be skipped by sophisticates. It was designed as a fairly self-contained handout for my first-years. Sophisticates might wish to consult it for revision, or as a reality check.

10.1.1 Preliminaries

I'm assuming that the reader knows what injections, surjections and bijections are, and that they know what it is for a relation to be *transitive* and what an equivalence relation is and what equivalence classes are, so that if $\sim$ is an equivalence relation on a set X then there is a surjection $X \twoheadrightarrow \{[x]_\sim : x \in X\}$, the set of equivalence classes of members of X. (The double barb on the arrow means "surjection"). I am going to assume that the reader is happy with the gadget of *disjoint union*. We will also need the concept of a *congruence relation*. We say $\equiv$ is a congruence relation "for" a function f of n variables if [we illustrate with $n = 2$ to keep things readable]

$$x \equiv x' \ \wedge \ y \equiv y' \ \rightarrow \ f(x, y) \equiv f(x', y')$$

For example, the equivalence relation on $\mathbb{Z}$ of congruence mod p is a congruence relation for $+$ and $\times$. You almost certainly know this fact already, even if not under that name. Miniexercise: take a moment to check it. Check also that congruence-mod-p is **not** a congruence relation for exponentiation! (you might like to find an illustration of this last fact).

Check that you have these prerequisites under your belt before reading further.

The study of countability is part of cardinal arithmetic, and with cardinal arithmetic the equivalence relation that matters is the equivalence relation on sets of being-in-bijection-with, and it's a congruence relation for all sorts of operations on sets. You can

think of cardinals as [arising from] equivalence classes of sets under this equivalence relation. It's sometimes called *equipollence*, and sometimes *equinumerosity*.

We use the double vertical bar notation for cardinals. You will sometimes see the hash symbol used: $\#(x)$, or even (in the older mathematics literature) a double overlining: $\overline{\overline{x}}$. Objects that are $|x|$ for some x are **cardinals**: $|x|$ is **the cardinal number of** the set x.

'$|X| \leq |Y|$' means that there is an injection from X into Y;

'$|X| = |Y|$' means that there is a bijection between X and Y;

'$|X| \leq^* |Y|$' means that there is a surjection from Y onto X.

In most of the cases you will be concerned with (at least for the moment) $|X| \leq^* |Y|$ implies $|X| \leq |Y|$, so you may act on that assumption – at least for the time being. The reader can check that $\leq$ and $\leq^*$ are transitive. We will see later (remark 19 "Cantor-Bernstein") that $\leq$ is antisymmetric.

The equivalence relation of being-in-bijection-with is a congruence relation for disjoint union, cartesian product, and the operation $X \to Y$ that gives you the set of all functions from X to Y. [For your own satisfaction you might wish to check all these allegations[1]].

Thus cardinals support addition, multiplication and exponentiation. Cardinal addition arises from disjoint union, cardinal multiplication from cartesian product. Thus

$$|X| + |Y| = |X \sqcup Y| \text{ and } |X| \cdot |Y| = |X \times Y|$$

... where $x \sqcup y$ is the disjoint union of x and y. Cardinal exponentiation arises from the operation of forming the set of all functions from one set to another. How many functions are there from X to Y? Check that you understand why the answer is $|Y|^{|X|}$. ("Multiply probabilities of independent events"). Check for yourself that $2^{|x|} = |\mathcal{P}(x)|$. ($\mathcal{P}(x)$ is the power set of x, the set of all subsets of x).

If you think about composition of functions you will have no difficulty persuading yourself that the following hold for all cardinals α, β, γ.

REMARK 18
(1) $\alpha \leq \beta \to \alpha^\gamma \leq \beta^\gamma$;
(2) $\alpha \leq \beta \to \gamma^\alpha \leq \gamma^\beta$.

The following theorem is very useful. You should know how to state it and how to use it... but you can probably get away with not knowing how to prove it.

REMARK 19 *"Cantor-Bernstein"*
If there is an injection from A into B and an injection from B into A, then there is a bijection between A and B.
Equivalently: the relation $\leq$ on cardinals is antisymmetric.

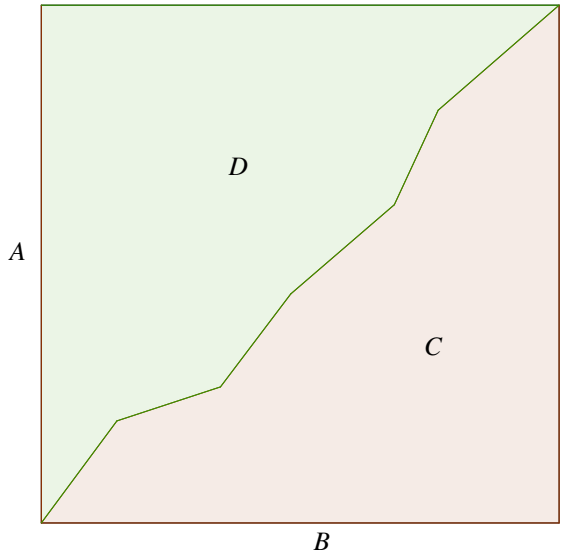
[1] And do not allow yourself to be confused by the fact that equipollence is a congruence relation for the operation $X \to Y$ that gives you the set of all functions from X to Y even though congruence-mod-p is not a conguence relation for exponentiation: the situations are not parallel.

You will often hear remark 19 referred to as "Schröder-Bernstein".

You might think this is blindingly obvious: after all, if f injects A into B, and B can be injected into A then f must have been a bijection all along. But this line of talk works only if A and B are finite: if A and B are both infinite you can have injections $f : A \hookrightarrow B$ and $g : N \hookrightarrow A$ neither of which is a surjection. The function that sends the natural number n to the rational number $n/1$ injects $\mathbb{N}$ into $\mathbb{Q}$, and the function that sends the rational number a/b to $2^a \cdot 3^b$ injects the positive rationals into $\mathbb{N}$, but neither f nor g is a surjection.

REMARK 20 *Bernstein's lemma*

$$\gamma + \delta = \alpha \cdot \beta \ \rightarrow \ \alpha \leq^* \gamma \vee \beta \leq \delta$$



Proof:

Suppose A and B are two sets (of size α and β). Suppose further that we have split $A \times B$ (represented by the square figure above) into two pieces, C and D (of size γ and δ), so that $C \cap D = \emptyset$ and $C \cup D = A \times B$. Now project the C region onto the A axis. Does it cover the whole of the A-axis? (I've tried to draw the picture so that it's not clear whether it does or not!) If it does, then $|A| \leq^* |C|$. If it doesn't, then there is a line through D parallel to the B axis, whence $|B| \leq |D|$.

■

This is quite useful. For example we can use it later to show that if X is a countable set of reals then $|\mathbb{R} \setminus X| = |\mathbb{R}|$. Try it, it's not hard. (You will need the fact that $(2^{\aleph_0})^2 = 2^{\aleph_0}$.

Do they yet know that $|\mathbb{R}| = 2^{\aleph_0}$?

10.1.2 Countable sets

We define $\mathbb{N}$ as the $\subseteq$-least set of cardinals containing 0 and closed under successor:

$$\mathbb{N} = \bigcap \{C : 0 \in C \wedge (\forall x \in C)(x + 1 \in C)\}.$$

DEFINITION 28 *We write '$\aleph_0$' for $|\mathbb{N}|$.*

(Yes there is a cardinal $\aleph_1$ – and $\aleph_2$ and beyond, but that's for later.)

You are a countable set iff you are equipollent with (in $1-1$ bijection with) $\mathbb{N}$. Some people still use the word 'countable' in a wider sense that includes finite sets, so don't be surprised if you hear the word used in this way. In that tradition a set is countable iff it is in bijection with *some* set of naturals, not necessarily with the set of *all* naturals. Or, equivalently: X is countable if $|X| = \aleph_0$ or $|X| \in \mathbb{N}$. Or $|X| \leq \aleph_0$.

Basic useful fact:

REMARK 21
$\aleph_0$ is the smallest infinite cardinal: if α is a cardinal with $\alpha \leq \aleph_0$ then $\alpha \in \mathbb{N} \vee \alpha = \aleph_0$. Equivalently: $\alpha \in \mathbb{N} \longleftrightarrow \alpha < \aleph_0$.

Proof:
This is because if you are a set of size $\leq \aleph_0$ then there is an injection from you into $\mathbb{N}$, so you are the same size as a set of natural numbers. Now every set of natural numbers is either bounded (in which case it is of size n for some $n \in \mathbb{N}$) or unbounded. If it is unbounded then it is clearly in bijection with $\mathbb{N}$– count it, using the order structure it has in virtue of being a subset of $\mathbb{N}$! ■

In fact $\aleph_0$ is minimal among infinite cardinals even w.r.t. the weaker relation $\leq^*$: we can show that a surjective image of a countable set is countable. If you are the surjective image of a countable set then without loss of generality you are a surjective image of $\mathbb{N}$. But then it's easy to put you in 1-1 correspondence with a set of natural numbers: pair off each of your members with the first element of the preimage.

> (To be formal about it, if $f : \mathbb{N} \twoheadrightarrow X$ you inject $X \hookrightarrow \mathbb{N}$ by sending each $x \in X$ to the least natural number in $f^{-1}\text{“}\{x\}$. '$f^{-1}\text{“}\{x\}$' (also written '$f^{-1}(\{x\})$') is $\{n \in \mathbb{N} : f(n) = x\}$, commonly described as a **fibre** of f . . . you might find this terminology useful.)

This minimality of $\aleph_0$ is important, and it can save you a lot of time. It means that if you want to show that a set is countable you don't have to go the extreme lengths of finding a bijection between it and the whole of $\mathbb{N}$: it suffices to find a bijection between it and an infinite subset of $\mathbb{N}$.

Another manifestation of this minimality is the following fact:

REMARK 22 *For α a cardinal, $\alpha = \alpha + 1 \longleftrightarrow \alpha \geq \aleph_0$.*

Some people take "$\alpha = \alpha + 1$" to be the *definition* of α being an infinite cardinal. The usual definition is $\alpha \not< \aleph_0$ or – equivalently – $\alpha \notin \mathbb{N}$.

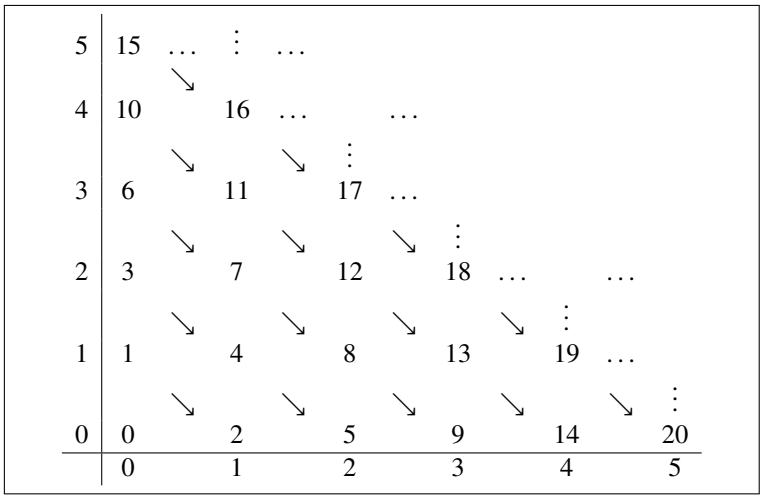
You might like to prove remark 22 for yourself. Catchphrase: *Hilbert's Hotel*. . . you might like to google it.

Let's now have some examples of sets that are countable

$\aleph_0 + 1 = \aleph_0$; Add an extra member to a countable set: the result is countable.

$\mathbb{N} \sqcup \mathbb{N}$ is countable, which is to say $\aleph_0 + \aleph_0 = \aleph_0$. So $\mathbb{Z}$ is countable, co's it's the union of two copies of $\mathbb{N}$: $\mathbb{N}$ itself and the negative integers.

$\mathbb{N} \times \mathbb{N}$ is countable by **zigzagging**, so we can conclude that $\aleph_0 \cdot \aleph_0 = \aleph_0$.



The fact that the cartesian product of two countable sets is countable can be very useful. If each A_i with $i \in \mathbb{N}$ is a countable set equipped with a counting then you can use those countings to do the same zigzag construction that counts $\mathbb{N} \times \mathbb{N}$ to count the union $\bigcup_{i \in \mathbb{N}} A_i$. The zigzag algorithm needs those countings to work on, of course, so to say – as people often do – that this shows that *a union of countably many countable sets is countable* is not straightforwardly correct. You need an axiom that says that

$$(\forall x)(\exists y)F(x, y) \;\rightarrow\; (\exists f)(\forall x)F(x, f(x))$$

which will reassure you that if all your A_i have countings then there is a function that, to each A_i, assigns a counting of it; you then use those assigned countings in your run of the zigzag algorithm. This axiom is called the "Axiom of Choice" and you will be hearing more of it later.

The following observation will turn out to be very useful:

REMARK 23 *(The* **Prime Powers Trick***)*
The set of finite sequences from a countable set form a countable set.

Proof:
We map finite sequences of naturals to naturals by sending – for example – the tuple $\langle 1, 0, 8, 7, 3\rangle$ to $2^{1+1} \cdot 3^{0+1} \cdot 5^{8+1} \cdot 7^{7+1} \cdot 11^{3+1}$. ■

Then the set of finite subsets of a countable set is countable because it is a surjective image of the set of finite sequences from that set – and we saw above that a surjective image of a countable set is countable.

This is an important fact with ramifications. If we think of a language as a set of finite strings of characters chosen from a finite – or even countably infinite – alphabet (as is the case for all the mathematical languages you are likely to encounter) then the set of expressions that constitutes the language is countable. You may later need to exploit the fact that the set of formulæ of such a language can be enumerated ... first formula, second formula ... nth formula ...

We can show $|\mathbb{Q}| = \aleph_0$ by injecting $\mathbb{N}$ into $\mathbb{Q}$ (send the natural number n to the rational number n) and injecting $\mathbb{Q}$ into $\mathbb{N} \times \mathbb{N}$ (send x/y – with no common factors – to $\langle x, y \rangle$) and then using remark 19.

We can think of $\mathbb{Q}$ as a quotient of $\mathbb{Z} \times \mathbb{Z} \setminus \{0\}$. Say $\langle x, y \rangle \sim \langle u, v \rangle$ iff $x \cdot v = y \cdot u$. Then we can think of the equivalence classes as rationals. If we think of $\mathbb{Q}$ that way then it is clear that it is countable because it's an infinite surjective image of a countable set.

10.1.3 Uncountable sets

Are there any? Yes–there are, but it's a nontrivial fact that not all infinite sets are countable. The key fact here is **Cantor's theorem** which tells us that every set is smaller than its power set. Or – to put it another way – $\alpha < 2^\alpha$ for all cardinals α. What we actually prove is – on the face of it – slightly stronger.

THEOREM 19 *Cantor's theorem.*

$$|\mathcal{P}(X)| \not\leq^* |X|$$

Proof:

Suppose $f : X \to \mathcal{P}(X)$. We will prove that f is not surjective. Suppose *per impossibile* that it were. Consider $r = \{x \in X : x \notin f(x)\}$. We will show that r cannot be in the range of f. For suppose r were $f(a)$. We consider the proposition (or perhaps one should say the *question*)

$$¿a \in r?$$

By definition of r this is equivalent to

$$a \in f(a)$$

but $f(a) = \{x \in X : x \notin f(x)\}$ so this is equivalent to

$$a \notin f(a)$$

but $f(a) = r$ so this is equivalent to

$$a \notin r$$

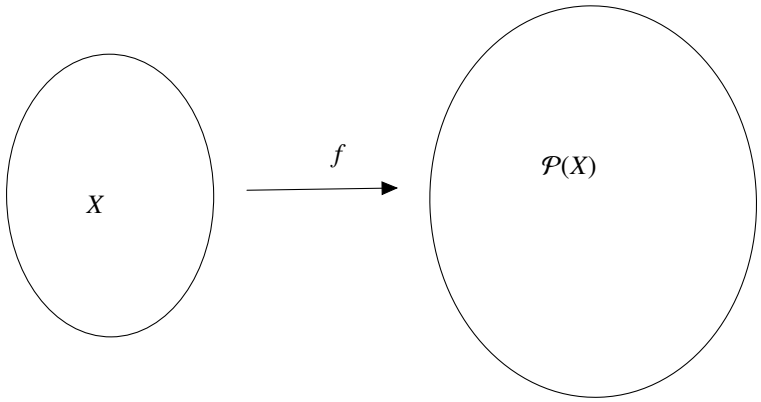
So we have proved $a \in r \longleftrightarrow a \notin r$ which is self-contradictory. ■

Notice that we have proved $a \in r \longleftrightarrow a \notin r$ (which is not explicitly a contradiction) rather than $a \in r \wedge a \notin r$ (which is). It's possible to derive the conjunction from the biconditional but it's a bit fiddly and unless you are a compsci student of a particularly

theoretical cast of mind you may well feel that you can put off the task of mastering the fiddly bits until later. However it is worth understanding this proof... at some point – even if not this very minute and second – since echoes of it reappear in the proof of the unsolvability of the Halting Problem for Turing machines, and the derivation of Russell's paradox, among others.

We've proved lots of equations, and they are all easy. There is one major theorem in the form of an *in*equation, and it is easy too. It is **Cantor's Theorem**.

THEOREM 20 *Cantor's theorem*
Suppose $f : X \to \mathcal{P}(X)$. Then f is not surjective.



Before we get stuck into the proof I want to identify a wee, *wee* assumption that we have to make. It is this: if there is a surjection from A onto B then there is an injection from B into A. This is another of those things (like the Cantor-Bernstein theorem) that is obvious when A and B are finite, but not obvious otherwise. (It's the axiom of choice again!)

Cantor's theorem says that that $n < 2^n$. Now if $n = |X|$ then $2^n = |\mathcal{P}(X)|$. Clearly there is an injection $X \to \mathcal{P}(X)$: the singleton map $\lambda x \in X.\{x\}$ is one. So to prove the inequality all we have to prove that there is no injection $\mathcal{P}(X) \to X$. In fact it's slightly easier to prove that there is no surjection $X \twoheadrightarrow \mathcal{P}(X)$ (which by assumption is the same thing) and that is what we will do. (I could have left out the bit about injections from A to B and surjections from B to A, and given instead a slightly more complicated proof that there is no injection from $\mathcal{P}(X)$ to X, but that proof is displeasingly messy. If you like, you can check and see how to do it for yourself. Determining which is easier is a delicate calculation)

The proof is now a doddle. Suppose f were a surjection from X onto $\mathcal{P}(X)$. Think about

$$\{x \in X : x \notin f(x)\}. \tag{10.1}$$

This is the set of those things in X that are not members of what f sends them to. Since f sends members of X to subsets of X, asking of a member x of X whether or not it is a member of what f sends it to is a perfectly sensible question, since x is a member of X and $f(x)$ is a subset of X.

If f is a surjection, this subset – 10.1 – of X must be f of something, x_0 say. Now (and I want you to work this out for yourselves) ask whether or not x_0 is a member of $\{x \in X : x \notin f(x)\}$. Think about this a bit before proceeding to the next paragraph.

If it is, it isn't, and if it isn't, it is. Clearly this is an impossible situation. How did we get into it? By assuming that f was a surjection. Evidently it wasn't! ■

Time invested in understanding this proof is time well spent. The same argument is used to great effect in complexity theory, and in (for example) the proof of the unsolvability of the Halting problem, which you will see in 1B.

You Absolutely Must Understand This Proof.

Observe that we have made no assumptions about the size of X whatever! We haven't even assumed that X is nonempty, and certainly not that it is finite. In particular there is no surjection $\mathbb{N} \twoheadrightarrow \mathcal{P}(\mathbb{N})$. Do not waste time trying to prove Cantor's theorem for natural numbers by mathematical induction! (And **do not** try to connect this with any ideas you might have about complex exponentiation: different beast altogether!!)

While we are about it we may as well make a note of the fact that the power set of $\mathbb{N}$ is the same size as the reals:

THEOREM 21 $|\mathbb{R}| = |\mathcal{P}(\mathbb{N})| = 2^{|\mathbb{N}|} = 2^{\aleph_0}$

It's perhaps not *blindingly* obvious that there is a bijection between $\mathbb{R}$ and $\mathcal{P}(\mathbb{N})$. The obvious thing to try – think of a real as a binary expansion, and send it to the set of addresses at which it has a '1' – doesn't quite work, because of double counting of dyadic rationals (rationals with denominator a power of 2) but there are various ways round the problem. One rather neat one (due to my supervisee Jonathan Holmes) is to reflect that every real number has at most one binary representation that contains infinitely many 0s. The set of these representations is in bijection with $\mathcal{P}(\mathbb{N})$! You can also use Bernstein's lemma, remark 20.

I like to think that the difficulty in finding this bijection reflects the fact that $\mathbb{R}$ is a continuous ("analogue") object while $\mathcal{P}(\mathbb{N})$ is a discrete ("digital") one, but I don't want to make *toooo* much of it!

At some point we have to show that there is a surjection from the reals to the countable ordinals.

10.1.4 Recognising the difference

It's very important to get a feel for which sets are countable and which are uncountable, and to be able to spot which is which without having to go through a laborious proof or computation. On the face of it, if one is to prove that a set is countable one has to show how to count it, and if one is to show that it is uncountable one has to use a diagonal argument as in the proof of Cantor's theorem, remark 19. However there are

some heuristics one can use, and I am going to tell you about one that my students have found helpful.

When confronted with a set (as it might be, one of the suspects from the exercise below) one of the things can one do to ascertain whether it is countable or not is to ask "How much information do I have to give to specify a member of this set X?" If the answer is "a finite amount" then X is countable. This is because if we have a way of specifying every member of X then we have a surjection onto X from the set of strings over some finite alphabet and we know that the set of such strings is countable because of the prime powers trick, remark 23. If the answer is "an infinite amount" then the set before you is most assuredly uncountable, and of size at least $2^{\aleph_0}$ at that.

If you have any intuition around expressions like "finite precision", "infinite precision" then you can put it to good use here. Reals are infinite precision objects: to specify a real you need to supply a digit between 0 and 9 for each of **infinitely many** decimal places – independently! The expression 'degree of freedom' might have some resonance for you... a point in the plane has two degrees of freedom ("coordinates"); a circle in the plane has three degrees of freedom: two to locate the centre and a third to tell you the radius. (That's why you can draw a circle through any three points. An ellipse has an extra degree of freedom – the eccentricity – so you can draw an ellipse through any four points – OK, as long as the quadrilateral is convex!) The number of objects you get is the number of options at each parameter raised to the power of the number of degrees of freedom (= the number of parameters).

In this sense, a real number has infinitely many degrees of freedom or – as you will later learn to say – a real number has *infinite entropy*. This is enough to show that there are uncountably many reals. You don't really need to know why this is the case, since what I am offering you here is a *heuristic* not a theorem.

In this hand-wavy sense, one can say that the natural numbers have finite entropy. How so? How many bits of information do I need to have available if I want to transmit a natural number to you? Now you have probably learnt that there is no probability distribution on the natural numbers that makes them equally probable. So suppose I pick natural number n with probability 2^{-n}. How many bits do I need *on average* to communicate a natural number to you? Well, half the time the number is 1, so I need only one bit, one quarter of the time it'll be 2, so i'll need two bits. It's easy to see (sum the geometric progression) that on average I will need only two bits. So the natural numbers (with this distribution) have an entropy of two bits. With a different distribution you'll get a different entropy, but you are not to worry about that [no, really!![2]]; the point is that there is a way a finding a probability distribution for $\mathbb{N}$ that gives the naturals finite entropy, whereas there is no way of doing that for the reals. Moral: the naturals (unlike the reals) are a countable set.

Don't worry if this looks hand-wavy – it is; it's a heuristic not a theorem. If it works for you that's cool, and if it doesn't, don't worry – forget the previous paragraph entirely. [snaps fingers: wake up now!].

So how many reals are there, if you think of them in binary? You have $\aleph_0$ independent trials (one at each binary place) and each trial has 2 possible outcomes. So the number of reals must be $2^{\aleph_0}$. (if I think of them in decimal I get $10^{\aleph_0}$ and you

[2] If you really want to think about this, perhaps have a look at the appendix.

can show that to be the same). Try another example: how many sets $X \subseteq \mathbb{N}$ of prime powers are there that, for every prime p, contains precisely one power of p? Clearly I can choose my powers of p independently, so there are precisely $\aleph_0^{\aleph_0}$ such sets. Now observe, using remarks 19 and 18

$$2^{\aleph_0} \leq^{(a)} \aleph_0^{\aleph_0} \leq^{(b)} (2^{\aleph_0})^{\aleph_0} = 2^{(\aleph_0{}^2)} =^{(c)} 2^{\aleph_0}$$

(a) and (b) both hold by remark 18 part (1);
(c) holds because $\aleph_0^2 = \aleph_0$.

Finally we infer

$$2^{\aleph_0} = \aleph_0^{\aleph_0}$$

from

$$2^{\aleph_0} \leq \aleph_0^{\aleph_0} \text{ and } \aleph_0^{\aleph_0} \leq 2^{\aleph_0}$$

by using remark 19.

10.1.5 Finite Objects

Move this to section 10.1.4. . . ?

I'm going to assume that you have a concept of *finite object*. A set X of things is a set of finite objects iff there is a system of notation for members of X such that every member of X has a finite description according to that system. (Natural numbers are finite objects; rationals and algebraics are finite objects; reals famously are not. They are *infinite precision* objects.) The observant reader will complain that – according to this definition – any object that belongs to a countable set X can be made to be a finite object: all that one has to do is fix in advance a bijection between X and $\mathbb{N}$, and then one can point to an object by saying that it is the nth member of X according to the given enumeration. Of course life is not that simple. One does not want X to be just any old random assemblage of things, one wants it to be a set in the rather stricter sense in which one speaks of a *set of spoons*, or a *set of plates*, or a *set of rules*, or a *chess set*: X must be a family of homologous objects admitting a uniform description (or a union of finitely many such families). Further, the enumeration of this non-random collection must be in some informal sense computable. Indeed there is a useful and practical converse to this, which I impress on all my first-years. If you are presented with a natural set (not a mere assemblage) and you want to know whether or not it is countable: ask yourself: are its members finite objects? Do I have a uniform finitary system of notation for its members? If I do, it's countable – and if it doesn't it isn't. This simple heuristic is a remarkably efficacious way for beginners to decide whether or not a candidate set is countable.

The concept of finite object is not a mathematically rigorous one, but it is very important nevertheless. I have a hunch that the most sympathetic (and quite possibly the most correct) way to understand the Hilbert programme is as an endeavour to represent as much as possible of mathematics as the study of finite objects. Finitism started off as a sensible idea: ideologies always do – however crazy they turn out to be later. Look at

how much progress in Mathematics involves reducing problems to finite calculations. Once you have any intuition of a difference between finite objects and infinite objects you notice that finite objects are tractable and infinite objects aren't, and progress in the study of particular kinds of mathematical objects happens when you find ways of thinking of them as finite objects. (Algebraic topology etc.; Euler's polyhedron formula is a nice example of distillation of finite information from infinite sources. Knots.) Proofs are finite objects; all of syntax is peopled with finite objects. It is not at all barmy to think that mathematics is really the study of finite objects, and that a preoccupation with trying to express everything in terms of structure of finite character is the way to go. It may be *mistaken* (beco's the aim of Mathematics is to *generalise*) but it certainly isn't *barmy*.

A set-of-finite-objects is a set equipped with enough structure for there to be a system of notation that allocates everything in the suite a description containing only finitely many symbols. The minimal conditions for this to happen seem to be for the set to be a recursive datatype of finite character, or – to put it another way – (using an encoding scheme) an *r.e.* or *semidecidable* set of naturals. This is why the (recursive) axiomatisablity of First Order Logic is so important: valid sentences of First Order Logic come equipped with proofs that are finite objects, but valid sentences of higher-order logic do not.

Given their importance, clarifying the concept of finite object is probably a good project. One way into it is to think about countable ordinals. We will see that the collection of countable ordinals is itself uncountable, and so its members cannot be thought of as finite objects. However all its proper initial segments are countable, so the inhabitants of any proper initial segment can be thought of as finite objects. But not uniformly! It was the thought that this nonuniformity could be an opening into the concept of finite object that was one of the attractions for me of the project of understanding countable ordinals.[3]

On the subject of "giving someone a countable ordinal" Think about what a certificate for a countable ordinal is. If $\alpha = \beta + 1$ then a certificate for α is a suitably decorated certificate for β. If λ is the sup of $\langle \lambda_n : n \in \mathbb{N} \rangle$ then a certificate for λ is a function f defined on $\mathbb{N}$ such that $f(n)$ is a certificate for λ_n. But f must be a finite object. Thus every certificate is a finite object. Observe that if $\alpha < \beta$ than any certificate for β has within it a certificate for α. This doesn't make it easily decidable when two limit ordinals are the same, beco's i can't know until the end of time whether or not two sequences have the same sup.

10.1.6 Exercises

(1) (i) Check that $\aleph_0 + 2^{\aleph_0} = 2^{\aleph_0}$.

[3] There is an apparent paradox here (which we shouldn't really discuss at this point, for fear of frightening the horses). We shall see later that, for any countable ordinal α, every countable ordinal $\beta > \alpha$ gives us a way of thinking of α (indeed of every ordinal $< \beta$) as a finite object. But there are uncountably many countable ordinals $\beta > \alpha$ so this means that there are *uncountably* many finitary systems of notation for countable ordinals. But a finitary system of notation is itself a finite object, being a finite set of rules over a countable alphabet, so there are only countably many of them. This will be resolved later in these notes (see p 97)by the concept of a *recursive* ordinal.

(ii) Check that $\aleph_0 + \alpha = 2^{\aleph_0} \to \alpha = 2^{\aleph_0}$. (Use Bernstein's Lemma).

(2) Which of the following sets are countable and which are uncountable?

(i) The set of complex numbers;
(ii) The set of partitions of $\mathbb{N}$ into finite pieces;
(iii) The set of partitions of $\mathbb{N}$ into finitely many pieces;
(iv) The set $\mathbb{Q} \to \mathbb{R}$ of functions from the rationals to the reals;
(v) The set of functions $f : \mathbb{N} \to \mathbb{N}$ s.t $f(n) = 0$ for all but finitely many n;
(vi) The set of functions $f : \mathbb{N} \to \mathbb{N}$ s.t $f(n) = 0$ or 1 for all but finitely many n;
(vii) The set of functions $f : \mathbb{N} \to \mathbb{N}$ s.t $f(n) = n$ for all but finitely many n;
(viii) The set of ("nonincreasing") functions $f : \mathbb{N} \to \mathbb{N}$ s.t $(\forall n)(f(n+1) \leq f(n))$;
(ix) The set of subsets of $\mathbb{N}$ with finite complement ("cofinite");
(x) The set of algebraic numbers;
(xi) The set of nonincreasing *partial* functions $\mathbb{N} \to \mathbb{N}$.

Of the sets that are uncountable say – with reasons – whether they are of size $2^{\aleph_0}$ or of size $2^{2^{\aleph_0}}$. You need not give a rigorous proof.

(3) How many injective functions $f : \mathbb{R} \hookrightarrow \mathbb{R}$ are there which satisfy $(\forall xy)(x \leq y \to f(x) \leq f(y))$? Are there $2^{\aleph_0}$ or $2^{2^{\aleph_0}}$?

(4) (Mathematics Tripos 1A, 2014.4.II.7E, modified). How many ω-sequences are there from {0, 1, 2, 3, 4, 5, 6, 7, 8, 9} that agree at infinitely many places with the decimal expansion of $\sqrt{2}$?

(5) Say two permutations of $\mathbb{N}$ are *equivalent* if they agree at all but finitely many arguments. What can you say about how many equivalence classes there are?

(6) If you have done some number theory (so you can remember what a multiplicative function is!) and are doing this for revision...
How many multiplicative functions $\mathbb{N} \to \mathbb{N}$ are there?
How many multiplicative functions $\mathbb{N} \to \mathbb{C}$?

(7) How many finite sets of reals are there?
How many countable sets of reals?
How many uncountable sets of reals?

10.1.7 Appendix

[with thanks to Ted Harding]

Here's a strategy for identifying a natural number uniquely using only finitely many bits. You ask "Is it greater than 1?", "Is it greater than 2?", "Is it greater than 4?", "Is it greater than 2^n?"...until you get the answer "no!", at $n = k$, say. Then you have located it in the block $[2^{k-1}, 2^k]$, whereupon you start asking "Is it between 2^{k-1} and $2^{k-1}+2$?"; "Is it between 2^{k-1} and $2^{k-1}+4$?" ...so you will locate m in no more than $\binom{m}{2}$ steps. There is no global finite bound (independent of m) on the number of questions you might have to ask, but you only ever have to ask finitely many.

But one can always find k with k questions: "Is it 1?"; "is it 2?", "is it 3?"...

This isn't really the same situation as the reals, co's these binary choices are not independent.

10.1.8 Afterthoughts

By thinking about degrees of freedom one persuades oneself that the answer to (5) should be "at least $2^{\aleph_0}$", and there is an easy proof that it is, indeed, at least $2^{\aleph_0}$, but the proof can be tricky to find. Here is a cute answer that occurred to me on my bike. [Well, actually, the *question* occurred to me on my bike.] Fix a conditionally convergent series, such as the Alternating Harmonic series, whose general term is $n^{(-1)^n}$. We know that by judiciously ordering the naturals we can get it to sum to any real that we like. (Alice biting from the two sides of the mushroom to get her to the correct height). This gives us an injection $i : \mathbb{R} \hookrightarrow$ the set of all permutations of $\mathbb{N}$. Now reflect that two permutations of $\mathbb{N}$ that differ on only finitely many arguments will give arrangements that sum to the same real. This means that all the permutations that are the values of this injection i belong to different equivalence classes. This gives us our lower bound of $2^{\aleph_0}$.

10.2 Declaring the Ordinals as a higher-order Rectype

The Indian Rope Trick.

10/xi/18. I now think i understand it. Ordinals i mean. The abstract datatype of ordinals and the order on it are defined by simultaneous recursion:

S of an ordinal is an ordinal
$0 < S(x)$;
$x < S(x)$;
If A and B are sets of ordinals we say $A \sim B$ iff

$$(\forall a \in A)(\exists b \in B)(a < b) \wedge (\forall b \in B)(\exists a \in A)(b < a)^4$$

If A is a set of ordinals then $\texttt{sup}\ \alpha$ is an ordinal;
If A is a $\sim$-equivalence class then $\texttt{sup}\ \alpha$ is an ordinal and $a \in \mathcal{A} \in \alpha \rightarrow a < \texttt{sup}\ \alpha$[5]

Then we can think of the family of isomorphism classes of wellorderings as an implementation of this ADT. This subordinates the definition of wellordering but it might be a clever move. OTOH i do like the old idea that there are fundamentally TWO ways of thinking about ordinals.

One can also give a recursive definition of the class of wellorderings.

Indeed we can define $\mathbb{N}$ and $<_{\mathbb{N}}$ by a simultaneous recursion. Probably a good idea!

We define On, $<_{On}$ and $=_{On}$ by a simultaneous recursion

[4]This ensures that A and B have no top elements.

[5]Notice that if A is the empty set of ordinals $\texttt{sup}\ (A) = 0$ so we don't really need a clause to say that 00 is an ordinal.

DEFINITION 29 *0 is an ordinal;*
If α is an ordinal, so is $\mathsf{succ}(\alpha)$*;*
If X is a set of ordinals, then $\mathsf{sup}(X)$ *is an ordinal;*
$0 \leq \alpha$*;*
$\alpha < \mathsf{succ}(\alpha)$*;*
$(\forall \alpha \in X)(\exists \beta \in Y)(\alpha \leq \beta) \rightarrow \mathsf{sup}(X) \leq \mathsf{sup}(Y)$*;*
$\alpha \in X \rightarrow \alpha \leq \mathsf{sup}(X)$*;*

and various boring axioms to make trivial facts obvious:

$\alpha \leq \beta \rightarrow \beta \leq \alpha \rightarrow \alpha = \beta$*;*
$\alpha \leq \beta \rightarrow \beta \leq \gamma \rightarrow \alpha \leq \gamma$*;*
$\alpha < \beta \rightarrow \beta < \gamma \rightarrow \alpha < \gamma$*;*
$\alpha = \beta \rightarrow \beta = \gamma \rightarrow \alpha = \gamma$*;*
$\alpha < \beta \rightarrow \beta < \alpha \rightarrow \bot$*;*
$\alpha = \beta \rightarrow \beta = \alpha$*;*
$\alpha = \beta \rightarrow \alpha \leq \beta$*;*
$\alpha < \beta \rightarrow \alpha \leq \beta$*.*
$(\forall \alpha \in S_1)(\exists \beta \in S_2)(\alpha \leq \beta) \rightarrow \mathsf{sup}(S_1) \leq \mathsf{sup}(S_2)$

(I omit the – even more boring – obvious axioms to the effect that = is a congruence relation for the other relations. Omitted too – for the moment – are axioms to characterise sup: I'm thinking of things like $(\forall \alpha)(\forall S \subset On)((\alpha < \mathsf{sup}(S)) \rightarrow (\exists \beta \in S)(\alpha \leq \beta))$ which i think is Horn.)

In the above definition $\leq$ and $<$ are a pair of partial order/strict partial order. I have exploited both notations in order to ensure that all the clauses in the declaration are Horn and we thereby have a legitimate datatype declaration.

The strict order $<$ (I have omitted the subscript) is the **engendering relation** of the datatype of ordinals. It is wellfounded for the usual reasons.

Once one has equipped *On* with a wellorder, one can use ideas like that of *order topology*. Conveniently and unsurprisingly it turns out that this gives us the same notion of limit as we presupposed in the extra constructor sup. The notion of continuous function will of course be important to us.

H I A T U S

Or do we define $\leq$ and *On* by a simultaneous recursion and define = as $\leq \geq$?

10.3 The engendering relation on *On* is a wellorder

THEOREM 22 $<_{On}$ *is a wellorder.*

Proof:

The engendering relation on ordinals is a wellfounded partial order – for the usual reasons; the hard part is showing that it is a *total* order.

The proof was discovered simultaneously and independently by Witt [29] and Weil [2] (tho' neither of these two gentlemen would have described it in those terms[6]) and was used by them to establish that every inflationary function f from a chain-complete poset with a bottom element into itself has a fixed point. The proof proceeds by considering the inductively defined set containing the bottom element, closed under f and suprema of chains. The part of the proof that concerns us here is the proof that this object is a chain. This of course is simply a proof that the ordinals are wellordered by $<$. All I have done is recast their argument as a proof of this fact about ordinals.

Let us say an ordinal α is **normal** if

$$(\forall\beta)(\beta < \alpha \rightarrow \mathsf{succ}(\beta) \leq \alpha).$$

If α is normal, then we prove by induction on 'β' that

$$(\forall\beta)(\beta \leq \alpha \vee \mathsf{succ}(\alpha) \leq \beta).$$

That is to say, we show that, if α is normal, then

$$\{\beta : \beta \leq \alpha \vee \mathsf{succ}(\alpha) \leq \beta\}$$

contains 0 and is closed under succ and sups of chains and is therefore a superset of On. Let us deal with each of these in turn.

1. (Contains 0); By stipulation.
2. (Closed under succ); If $\gamma \in \{\beta : \beta \leq \alpha \vee \mathsf{succ}(\alpha) \leq \beta\}$, then either
   (a) $\gamma < \alpha$, in which case $\mathsf{succ}(\gamma) \leq \alpha$ by normality of α and $\mathsf{succ}(\gamma) \in \{\beta : \beta \leq \alpha \vee \mathsf{succ}(\alpha) \leq \beta\}$; or
   (b) $\gamma = \alpha$, in which case $\mathsf{succ}(\alpha) \leq \mathsf{succ}(\gamma)$ so $\mathsf{succ}(\gamma) \in \{\beta : \beta \leq \alpha \vee \mathsf{succ}(\alpha) \leq \beta\}$; or
   (c) $\mathsf{succ}(\alpha) \leq \gamma$, in which case $\mathsf{succ}(\alpha) \leq \mathsf{succ}(\gamma)$ (because succ is inflationary) and $\mathsf{succ}(\beta) \in \{\beta : \beta \leq \alpha \vee \mathsf{succ}(\alpha) \leq \beta\}$.
3. (Closed under sups of chains); Let $S \subseteq \{\beta : \beta \leq \alpha \vee \mathsf{succ}(\alpha) \leq \beta\}$ be a chain. If $(\forall\beta \in S)(\beta \leq \alpha)$, then $\mathsf{sup}(S) \leq \alpha$. On the other hand, if there is $\beta \in S$ s.t. $\beta \not\leq \alpha$, we have $\mathsf{succ}(\alpha) \leq \beta$ (by normality of α); so $\mathsf{sup}(S) \geq \mathsf{succ}(\alpha)$ and $\mathsf{sup}(S) \in \{\beta : \beta \leq \alpha \vee \mathsf{succ}(\alpha) \leq \beta\}$.

Next we show that everything in On is normal. Naturally we do this by induction: the set of normal ordinals will contain 0 and be closed under succ and sups of chains.

1. (Contains 0); 0 is clearly normal.
2. (Closed under succ); Suppose $\alpha \in \{\gamma : (\forall\beta)(\beta < \gamma \rightarrow \mathsf{succ}(\beta) \leq \gamma\}$. We will show $(\forall\beta)(\beta < \mathsf{succ}(\alpha) \rightarrow \mathsf{succ}(\beta) \leq \mathsf{succ}(\alpha))$. So assume $\beta < \mathsf{succ}(\alpha)$. This gives $\beta \leq \alpha$ by normality of α. If $\beta = \alpha$, we certainly have $\mathsf{succ}(\beta) \leq \mathsf{succ}(\alpha)$, as desired, and if $\beta < \alpha$, we have $\mathsf{succ}(\beta) \leq \alpha \leq \mathsf{succ}(\alpha)$.

[6] Thanks to Peter Johnstone for showing me this material.

3. (Closed under sups of chains); Suppose $S \subseteq \{\gamma : (\forall \beta \in On)(\beta < \gamma \rightarrow \mathsf{succ}(\beta) \leq \gamma)\}$ is a chain. If $\beta < \mathsf{sup}(S)$, we cannot have $(\forall \gamma \in S)(\beta \geq \mathsf{succ}(\gamma))$ for otherwise $(\forall \gamma \in S)(\beta \geq \gamma)$ (by transitivity of $<$ and inflationarity of succ), so for at least one $\gamma \in S$ we have $\beta \leq \gamma$. If $\beta < \gamma$, we have $\mathsf{succ}(\beta) \leq \gamma \leq \mathsf{sup}(S)$ since γ is normal. If $\beta = \gamma$, then γ is not the greatest element of S, so in S there is $\gamma' > \gamma$ and then $\mathsf{succ}(\beta) \leq \gamma' \leq \mathsf{sup}(S)$ by normality of γ'.

If α and β are two things in On, we have $\beta \leq \alpha \ \vee \ \mathsf{succ}(\alpha) \leq \beta$ by normality of α, so the second disjunct implies $\alpha \leq \beta$, whence $\beta \leq \alpha \vee \alpha \leq \beta$. So On is a chain as promised,

Chapter 11

Preposterously Large Countable Ordinals

11.0.1 A conversation with Michael Rathjen in Leeds, 1/v/2014

The following gadgetry goes back to Bachmann.

Start with a countable ordinal β and a ridiculously large ordinal, always written 'Ω' which can in fact safely be taken to be ω_1^{CK} but is usually taken to be uncountable, since that makes life much simpler.

I'm not 100% clear about the next bit but i think i have the general idea. That general idea is to construct a $\subseteq$-increasing sequence of sets of ordinals, indexed by ordinals. The first set is $C(\omega, \beta)$ and it contains ω and the ordinals less than β. At each stage η we announce that $\theta(\eta)$ is the least ordinal not in the set we have constructed at that stage. At each stage you close under addition and $\lambda\alpha.\omega^\alpha$. Apparently it's straightforward to show that $C(\Omega, \beta)$ never exhausts all the ordinals, so that $\theta(\alpha)$ is well-defined. no, that bit is wrong

It transpires that $\theta(\Omega)$ is the first fixed-point $\in$-number, aka $\phi(2, 0)$.

$\theta(\Omega + 1)$ is the second fixed-point $\in$-number.

$\theta(\Omega^2) = \Gamma_0$.

All values of θ are less than Ω.

Also the values of θ do not depend on the choice of Ω.

Every ϵ-number below the Bachmann-Howard ordinal is a value of θ.

$C(\epsilon_{\Omega+1}, 0) \restriction \Omega$ is the ordinals below the Bachmann-Howard ordinal

11.1 Notes of Countable Ordinals Reading Group meeting on 16/v/2014

(look also at Taranovsky's ordinalnotations.ps in my assorted-paper-archive folder)

Under the guidance of Jeroen van der Meeren and Michael Rathjen I finally *began* to get the first glimmers of an understanding of the use of a large ordinal in describing initial segments of the countable ordinals. What follows is my notes of the discussion of this topic at the meeting of the ordinals reading group on 16/v. Present were: your humble correspondent, Professors Leader and Dawar, Arno Pauly, Philipp Kleppmann and an unidentified Ph.D. student from the Lab. We put our heads together and made some progress, and this file records my understanding of that progress.

Key word lurking in the background is **impredicativity**.

The following gadgetry goes back to Bachmann. [need a ref]

It's probably a good idea for the reader to start off by keeping in mind the Veblen picture of rows and rows of ordinals. The top row consists of powers of ω, written in increasing order left-to-right. Going down the page, each subsequent successor row consists of the fixed points in the enumeration of the row immediately above it; at limit stages the row is the intersection of all the rows above it. We assume that the reader is familiar with this picture.

For ordinals α and ζ we define a set $C(\alpha, \zeta)$ of ordinals and a function $\vartheta : On \to On$, by a *simultaneous* recursion on On^2. The thing we are really interested in is the function ϑ; the $C(\alpha, \zeta)$ are mere scaffolding, and they play no rôle in the system of notations with which the ϑ gadgetry will eventually furnish us.

The way to understand what is going on is to fix α and consider $C(\alpha, 0)$, $C(\alpha, 1)$ and so on. At these early stages it is pretty clear that $\zeta \in C(\alpha, \zeta)$ (and this is true whatever ϑ does, so we don't need to worry just yet about what ϑ actually does). However there may come a point at which $\zeta \notin C(\alpha, \zeta)$. The first ordinal at which this happens is declared to be $\vartheta(\alpha)$. This definition reminds me a bit of the definition of diagonal intersection: it's unstratified in the same way.

To construct $C(\alpha, \zeta)$ you start with a set containing 0 and Ω, all the ordinals less than ζ, and $\vartheta(\gamma)$ for all $\gamma < \alpha$; you then close under $+$ and $\alpha \mapsto \omega^\alpha$. Our first stab at the definition of $\vartheta(\alpha)$ is: the least ζ such that $\zeta \notin C(\alpha, \zeta)$. Bear in mind that $\vartheta(\alpha)$ is **not** defined as the least thing not in $C(\alpha, \zeta)$. For one thing, it would need *two* arguments – $\vartheta(\alpha, \zeta)$ – not one. It's a complex diagonalisation and you need to read the definition carefully. Bind the 'ζ' somehow, and "the least ζ such that $\zeta \notin C(\alpha, \zeta)$" sounds sensible. **However** we add a clause so that $\vartheta(\alpha)$ is not the first ζ s.t. $\zeta \notin C(\alpha, \zeta)$ but rather the first ζ s.t. $\zeta \notin C(\alpha, \zeta) \wedge \alpha \in C(\alpha, \zeta)$. It will become clear later what purpose is served by this extra $\alpha \in C(\alpha, \zeta)$ clause, but you should not expect it to be clear at this stage.

Here is something that threw me and it might throw you. It's pretty clear that $\lambda\alpha\zeta.C(\alpha, \zeta)$ is $\subseteq$-increasing in both arguments, but you mustn't jump to the conclusion that ϑ is strictly increasing – it isn't! Observe also that it is not immediately clear whether or not $\alpha \in C(\alpha, \zeta)$. It will transpire that this happens only when α has some strong limit property.

The best way to understand what is going on is to fix a small α and consider $C(\alpha, 0)$, $C(\alpha, 1)$ and so on, so let's do some of these by hand to calm our nerves. We will see that the first few values of ϑ are the first few ϵ-numbers.

If $\alpha < \epsilon_{\Omega+1}$ then α has a CNF with base Ω. That much is obvious. Let $K(\alpha)$ be the set of ordinals that appear in the CNF for α, and let $\alpha^* = \max(K(\alpha))$. Then we can say

$$\vartheta(\alpha) < \vartheta(\beta) \text{ iff either } \alpha < \beta \wedge \alpha^* < \vartheta(\beta)$$
$$\text{or} \quad \alpha > \beta \wedge \vartheta(\alpha) \leq \beta^*$$

Then

$$\vartheta(\alpha) = \min\{\zeta \in E : \alpha^* < \zeta \wedge (\forall \beta < \alpha)(\beta^* < \zeta \rightarrow \vartheta(\beta) < \zeta)\}$$

where $\zeta \in E$ means that ζ is an ϵ-number.

Compute a few values of C for small arguments to get a feel for things: you will see that the first few values of ϑ are the first few ϵ-numbers. Note that at these early stages Ω hasn't been doing anything.

We note a couple of facts that might help us get oriented, and we may get round to proving them later. ϑ is injective and all its values are ϵ-numbers. $\alpha < \Omega \rightarrow \alpha < \vartheta(\alpha)$

$C(0, 0)$ contains 0 and Ω. We don't have to put any values of ϑ into it co's the first argument is 0. We then close under addition and $\beta \mapsto \omega^\beta$. Pretty clearly it is going to contain everything less than ϵ_0. It *won't* contain ϵ_0 itself (how could it, after all?) but it does contain a lot of stuff beyond Ω. We will see later [*much* later] what that stuff does. For the moment it does nothing.

What about $C(0, 1)$? It's just going to be the same set. $C(0, \omega)$ is going to be the same set, too. Observe that if $\zeta < \epsilon_0$ then $\zeta \in C(0, \zeta)$, so *all* the $C(0, \zeta)$ are going to be the same set all the way through all the ordinals less than ϵ_0. Indeed even $C(0, \epsilon_0)$ is the same (tho' $C(0, \epsilon_0 + 1)$ is bigger).

The first ζ such that $\zeta \notin C(0, \zeta)$ is therefore ϵ_0. The second ☠ condition on candidates for $\vartheta(\alpha)$ (the condition that requires that $\alpha \in C(\alpha, \zeta)$) is satisfied – all it requires in this case is that $0 \in C(0, 0)$ – so we conclude that $\vartheta(0)$ is ϵ_0.

Notice that there is never any need for us to compute $C(0, \zeta)$ for any $\zeta > \vartheta(0)$; since the only purpose served by the $C(\alpha, \zeta)$ is to enable us to calculate $\vartheta(\alpha)$, once that is done we lose interest.

How about $C(1, 0)$? It's like $C(0, 0)$ except that we put $\vartheta(0)$ (which is ϵ_0) into it before closing under the operations. This means that we get everything less than ϵ_1 (think: Cantor Normal Forms for ordinals $< \epsilon_1$). As we run through the $\zeta < \epsilon_1$ we get nothing new in $C(1, \zeta)$ until we reach ϵ_1 itself, so we conclude that $\vartheta(1) = \epsilon_1$. As before, the ☠ condition on ζ does nothing because all it requires is that $C(1, \zeta)$ should contain 1, and we already know it contains everything below ϵ_1.

Similarly we conclude that $\vartheta(n) = \epsilon_n$ for $n < \omega$. A picture emerges in which, for small arguments, ϑ enumerates the ϵ numbers. In fact Jeroen tells me that ϑ is injective and all its values are ϵ-numbers.

Fixed point ϵ numbers are sometimes called *κ-numbers*, so that κ_0 is the least solution to $\kappa = \epsilon_\kappa$. Let us think a bit about what $\vartheta(\kappa_0)$ might be. We start with $C(\kappa_0, 0)$. This set contains Ω and all the ϵ-numbers below κ_0, and is closed under + and $\zeta \mapsto \omega^\zeta$. Now, recalling what we know about Cantor Normal Forms, we can see that this act of

closure will put into $C(\kappa_0, 0)$ every ordinal below κ_0 (plus a lot of big rubbish beyond Ω). This immediately tells us that the sets $C(\kappa_0, \zeta)$ for $\zeta \leq \kappa_0$ are all going to be the same set as $C(\kappa_0, 0)$. We observe that $\kappa_0 \notin C(\kappa_0, \kappa_0)$ so we might expect that we then declare $\vartheta(\kappa_0)$ to be κ_0. However note that κ_0 is not only the *second* argument at this stage, but also the *first*, so we look at the ☠ condition – "$\alpha \in C(\alpha, \zeta)$" – and we see that it is not satisfied! So we have to look at a few more $C(\kappa_0, \zeta)$ before we can say we have reached $\vartheta(\kappa_0)$. In fact we have to go as far as $C(\kappa_0, \epsilon_{\kappa_0+1})$.

The picture I now have is that, for $\alpha < \Omega$, ϑ enumerates the ϵ-numbers less than Ω – except that it misses out the fixed points (that is what the ☠ condition is doing). Another way of putting this is that it enumerates those ordinals in the first row that do not appear in the second row; *yet* another way of putting it is to say that the purpose of the ☠ clause is to prevent ϑ from having fixed points.

That was what one might call the *first pass*. I am assured by Jeroen that $\vartheta(\Omega)$ is the first fixed-point ϵ-number (the first κ-number) – aka $\phi(2, 0)$ – and that $\vartheta(\Omega + 1)$ is the second fixed-point ϵ-number.

OK, so: thus emboldened, let us check these allegation for ourselves and start by thinking about what $\vartheta(\Omega)$ might be. We obtain $C(\Omega, \zeta)$ by starting with $\{\vartheta(\alpha) : \alpha < \Omega\}$ and all the ordinals less than ζ and closing under $\beta \mapsto \omega^\beta$ and $+$. If I was right earlier, then we have all the ϵ numbers less than the first κ number. So $C(\Omega, \kappa_0)$ contains Ω but does not contain κ_0 so $\vartheta(\Omega)$ is going to be κ_0 as foretold. Observe that we have now reached a stage where all the stuff $\geq \Omega$ that we always put into the $C(\alpha, \zeta)$s starts doing something.

This is consonant with what the preceding paragraph is telling us, namely us that, in the *second* pass, ϑ goes back and enumerates those ordinals in the *second* row that do not appear in the *third* row. Indeed one has the impression that in the αth pass ϑ enumerates in increasing order those ordinals in the αth row of the Veblen table that do not appear in the $\alpha + 1$th row. Jeroen and Michael tell me that $\vartheta(\Omega^2) = \Gamma_0$. This would appear to confirm what i have just been saying, because, after all, once one has made Ω passes (and thereby reached $\vartheta(\Omega^2)$) one should have hit every power of ω below Γ_0.

Stuff to sort out

There now follow some observations from Jeroen and Michael that I am reassured to find plausible but which I can't at this stage actually prove.

Jeroen also sez $\alpha < \Omega \to \alpha < \vartheta(\alpha)$.

All values of ϑ are less than Ω.
ϑ is injective.

[These last two observations cannot both be true! What did he mean?]

The values of ϑ do not depend on the choice of Ω. You can even take Ω to be ω_1^{CK}.

Every ϵ-number below the Bachmann-Howard ordinal is a value of ϑ.

$C(\epsilon_{\Omega+1}, 0) \restriction \Omega$ is the ordinals below the Bachmann-Howard ordinal.

All this machinery presumably supports a notational system. There is a binary ϕ(-,-) function that we can use to denote ordinals in sufficiently early levels of the Veblen table. I would like to understand that properly.

Should say something about why all these ordinals described by this Bachmann gadgetry are recursive. Anuj says that the ordering on the ordinals denoted by these notations is decidable. So, for any of these ordinals – α,say – the set of [gnumbers of] notations for ordinals below α gives a wellordering of $\mathbb{N}$. [but why is this set of notations for ordinals below α a decidable set? Why isn't it merely r.e.. . . ?]

Apparently it's straightforward to show that $C(\Omega, \beta)$ never exhausts all the ordinals, so that $\vartheta(\alpha)$ is well-defined. Should find something to say about this.

Chapter 12

Miscellaneous thoughts on ordinals

Deeply important fact that you cannot compute an enumeration of a countable set merely from a wellordering of it. Let $\langle X, <_X \rangle$ be a wellordering, living in some model of ZF that believes it to be uncountable. In a bigger model it might become countable. If there were an engine that could take a wellordering of a countable X and returned an enumeration of X then clearly it couldn't do it just by looking inside X. And it evidently can't do it by using machinery available to it by virtue of living inside a model of ZF, co's if it could then any set that could be made countable in a larger model could be shown to be countable earlioer, in a smaller model.

12.1 automatic and suitable ordinals

ω^ω

EXERCISE 19 *The ordinal ω^ω is the least ordinal not the length of an automatic wellordering of $\mathbb{N}$. The Von Neumann ordinal ω^ω is the least Von Neumann ordinal that is not "suitable" for Basic Set Theory.*

Prove these two facts and establish the connection (if any) between them (if any).

There are two texts on this, one by Delhommé and one by Gandy, but i have not been able to get my hands on either of them, so this has become an exercise. (I don't want to fall foul of the parable of the talents by doing nothing). My first worry (not the kind of thing that would bother Adrian!) is occasioned by the fact that the first property of ω^ω is a property of the set that is the Von Neumann implementation of it, whereas the second is genuinely a property of the ordinal itself. This suggests to me that the co-incidence we have noticed is a mere coincidence. But we shall see!

[Actually i have just found my photocopy of Gandy's ms. but – as they say – I've started so i'll finish.]

12.1.1 Suitable ordinals

My understanding is that a term t is T-**suitable** iff whenever $\phi(\vec{x})$ is Δ_0^T then so is $[t/x_i]\phi$.

There are four ways in which a term t could appear in a formula ϕ.

(i) t might occur in an equation $t = x_i$ or on either side of an '$\in$' as in

(ii) '$x_i \in t$' or

(iii) '$t \in x_i$'. Finally

(iv) we might have restricted quantifiers '$(\forall x \in t)$'.

First, some preparatory work. In this section "ordinal" means "Von Neumann ordinal", and the "successor" of x is $x \cup \{x\}$.

Observe that "x is an ordinal" is Δ_0, beco's it is "x is transitive and totally ordered by $\in$". "y is the successor of z" is $y = z \cup \{z\}$ which is $(\forall w \in y)(w = z \vee w \in y) \wedge z \in y \wedge (\forall w \in z)(w \in y)$ and is accordingly Δ_0. Consequently "x is a successor ordinal" and "x is a limit ordinal" are both Δ_0.

Not only is "y is the succcessor of x" Δ_0, so too is "y is the next limit ordinal after x". It is "y is an ordinal and $x \in y$ and everything in $y \setminus x$ is a successor of a member of $y \setminus x$". That will come in handy later on ...

DEFINITION 30 *Let us say x is limit$_{n+1}$ if (x is an ordinal and is nonempty and) for every y in x there is a $z \in x$ with $y \in z$ and z is limit$_n$. "limit$_1(x)$" of course is just "x is nonempty and not a successor".*

What about '$x \in \omega$'? That is: x is an ordinal plus an extra condition, namely x is the [Von Neumann] successor of one of its members and every member of x is the successor of another member of x: $(\forall y \in x)(\exists z \in y)(y = z \cup \{z\})$.

We can now say "$x = \omega^n$" in a Δ_1^T way. It's just

$$\text{limit}_n(x) \wedge (\forall y \in x)(\neg\text{limit}_n(y)).$$

"$t \in x$" is equivalent both to $(\exists z)(z = t \wedge z \in x)$ and to $(\forall z)(z = t \rightarrow z \in x)$, which means that if "$t = x$" is Δ_1^T then so is "$t \in x$".

What about restricted quantifiers? $(\exists x \in t)(\phi)$, where ϕ is Δ_0? Well, this is both $(\exists y)(y = t \wedge (\exists x \in y)\phi)$ and $(\forall y)(y = t \rightarrow (\exists x \in y)\phi)$ so it's Δ_1^T.

So, working in the special case where $T = BST$ and assuming every Δ_1^{BST} formula is also Δ_0^{BST}, we're OK.

How about larger ordinals? ω^2? Everything in ω^ω is either empty or is a successor or is a "next limit" as above.

12.1.2 Automatic Ordinals

An automatic ordinal is the ordertype of a countable wellordering with special properties involving finite automata. And here we need my first-year definition of a countable set as a set for whose members we have a system of finite notation. That is, we can think of its elements as finite strings over a finite alphabet. Very handy anyway (this is, in my experience, by far the best way to give beginners a nose for telling which sets in the real world are countable and which are not), but particularly so here, where we are dealing with FSAs, which have strings for breakfast. Then it is easy to show that the class of automatic *wellorders* is closed under lexicographic product.

We start with an illustration of why ω is automatic. Think of a natural number n in unary, as a string of of n '1's capped off by an infinite string of '0's, and we order these strings lexicographically. The machine $\mathfrak{M}$ we want is one that reads characters from the 4-element alphabet $\{\langle 1,1\rangle, \langle 1,0\rangle, \langle 0,1\rangle, \langle 0,0\rangle\}$. When the machine reads, for the kth time, a character from this alphabet, it is looking at the pair of the two kth coordinates of the two inputs. $\mathfrak{M}$ is a three-state machine that stays in its initial state until it sees something other than $\langle 1,1\rangle$. If it sees $\langle 0,1\rangle$ it accepts; if it sees $\langle 1,0\rangle$ it rejects. So ω is automatic. A tweak to this will show that $\omega + \omega$ is automatic.

? We can put all the odd numbers in increasing order before all the even numbers in increasing order. This time the machine we want has *four* states. It cycles between two states ("odd" and "even") until it sees something other than $\langle 1,1\rangle$. Then which way it jumps depends on whether it is an odd or an even state when it sees a pair containing a 0.

But we can do something more general, recalling that an automatic ordinal is the order type of an automatic wellordering of a countable set, and that the countable set doesn't have to be $\mathbb{N}$. We can show that if two total orders $\langle A, <_A\rangle$ and $\langle B, <_B\rangle$ are both automatic (in virtue of two machines $\mathfrak{M}_A$ and $\mathfrak{M}_B$) then so too are their disjoint union and their lexicographic product. In general the product of two automatic structures is automatic. This tells us that the set of automatic ordinals is closed under + and $\cdot$.

12.1.3 Something to do with ordinals

For any countable limit ordinal α there is a bijection $f : \mathbb{N} \to \{\beta : \beta < \alpha\}$.

Dissect $\{\beta : \beta < \alpha\}$ into countably many copies of $\mathbb{N}$, namely the intervals starting with limit ordinals. Then appeal to the fact that, if $\langle\langle \mathbb{N}_i, <_i\rangle : i \in \mathbb{N}\rangle$ is a sequence of copies of $\langle \mathbb{N}, <\rangle$ then the $\mathbb{N}_i$ can be interleaved to obtain $\langle \bigsqcup_{i\in\mathbb{N}} \mathbb{N}_i, <\rangle$ where $<$ is of order-type ω and $<\restriction \mathbb{N}_i = <_i$.

What on earth was i thinking of here?

12.1.4 Another question about ordinals

Suppose $f : On \times On \to On$. Consider the functions (for all α) $f_{1,\alpha} : \beta \mapsto f(\alpha,\beta)$ and $f_{2,\alpha} : \beta \mapsto f(\beta,\alpha)$. Can $f_{1,\alpha}$ and $f_{2,\alpha}$ both be normal for all α?

From Andrés Caicedo, a theorem of Specker

This gives us the flavour ...

Let's define $\tau(\alpha,\beta)$ to be the least ordinal γ such that if you two-colour the complete graph on the ordinals below γ then you either have a pink monochromatic set of [inherited] order type α or a blue monochromatic set of [inherited] order type β. We say $\gamma \to (\alpha,\beta)$. Here we are considering unordered pairs only, and in a more general context we would make the 2 explicit in an exponent: $\gamma \to (\alpha,\beta)^2$.

Let α be a countable ordinal, and consider the complete graph on the set A of all ordinals below α. A is countable, so there is a bijection between A and $\mathbb{N}$ and we can use this bijection to copy $<_{\mathbb{N}}$ to a worder of A. We now have two worders on A and we colour the edges in $[A]^2$ depending on whether or not these two orders agree on the given edge. There will be monochromatic sets, coloured `agree` and `disagree`, and we ask how long they can be in the order inherited from the longer order, of order type α. Clearly no monochromatic set coloured `agree` can be longer than ω and no monochromatic set coloured `disagree` can be as long as ω.

The argument of the first paragraph establishes that if $\alpha < \omega_1$ then $\alpha \not\to (\omega+1,\omega)$. In other words, $\tau(\omega+1,\omega) \leq \omega_1$, and we probably have equality... haven't checked.

On Mar 5 2019, Thomas Forster wrote:

The Doner-Tarski hierarchy - plus, times, exp.... on ordinals. Think of it as a function with three arguments: $DT(\alpha,\beta,\gamma)$. It's pretty clear that if α,β and γ are all countable then so too is $DT(\alpha,\beta,\gamma)$. It's easy if one uses countable choice. I'm hoping that countable choice is not needed, but i have an awful feeling that it might be ... Do you good people have any light to shed on this?

Am 05/03/2019 um 11:52 schrieb Thomas Forster:

This always happens – to me at any rate. I worry about some problem, and then finally pluck up courage to ask an expert, and then i see the answer! I think the answer to my question is: yes, it really *is* easy. All you have to do is show that, for countable α,β,γ, the set of ordinals notated by $DT(\alpha',\beta',\gamma')$ for $\alpha' < \alpha, \beta' < \beta\gamma' < \gamma$ is a proper initial segment of the ordinals. That shouldn't be too hard. It should be easy to prove that it's a countable set. That'll do it. You don't have to do a scary triple induction. No countable choice needed.

Am i right? Sorry to be wasting your time like this!

Michael replies

If you have countable wellorderings X, Y, it is possible to explicitly construct orderings $X.Y$ and X^Y (and many more) in RCA_0 that have order-type $\alpha.\beta$ and α^β, resp., if alpha and beta are the ordinals corresponding to X and Y, respectively. This explicit construction is familar from ordinal representation systems (can e.g. be found in Girard "Proof Theory and Logical complexity" 5.4.15). So I think one doesn't need AC. However, it might be interesting to figure what background set theory one needs. I surmise that a restricted form of KP with elementhood induction for Σ_1 formulas suffices.

Best

M.

12.2 A Question from Peter Smith

Peter is asking me about the "synthetic" definition of ordinal exponentiation.

Let $\langle A, <_A\rangle$ and $\langle B, <_B\rangle$ be wellorderings of length α and β respectively, with their bottom elements notated '0_A' and '0_B' respectively.

A function $f : A \to B$ is said to be "of "finite support" iff it sends all but finitely many of its arguments to 0_B.

The idea is that if α is the order type of $\langle A, <_A\rangle$ and β is the order type of $\langle B, <_B\rangle$ then α^β is the order type of the set of functions $B \to A$ of finite support, ordered "colex" – by last difference. And let us – strictly in this environment only – write '$B \to A$' to mean nonstandardly the set of functions from B to A *of finite support* (rather than – as is customary – the set of *all* functions $B \to A$).

[Why do we not take a "function of finite support" to be not a total function that sends all but finitely many of its args to 0 but rather one that is undefined except at finitely many arguments? I am not sure, but it's perhaps beco's it (slightly) complicates the definition of the colex ordering. Also there is the consideration that exponentiation of this kind is defined also between arbitrary linear order types with a bottom element, not merely between ordinals, and it outputs linear order types. (Notice that to output linear order types it has to restrict itself to functions of finite support; this means that the connection to cardinals is lost). And it looks wrong that this definition of exponentiation for linear order types should work only if the order type has a bottom element. Actually this looks like a good reason for using the partial function definition!]

So let's write out a proof that the order type of $B \to A$ [finite support version] really is α^β (where the ordinal exponentiation is defined by the usual recursion). Obviously we fix α (so we are doing a UG at top level) and then run a recursion on the exponent.

My students were given this exercise by Paul Russell, and they spent a lot of time proving that the colex ordering on $B \to A$ is in fact a total ordering. This involves a nasty hacky case analysis, which i think can be sidestepped by fixing A and α, and then proving – by induction on β – that any $B \to A$ where otype$(B) = \beta$ is of otype α^β... which is what i now propose to do.

Let's take A to be I_α and B to be I_β. (The set of ordinals $< \alpha$ and $< \beta$ respectively).

Base case ... α^0 and α^1 can be done by hand, as it were. Let's start with α^2.

Case $\beta = 2$

This matches the usual definition of $\alpha \cdot \alpha$.

Case $\beta = \gamma + 1$

Let us write 'C' for I_γ' to make things readable.

To get α^β consider a γ-shaped skeleton list, waiting to have its locations filled in by ordinals below α, all but finitely many of them 0. Order the results colex, by last difference. Now consider the effect of adding an additional address on the end, so there are now $\gamma + 1$ locations, no longer merely γ. We get lots of new functions $B \to A$ of finite support. For each $\zeta < \alpha$ we will get a copy of all the old sequences that made up α^β. The old functions from C to A are not total functions B to A so we have to turn them into such functions if we are to make them into members of $B \to A$. Best to do that by deeming them to all send γ to 0. We now find that they are duplicated by new functions

so we can simply ignore them. However we are interested in their order type, since that is the ghost that remains. Think about the difference between the legacy functions from C, and the new functions that send γ to something other than 0. Since we are ordering things by *last* difference this collection is divided into bundles according to the last element, and each bundle is a copy of the bundle of legacy functions. Each such bundle is of order type α^γ and there are α of them, so the new collection is of order type $\alpha^{\gamma+1} = \alpha^\beta$ as desired.

Case: β is limit.

The key observation here is that every function in $\alpha^{\beta+1}$ appears on the end of everything in α^β so we are talking **end-extensions**, which makes everything continuous. The point is that it is standard that whenever $\langle \mathcal{W}_i : i \in I \rangle$ is a family of wellorderings linearly ordered by end-extension then the order type of the union is the sup of the order types of the $\mathcal{W}_i$.

It follows from the foregoing that

$$\alpha^{\beta_1+\beta_2} = \alpha^{\beta_1} \cdot \alpha^{\beta_2},$$

but it might be enlightening to have a independent hand-crafted artisan proof such as you might pick up in Camden market. Let's have a go.

We have two wellorders B_1 and B_2, with B_2 concatenated on the end of B_1, and a wellorder A. A function f [of finite support] from $B_1 \sqcup B_2$ to A can naturally be thought of as a pair of functions $f_1 : B_1 \to A$ and $f_2 : B_2 \to A$. We have to verify that the lexicographic order on $(B_1 \to A) \times (B_2 \to A)$ is the same as the colex order on $(B_1 \sqcup B_2) \to A$. But that is obvious (isn't it...?)

12.2.1 A snippet from my supervision notes that needs to be worked in

[a question that asks if there is an (initial) ordinal α such that $\alpha = \omega_\alpha$]

Consider the sequence $S = \omega, \omega_\omega, \omega_{\omega_\omega} \ldots$ of von Neumann ordinals. It's supremum (union) is obviously going to be a fixed point. However, this question is on a *Set Theory* sheet not an *Ordinals* sheet, so you should be thinking quite hard about how we use the resources of set theory to prove that there really is a wellordering of this length. So we should be asking: how do we know the ordinals stretch that far? The proof is a long road...

For a start, how do we even know that the sequence is even there at all for us to take its sup? Clearly we are going to need an instance of the axiom scheme of replacement. Whack $\mathbb{N}$ with the function class that sends n to $\omega_{\ldots\omega}$ with n dots. How do we know that this function is defined for all natural numbers? Probably by induction on naturals. Start with ω_ω. How do we know that there is a wellordering of this length? Well, ω_ω is the sup of ω, ω_1, ω_2 ..., and we know that each of these exists by Hartogs' lemma. Then we obtain ω_ω by replacement again. (And it is known that you need replacement to prove the existence of wellorderings that long.) And how are you going to get from ω_ω to ω_{ω_ω}?

"(iv) Show that $\omega^{\omega_1} = \omega_1$. Is ω_1 the least ordinal α such that $\omega^\alpha = \alpha$?
[You may use standard facts about ordinal arithmetic.]"

This is mostly bookwork. However there is a subtlety to part (iv). ω^{ω_1} is of course $\sup\{\omega^\alpha : \alpha < \omega_1\}$ and we want this to be no more than ω_1. It's clearly no *less* than ω_1 because $\alpha \leq \omega^\alpha$ always and the α we are summing over are unbounded below ω_1; for it to be no *greater* than ω_1 we need ω^α to be countable whenever α is. If we try to do this by induction on α we have no problem at successor ordinals of course, co's we're just multiplying by ω, but at limit stages we are liable to find ourselves appealing to the principle that a union of countably many countable sets is countable. Why is ω^λ countable? Well, if λ is countable limit it is $\sup\langle\lambda_n : n \in \mathbb{N}\rangle$ and each (von Neumann ordinal) ω^{λ_n} is [a] countable [set] by induction hypothesis, so the (von Neumann ordinal) ω^λ is [a] countable [set] by countable-union-of-countable-sets-is-countable. This use of countable choice seems to be unavoidable.

However, if we use the synthetic definition of ordinal exponentiation we obtain a set (the set of all those functions from a wellordering of length α to $\mathbb{N}$ that take the value 0 at all but finitely many arguments) equipped with a natural wellordering that is of order type ω^α. This set can be shown to be countable, as follows. Each such function can be thought of as a finite set of ordered pairs of ordinals-below-α paired with naturals. There are countably many such pairs and therefore only countably many finite sets of such pairs.

You probably don't care about such things, Dear Reader (and i bet the examiners didn't) but i didn't get where i am today by being Edward Lear's Old Man of Thermopylæ who never did anything properlæ. As for whether or not you can prove the analogous result for the next operation after exponentiation (namely that the countable ordinals are closed under it) without using countable choice i have to confess that i'd never thought about it. I have an awful feeling that the answer might be 'no'.

Bill,

I've been thinking about that nice stuff about diagonal intersections that your mate The Wrong Ramsey turned up, and i don't like what i'm finding.

Consider a family $\{X_i : i \in \mathbb{N}\}$ of subsets of ω_1 or $\mathbb{N}$; (it won't much matter which). We want a diagonal intersection for it. Well, we pick the first thing – which we call x_1 – in X_1; then for x_2 we pick the first thing $> x_1$ that is in $X_1 \cap X_2$ then for x_3 we pick the first thing $> x_2$ that is in $X_1 \cap X_2 \cap X_3 \ldots$. That way, from x_n on (which is to say cofinitely often) everything is in $X_1 \cap \ldots X_n$. This ensures that the collection $\{x_n : n \in \mathbb{N}\}$ really is almost-below every X_i. (By "A almost-below B" i mean of course that $A \setminus B$ is finite (if i was working on subsets of $\mathbb{N}$) or countable (if i was working on subsets of ω_1).

Obvious question: does this depend on how we order the set of X_i? Another obvious question: what happens if we add not one x at each stage but finitely many? Do we get anything different? The answer to the second question, at least is: yes.

Consider the family $\{\{k \cdot 2^n : n \in \mathbb{N}\} : k \in \mathbb{N}\}$ of subsets of the naturals. If we do the construction i have just outlined above we obtain as our "diagonal intersection" the set $\{2^n : n \in \mathbb{N}\}$. But suppose now we add at each stage not just the first available

thing, but the first three. That way we put into the diagonal intersection first 1, 2 and 3. At stage two we add 2, 4 and 6; at stage three we add 4, 8 and 12; at stage four we add 8, 16 and 24. The difference between this set and the old one we constructed was that this one contains all naturals of the form $3 \cdot 2^n$. And there are infinitely many of them. The worst part of this is that we could decide at each stage to add the first five available, or the first seven, and so on. So there is no diagonal set we can construct that is maximal wrt almost-inclusion.

What this is telling us is that the quotient algebra $\mathcal{P}(\mathbb{N})/\sim$ (where $x \sim y$ iff the symmetric difference $x\Delta y$ is finite) is not a complete boolean algebra. I seem to remember that the boolean algebra $\mathcal{P}(X)/\sim_I$ where $x \sim_I y$ iff the symmetric difference $x\Delta y$ is in the ideal I) is κ-complete as long as the ideal I is κ-saturated – whatever that is. Mind you, we can work out what it is from this theorem!

Dear Richard, David, Dugald and John,

Sorry to trouble you gentlemen, but I have a question about automorphisms of set theory and countable ordinals that you might know something about, and it just might pique your fancy. (Harold and I are giving a minicourse about countable ordinals in the computer lab at the end of this month and it has set me thinking)

The background to these thoughts is that in any axiomatic development of set theory (which is the obvious context for thinking about countable ordinals) there is always the possibility of the models we work in being nonstandard. Nobody is freaked out by the thought of nonstandard naturals. But of course if there are nonstandard naturals then there are nonstandard countable ordinals too. After all, if n is a nonstandard natural, then $\omega + n$ is a nonstandard countable ordinal. This is just an illustration of the fact that any system of notations for countable ordinals will – if there are nonstandard naturals – engender lots of nonstandard countable ordinals too. More of that later.

Of course there are not only models with nonstandard integers but (by Ehrenfeucht-Mostowski for example) there are models with automorphisms that move them! Of course if we are doing this development in set theory (which we probably are) then these automorphism quite possibly act on the rest of the universe as well, and they will certainly act on the countable ordinals as illustrated above. σ of $\omega + n$ will have to be $\sigma(\omega) + \sigma(n)$. ω is definable so $\sigma(\omega) = \omega$. So $\sigma(\omega + n)$ will have to be $\omega + \sigma(n)$.

OK, so suppose we have a nonstandard model of set theory, with an external automorphism σ that moves some naturals. Clearly it moves some countable ordinals as well, by virtue of the systems of notations we have for countable ordinals. If i understand the literature properly then for any countable ordinal α whatever there is a bijection between the ordinals below α and some family-or-other of finite trees decorated by natural numbers, and this bijection preserves enuff structure for us to think of it as a system of notations for ordinals below α. If I understand this correctly, then any automorphism of the naturals can act on the second number class in $\aleph_1$ different ways.

The question this is leading us to is as follows: how informative is this availability of systems of notations for initial segments of the countable ordinals? Does it enable us to calculate precisely what σ does to the countable ordinals once we know what it does to the naturals? For example (and this is actually the particular example I am after) if

we know that $n \geq \sigma(n)$ for n a natural number, does it follow that $\alpha \geq \sigma(\alpha)$ for α an arbitrary countable ordinal?

Put like this, it becomes a general question about the relation between Aut(countable ordinals) and Aut(naturals) in an arbitrary nonstandard model of ZF. How different can two automorphisms of the second number class be if they agree on the naturals?

Joe Shipman writes:

A better example of double exponential growth comes from Conway: the finite ordinals which form a field under nim-addition and nim-multiplication are those of the form 2^{2^n}

Postscript for those who don't have "On Numbers and Games":

Nim-addition = adding base 2 without carrying; the Nim-product of x and y is most simply defined by the following rules:

1. if $x < y$ and y is 2^{2^n}, $x\#y = xy$
2. if $y = 2^{2^n}$, $y\#y = (3y/2)$;
3. use associative and distributive laws to derive the rest

The infinite ordinals which are fields under the Nim operations are much more interesting. ω^{ω^ω} is the first algebraically closed field under the Nim-operations (that is, the ordinal ω^{ω^ω} is the first ordinal transcendental over the earlier ones); the next transcendental is very large, and Conway leaves as an open question what its relationship is to the first impredicative ordinal Γ_0.

John Baez writes:

Gentzen proved the consistency of Peano arithmetic in 1936:

3) Gerhard Gentzen, Die Widerspruchfreiheit der reinen Zahlentheorie, Mathematische Annalen 112 (1936), 493-565. Translated as "The consistency of arithmetic" in M. E. Szabo ed., The Collected Works of Gerhard Gentzen, North-Holland, Amsterdam, 1969.

Goodstein's theorem came shortly afterwards:

4) R. Goodstein, On the restricted ordinal theorem, Journal of Symbolic Logic, 9 (1944), 33-41.

but Kirby and Paris proved it independent of Peano arithmetic only in 1982:

5) L. Kirby and J. Paris, Accessible independence results for Peano arithmetic, Bull. London. Math. Soc. 14 (1982), 285-93.

That marvelous guy Alan Turing wrote his PhD thesis at Princeton under the logician Alonzo Church. It was about ordinals and their relation to logic:

6) Alan M. Turing, Systems of logic defined by ordinals, Proc. London Math. Soc., Series 2, 45 (1939), 161-228.

This is regarded as his most difficult paper. The idea is to take a system of logic like Peano arithmetic and throw in an extra axiom saying that system is consistent, and then another axiom saying *that* system is consistent, and so on ad infinitum - getting

a new system for each ordinal. These systems are recursively axiomatizable up to (but not including) the Church-Turing ordinal.

These ideas were later developed much further....

But, reading original articles is not so easy, especially if you're in Shanghai without access to a library. So, what about online stuff - especially stuff for the amateur, like me?

Well, this article is great fun if you're looking for a readable overview of the grand early days of proof theory, when Hilbert was battling Brouwer, and then Goedel came and blew everyone away:

7) Jeremy Avigad and Erich H. Reck, "Clarifying the nature of the infinite": the development of metamathematics and proof theory, Carnegie-Mellon Technical Report CMU-PHIL-120, 2001. Also available at
http://www.andrew.cmu.edu/user/avigad/Papers/infinite.pdf

But, it doesn't say much about the newer stuff, like the idea that induction up to a given ordinal can prove the consistency of a logical system - the bigger the ordinal, the stronger the system. For work up to 1960, this is a good overview:

8) Solomon Feferman, Highlights in proof theory, in Proof Theory, eds. V. F. Hendricks et al, Kluwer, Dordrecht (2000), pp. 11-31. Also available at
http://math.stanford.edu/~feferman/papers.html

For newer stuff, try this:

9) Solomon Feferman, Proof theory since 1960, prepared for the Encyclopedia of Philosophy Supplement, Macmillan Publishing Co., New York. Also available at
http://math.stanford.edu/~feferman/papers.html

Also try the stuff on proof theory, trees and categories mentioned in "week227", and the book by Girard, Lafont and Taylor mentioned in "week94".

Finally, sometime I want to get ahold of this book by someone who always enlivened logic discussions on the internet until his death in April this year:

10) Torkel Franzen, Inexhaustibility: A Non-Exhaustive Treatment, Lecture Notes in Logic 16, A. K. Peters, Ltd., 2004.

The blurb sounds nice: "The inexhaustibility of mathematical knowledge is treated based on the concept of transfinite progressions of theories as conceived by Turing and Feferman."

I have long suspected that we will eventually be able to expand the foundations of mathematics by using computer technology to define larger recursive ordinals than is possible with out such an aid. To that end I have developed and just released an interactive command line ordinal calculator that supports ordinal notations through and bit beyond those definable by the Veblen function.

The program can be an aid to understanding the recursive ordinals. It supports ordinal arithmetic: (addition, multiplication and exponentiation) displaying the normal form output in plain text and/or LaTeX format. For any ordinal notation in the system, it can list a sequence of smaller ordinals whose union is the original ordinal. Of course, for limit ordinals, it can only list a finite subset of the complete sequence.

This program is licensed for free use and distribution under the GPL version 2 and can be downloaded from
http://www.mtnmath.com/ord or https://sourceforge.net/projects/ord/

This is a beta (first public) release. Any and all feedback including suggested improvements and problem reports will be appreciated.

The program is designed to be expandable and others are encouraged to expand it. In addition to a 6 page user's manual there is a second manual that describes the program structure and gives an overview of and references for the mathematics on which the program is based.

Paul Budnik

www.mtnmath.com

i lookd at schmidt's paper(s). if i have it right she left open the Q whether you can choose a ladder system such that F_i is increasing for all ctble i?

i am not clear if this is now known? the only papers i can find which refer to schmidt are

MR0963205 (89m:03053) Aoyama, Kiwamu(J-KYUSS); Kadota, Noriya(J-HROSEE) A note on built-upness. Mem. Fac. Sci. Kyushu Univ. Ser. A 42 (1988), no. 2, 159–165. 03F15 (03D55) More links PDF Doc Del Clipboard Journal Article Make Link

This note extends the concept of built-up systems of fundamental ordinal sequences by D. Schmidt [Arch. Math. Logik Grundlag. **18** (1976/77), no. 1-2, 47–53; MR0476462 (57 16025a)] and the authors' concept of (n)-built-up system ("(0)-built-up" agrees with "built-up"). The paper introduces the notion of (n)-k-diagonal-built-up systems of fundamental sequences and shows that the canonical system of fundamental sequences used by J. Ketonenn and R. Solovayn [Ann. of Math. (2) **113** (1981), no. 2, 267–314; MR0607894 (84c:03100)] is not (0)-built-up but is (1)-built-up, (1)-0-diagonal-built-up and also (0)-1-diagonal-built-up. The Löb-Wainer system of fundamental sequences [M. H. Löb and S. S. Wainer, Arch. Math. Logik Grundlag. **13** (1970), 39–51; ibid. **13** (1970), 97–113; MR0282922 (44 156) 8ab; correction; MR0317912 (47 6461)] turned out not to be (n)-built-up for any $n < \omega$ but the note shows that this system is (1)-0-diagonal-built-up and also (0)-1-diagonal-built-up.

AND

MR0541689 (81a:04002) McBeth, Rod A note on Hardy's persistent numbers. Z. Math. Logik Grundlag. Math. 25 (1979), no. 4, 375–378. 04A10 (03F15)

More links

PDF Doc Del Clipboard Journal Article Make Link

In 1903, G. H. Hardy [Quart. J. Pure Appl. Math. 35 (1903), 87–94; Jbuch 34, 77] defined for each countable ordinal α a strictly increasing sequence $\{\alpha_k\}$ of positive integers, and was thus able to obtain $\aleph_1$ distinct integer sequences. The construction assumed the existence of ω-fundamental sequences for each countable limit ordinal. The author defines a "natural" fundamental sequence for each limit ordinal $\alpha < \varepsilon_0$ and an associated set of increasing functions $\{h_\alpha : \omega \to \omega | \alpha < \varepsilon_0\}$. Properties of this particular collection of increasing sequences of integers demonstrate the impossibility of defining such "natural" fundamental sequences for all countable limit ordinals. Reviewer's remarks: The impossibility of defining fundamental sequences for all countable limit ordinals with the "natural" properties required by the author has already been proved by H. Bachmann [Transfinite Zahlen, see p. 49, Ergeb. Math. Grenzgeb., Band 1, Springer, Berlin, 1967; MR0219424 (36 2506)]. See also the paper of Diana Schmidt [Arch. Math. Logik Grundlagenforsch. 18 (1976/77), no. 1–2,

47–53; MR0476462 (57 16025a); postscript, ibid. 18 (1976/77), no. 3–4, 145–146; MR0476463 (57 16025b)].

This looks like a message from James

here are the standard proofs of solovay splitting

proof 1: choose a ladder system (IE assign to each delta an increasing cofinal sequence $\alpha(\delta, n) : n < \omega$)

i claim that there is n such that $\alpha(\delta, n)$ "tends to ω_1 modulo the club filter", IE there is n such that for every α there are stat many δ with $\alpha(\delta, n) > \alpha$

suppose not. then for all n there is α_n such that $\alpha(\delta, n) \leq \alpha_n$ for club many δ. intersect the clubs and take the sup α^* of the α_n. then for club many δ we have that for every n, $\alpha(\delta, n) \leq alpha^*$ ... absurd since we can find such a $\delta > \alpha^*$ and then the $\alpha(\delta, n)$ are not cofinal

fix such an n. now we choose by induction increasing countable ordinal β_i such that for every i the set of δ with $\alpha(\delta, n) \in [\beta_i, \beta_{i+1})$ is stationary. the point is to apply Fodor to the stationary set with $\alpha(\delta, n) > \beta_i$ to choose a suitable β_{i+1} [noting that $\delta \mapsto \alpha(\delta, n)$ is regressive!]

proof 2 (much my favourite): suppose that S can't be split. then the ideal NS restriction S is saturated, in fact even more as the quotient algebra has ccc. so force with $\mathcal{P}(\omega_1)/NS$ restruction S to get an ultrafilter $\mathcal{U}$ on the V-powerset of ω_1 which gives S measure one. Now work in $V[U]$ to form the generic ultrapower $V^{omega_1}/\mathcal{U}$, and by standard results of solovay we get a generic embedding $j : V \hookrightarrow M \subseteq V[\mathcal{U}]$, with $\omega_1 \in j(S)$ and $\omega_1 = crit(j)$. this is absurd as S is a set of countable ordinals, so M thinks ω_1 is countable, but M is a submodel of the ccc extension $V[\mathcal{U}]$

On 5/22/2011 10:02 AM, William Tait wrote:

ϵ_0 has various representations. Here's one, due to Lev Beklemishev, that should appeal to computer programmers because the only datatypes involved are integers and strings, no trees or other such representations of Cantor normal form.

Let w be a word over the alphabet $\mathbb{N} = \{0, 1, 2, ...\}$

At stage m, beginning from $m = 1$:

If w is empty then halt;

else if the last character of w is 0 then delete it;

else {

1. Identify the longest suffix of w all of whose characters are at least as large as the last character of w;

2. Decrement the last character of w (and hence of the suffix).

3. Append m copies of the suffix to w.

}

So for example if initially w = 2102031 then w evolves as follows.

1: 210203030

2: 21020303

3: 21020302222

4: $21020302221(2221)^4$

5: $2102030222122212221222122122 12220(22212221222122212220)^5$

and so on.

Those for whom *C* is clearer than English can find further disambiguation at `http://boole.stanford.edu/bek.c`

In `http://www.phil.uu.nl/preprints/preprints/PREPRINTS/preprint219.ps.gz` Beklemishev argues that termination of this process for all words w is equivalent to 1-consistency of PA in Elementary Arithmetic as defined there. (I'd say "shows" instead of "argues" were his argument not well above my pay grade.) Separately he also proves its termination by induction on ϵ_0.

I would have thought termination of the above process for all w was an entirely finitistic matter, so if it isn't then you have my full attention.

I'd be interested to know whether his equivalence result still holds when "m copies" is replaced by "2 copies," or even "1 copy," in step 3.

Vaughan Pratt

Chapter 13

Answers to selected exercises

Exercise1

If every subordering of a given toset is iso to an initial segment then the toset is a wellordering.

Let $\langle X, \leq_X \rangle$ be a nonempty toset whose every suborder is isomorphic to an initial segment. (If it isn't nonempty then it's certainly a wellordering). Since it's nonempty it has a singleton subordering, which must be isomprhic to an initial segment. So $\langle X, \leq_X \rangle$ has a bottom element. So every initial segment has a bottom element. So every subordering has a bottom element. So $\langle X, \leq_X \rangle$ is a wellordering.

Elementary, but important. Curiously the earliest published proof I know of is in my book *Reasoning about theoretical Entities* where i proved it to demonstrate the fitness-for-purpose of an ordinal analysis i was developing. I did that beco's it was a standard fact that my analysis needed to reproduce (Like Russell and Whitehead proving 1 + 1 = 2). I will be grateful to any reader who can find an earlier published proof.

Exercise2

Part 4[1]

```
On May 18 2022, Nikita Fufaev wrote:

> Hello Dr. Forster.
>
> I am in the process of reading  your draft of book, "A Tutorial on
> (mainly countable) Ordinals" found here:
> \url{https://www.dpmms.cam.ac.uk/~tef10/ordinalsforwelly.pdf} but i can't seem
> solve the second exercise. One of the questions asked is 4. Can you simplify
```

[1] There once was a fellow of Trinity
who raised $x\ y\ z$ to infinity;
and then the old brute
extracted the root;
he afterwards took to Divinity.

```
> (\alpha\beta\gamma)^\omega? Disregarding the phrasing of the question
> (which allows me to answer "no" and move on), what is the solution? Or at
> least, what form is the solution? I saw the limerick but i still can't
> find the answer. Should it be an expression consisting of ordinary
> ordinal addition, multiplication and exponential that gives value equal to
> (\alpha\beta\gamma)^\omega for any choice of \alpha, \beta, \gamma from On?
> Should it have less than three operations?
```

The first thing to get straight is whether or not $\alpha\beta\gamma$ can be simplified. So we want to check whether any of these guys "multiplicatively absorb" any of the others. Specifically ask whether or not $\alpha \cdot \beta > \beta$ and $\beta \cdot \gamma > \gamma$. If the answers to these two questions are 'no' then we can't simplify $\alpha\beta\gamma$. The other questions we want to ask are are $\beta\alpha = \alpha$? and $\gamma\beta = \beta$?

$(\alpha\beta\gamma)^\omega$ is of course the sup of $(\alpha\beta\gamma)^n$ for $n < \omega$. This directs our attention to finite multiples like

$$\alpha\beta\gamma\alpha\beta\gamma\alpha\beta\gamma \cdots \alpha\beta\gamma$$

This is the stage at which we have to consider the equations and inequalities alluded to above. If α multiplicatively absorbs β and β multiplicatively absorbs γ then any finite product $(\alpha\beta\gamma)^n$ simplifies to $\alpha^n\beta\gamma$ and the infinite product becomes α^ω.

So my best guess at this stage is that either $\alpha\beta\gamma$ simplifies or, failing that, it's α^ω.

Exercise 3

Give a recursive definition of ordinal subtraction, and prove that your definition obeys $\beta + (\alpha - \beta) = \alpha$.

This is quite a good exercise. Do you fix α and do it by recursion on β? No, beco's you would need to think about deleting the first member of a wellordered set, and that is ungainly. You fix β and declare it by recursion on α

DEFINITION 31

If $\alpha \leq \beta$ *then* 0*; else*
$\mathsf{succ}(\alpha) - \beta = \mathsf{succ}(\alpha - \beta)$*;*
$\mathsf{sup}(A) - \beta = \mathsf{sup}\{\alpha - \beta : \alpha \in A\}$

Exercise 4

1. *Write down subsets of* $\mathbb{R}$ *of order types* $\omega + \omega$, ω^2 *and* ω^3 *in the inherited order.*

For $\omega+\omega$ one of my students came up with $\{1-1/n : n \in \mathbb{N}\}\cup\{10-1/n : n \in \mathbb{N}\}$. Why that rather than $\{1 - 1/n : n \in \mathbb{N}\} \cup \{2 - 1/n : n \in \mathbb{N}\}$, i wondered...[2]? *His* answer is the range of an order-preserving map from the ordinals below $\omega + \omega$ into $\mathbb{R}$. *My* preferred answer is the range of a *continuous* order-preserving map from the ordinals below $\omega + \omega$ into $\mathbb{R}$. [What is the topology on the ordinals in virtue of which this map is cts?]

ω^2 is not that hard: $\{n - 1/m : n, m \in \mathbb{N}\}$, but ω^3 requires a bit of work. The key observation is that, in each copy of ω, the gap between the mth and the $m + 1$th point is $\frac{1}{m(m+1)}$ wide, so if you want to squeeze an extra copy of ω in there you do

$$\{n - \frac{1}{m} - \frac{1}{km(m + 1)} : n, m, k \in \mathbb{N}\}$$

Actually an answer i have just seen from one of my students (thank you Louie Gabriel!) suggests that you can get ω^n by continued fractions of length n. I think that works, and that the key is to show that the set of continued fractions of length n with coefficients from $\mathbb{N}\backslash\{0\}$, (using subtraction not addition!) is legicographically ordered to order type ω^n:

$$a_0 - \cfrac{1}{a_1 - \cfrac{1}{a_2 - \cfrac{1}{a_3 + \cdots}}} \tag{CF1}$$

For example:

$$\{a_0 - \frac{1}{a_1} : a_0, a_1 \in \mathbb{N} \setminus \{0\}\} \tag{CF2}$$

gives ω^2.

Key observation: multiplicative inversion and additive inversion are both order-reversing, so their composition is order-preserving, with the effect that expressions like (CF1) and (CF2) above are monotone increasing in all the a_i. We can make this explicit by rearranging $a_0 - \frac{1}{a_1}$ to $(a_0 \cdot a_1 - a_1)/a_1$ and $((a_0 - 1) \cdot a_1)/a_1$; finally ignoring the denominator since is it positive and doesn't affect the order (and ignore the '-1' similarly) to get $a_0 \cdot a_1$ which looks like $\mathbb{N} \times \mathbb{N}$.

So the next term we want is

$$a_0 - \frac{1}{a_1 - \frac{1}{a_2}} \tag{CF3}$$

which is $(a_0 \cdot a_1 \cdot a_2 - 1 - a_2)/(a_1 \cdot a_2 - 1)$ which we can analogously process into $(a_0 \cdot a_1 - 1) \cdot a_2$ which looks like $\mathbb{N}^3$

[2] Actually it has just occurred to me that his '10' is binary!!

If the order is genuinely to be lexicographic we need to know that altering a_2 *ad lib* cannot have as much effect as altering a_1 by even 1. And this is clear: however small we make a_2 (and it cannot be smaller than 2) we cannot get the effect of altering a_1.

So the claim is that

$$\{a_0 - \frac{1}{a_1 - \frac{1}{a_2 - \frac{1}{a_3}}} : a_0, a_1, a_2, a_3 \in \mathbb{N} \setminus \{0\}\}$$

is a subset of $\mathbb{Q}$ of order type ω^4 in the inherited order. And so on!

I think it's pretty clear that this works for continued fractions of this (rather restricted) style for all n, so we get – for each $n \in \mathbb{N}$ – a set of rationals of length ω^n in the inherited order. Let us call the nth subset of the rationals thus obtained W_n, so that the displayed set is W_0.

Notice that we do *not* have $W_n \subseteq W_{n+1}$! This is an infelicity rather than a bug. When we replace W_n by W_{n+1} we do not so much put a copy of $\mathbb{N}$ at each place where we had a point before, as *delete* that point and then insert a copy of $\mathbb{N}$ *after* the hole we have just made. W_0 contains all the natural numbers, but W_1 doesn't contain any natural numbers. So really the representation of ω^n that we want is not so much W_n as $\bigcup_{m \leq n} W_m$.

I don't think there is any real mathematics in this, but it is quite cute.

It is natural to expect that if we redefine W_n in this way then the order type of the union must be ω^ω. A word of warning is perhaps in order here. It is not generally clear that the union of a nested family of wellorderings is a wellordering. After all, the negative integers is the union of the nested finite wellorderings $[-n, 0]$.

In fact we do *not* get ω^ω. This is because lots of things have stuff inserted *below* them at later stages, so one obtains infinite descending sequences in the union. There is an old tripos question about this is which it will do you no harm to look at: 2009 paper 3 16G. I have a discussion answer to this question which is linked from my home page.
`https://www.dpmms.cam.ac.uk/~tef10/cam_only/oldLSTtriposquestions.pdf`

Better make it universally visible

2. Let α, β and γ be ordinals.

   If $\alpha \leq \beta$, must we have $\alpha + \gamma \leq \beta + \gamma$?

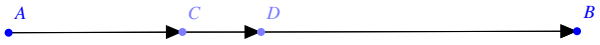
   If $\alpha < \beta$, must we have $\alpha + \gamma < \beta + \gamma$?

   The first thing to do is to recall lemma 1 to the effect that the two definitions of $\leq$ for ordinals are equivalent.

   Does a picture serve for a proof for questions like these? Depends partly on whether you are (i) trying to persuade yourself of the truth of the allegation

(by gaining understanding) in which case it's probably all right, or (ii) trying to remove all doubt, in which case it might not be.

In any case, the way to understand these questions is by thinking of ordinals as isomorphism classes of wellorderings. Don't even think about trying to prove them by reasoning about von Neumann ordinals. There are many reasons for this. One fairly compelling one is that there is no corresponding way of concretising order types of total orders that don't happen to be wellorderings. So if you think of ordinals as von Neumann ordinals not only do you burn in hell for all eternity but you lose the connection with order types in general.



AC is of length α;
AD is of length β;
DB is of length γ.

This picture makes it obvious that the answer to the first part is 'yes'; so of course you expect the answer to the second part to be 'no', and you are correct: $1 < 2$ but $1 + \omega = 2 + \omega = \omega$.

Notice that adding on the right preserves strict inequality: $\omega + 1 < \omega + 2$

3. *Show that the inductive and synthetic definitions of ordinal multiplication agree.*

   This question goes to the heart of how to think of ordinals.

   The correct way to prove that the two definitions are equivalent is to fix α and prove by induction on β that the two definitions agree on $\alpha \cdot \beta$.

   Well it's obviously true for $\beta = 0$! (OK, it's trivial, but at least it's a start.)

   Suppose $\beta = \gamma + 1$. Then the recursive definition tells us that $\alpha \cdot \beta = \alpha \cdot \gamma + \alpha$. But this is clearly the length of a wellorder (any wellorder) obtained by putting a wellorder of length α on the end of a wellorder of length $\beta \cdot \gamma$.

   It's at the limit stage that we have to do some work. So suppose the inductive and synthetic definitions of $\alpha \cdot \gamma$ agree for all $\gamma < \beta$. Consider a wellorder that is of length $\alpha \cdot \beta$ according to the synthetic definition. Up to isomorphism we can think of it as the lexicographic product of $\langle A, <_A\rangle \times \langle B, <_B\rangle$ for two wellorderings $\langle A, <_A\rangle$ and $\langle B, <_B\rangle$ of lengths α and β. Now let γ be an ordinal below β. Every such ordinal is the order type (length) of a unique initial segment of $\langle B, <_B\rangle$; let us write this as $\langle B, <_B\rangle \restriction \gamma$. Our lexicographic product $\langle A, <_A\rangle \times \langle B, <_B\rangle$ is now a colimit of all the $\langle A, <_A\rangle \times \langle B, <_B\rangle \restriction \gamma$ for $\gamma < \beta$. Each $\langle A, <_A\rangle \times \langle B, <_B\rangle \restriction \gamma$ is of length $\alpha \cdot \gamma$ – and that is according to *either* definition, by induction hypothesis.

So the length of $\langle A, <_A\rangle \times \langle B, <_B\rangle$ must be the supremum of $\{\alpha \cdot \gamma : \gamma < \beta\}$, and this is the recursive definition of $\alpha \cdot \beta$.

4. *Is there a non-zero ordinal α with $\alpha\omega = \alpha$? What about $\omega\alpha = \alpha$?*

   These are easy if you have correctly understood the (synthetic definition) of ordinal multiplication. Just in case you need a reality check, there is no α s.t. $\alpha \cdot \omega = \alpha$, whereas there are lots of α s.t. $\omega \cdot \alpha = \alpha$. Let β be any ordinal s.t. $1 + \beta = \beta$. Then $\omega^\beta = \omega^{1+\beta} = \omega \cdot \omega^\beta$.

   Why is there no ordinal α s.t. $\alpha = \alpha \cdot \omega$? Various ways of seeing this. You can argue that, beco's α is an ordinal, you have $\alpha < \alpha + 1 \leq \alpha \cdot \omega$. Or you can do this:

   Suppose α is a linear (aka total) order type satisfying $\alpha = \alpha \cdot \omega$. Then there is a linear order $\langle A, <_A\rangle$ which is isomorphic to a proper initial segment of it. Let π be the isomorphism. Consider any $x \in A \setminus \pi\text{“}A$. We must have $\pi(x) <_A x$, so $x >_A \pi(x) >_A \pi^2(x) \ldots$ is a subset of A lacking a least member. So $\langle A, <_A\rangle$ is not a wellorder, so α is not an ordinal.

   Moral: no wellordering can be isomorphic to a proper initial subset of itself.

   I am making two points here. One is that when it comes to proving things about ordinals *that rely on the things being ordinals* you don't *absolutely have to* do induction; there may be another way of exploiting the fact that these things are ordinals. The other point is that some of things that don't happen with ordinals might happen with other order types: $\alpha = \alpha \cdot \omega$ can happen if α is not an ordinal.

   (Can you find an example?)

5. *Let α, β, γ be ordinals.*

   Must we have $(\alpha + \beta)\gamma = \alpha\gamma + \beta\gamma$?

   Must we have $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$?

   The first is false and the second is true. Remember what multiplication is: $\alpha \cdot \beta$ is the order-type of a thing that is β copies of thing of length α – not the other way round. The definition is not symmetrical so you shouldn't expect multiplication of order types to be commutative. The only sane way to prove this is by using the synthetic definition. In fact it is *always* best to prove facts about ordinals synthetically (wherever possible) rather than by induction. Let me say a bit about why this is so. Doing it by induction relies on the three order-types being ordinals (or at last one on which you are doing the induction being an ordinal) but that's not why it's true. It's true for *arbitrary* linear order types; the fact that α, β and γ are ordinals is irrelevant and shouldn't be exploited!

   If you want to do it by induction there are some things you should think about. For a start there are two kinds of induction you can do over the ordinals. There is structural induction, where you consider three cases: (i) $\alpha = 0$, (ii) α successor, and (iii) α limit. Then there is *wellfounded* induction where you prove that α is F as long as every smaller ordinal is F. These correspond to the two kinds of

induction you can do over $\mathbb{N}$, and they are of course equivalent – just as those two kinds of induction over $\mathbb{N}$ were. But in practice of course it's sometimes much easier to do it one way rather than the other.

Now suppose you are trying to prove that $\phi(\alpha,\beta)$ holds for all ordinals α and β. There are six ways you could do it.

(i) Say: "let α and β be arbitrary", reason about them, conclude the things you want;

(ii) You could fix α, and prove by induction on β that $(\forall\beta)(\phi(\alpha,\beta))$, where your induction hypothesis is $\phi(\alpha,\beta)$; then say "but α was arbitrary…"

(iii) You could fix β, and prove by induction on α that $(\forall\alpha)(\phi(\alpha,\beta))$ where your induction hypothesis is $\phi(\alpha,\beta)$; then say "but β was arbitrary…"

(iv) You could prove by induction on α that $(\forall\beta)(\phi(\alpha,\beta))$ where your induction hypothesis is $(\forall\beta)(\phi(\alpha,\beta))$;

(v) You could prove by induction on β that $(\forall\alpha)(\phi(\alpha,\beta))$ where your induction hypothesis is $(\forall\alpha)(\phi(\alpha,\beta))$;

(vi) You could perhaps do a wellfounded induction on the lexicographic product … infer $\phi(\alpha,\beta)$ from the assumption that $\phi(\alpha',\beta')$ holds for all pairs α',β' below α,β in the lexicographic product.

That's bad enough. The thing we are challenged to prove here has *three* variables in it. We need a rule of thumb. One of my students made a rather good remark about this. He says: "always do the induction on the rightmost variable". Admittedly this sounds a bit hand-wavy but it looks to me like good advice[3]. The point is that the recursions for + and × and exp all work on the rightmost variable.

Some thoughts and advice is in order on this first crop of questions on ordinals and order types. You will encounter questions about equations and inequations, and invited to prove the true ones and find counterexamples to those that are false. Some of the true ones (like distributivity on the right of × over +, and associativity of × and +) work for arbitrary linear order types and therefore can be proved by hand and you don't need induction. *Don't use induction if you don't have to!* Some of them work only for ordinals and then you need to exploit the fact that you are dealing with ordinals. $\alpha + 1 > \alpha$ is true for ordinals but not for arbitrary linear order types (think of ω^*) *so you have to exploit somehow the fact that α is an ordinal.* Exploiting the fact that the characters in your play are ordinals doesn't necessarily mean you have to be doing an *induction* …tho' it usually does.

[3] Always learn from your students!

6. *Find two totally ordered sets such that neither is isomorphic to a subset of the other. Can you find three such sets?*

   You want three tosets none of which embeds in either of the others? Piece of cake. The rationals, the countable ordinals and the countable ordinals turned upside-down. In fact with a little work you can show – just using lots of copies of $\mathbb{N}$ and $\mathbb{N}$ upside-down (the negative integers) – that you can get finite antichains as wide as you like. Here's how to get an antichain of width 2^n. Take all your n-bit words, and in each replace the 0s by ω and the 1s by ω^* (recall that ω^* is the order type of the negative integers) , and concatenate them. Thus, when $n = 2$, you get the 2^2 order types: $\omega + \omega$, $\omega + \omega^*$, $\omega^* + \omega$ and $\omega^* + \omega^*$ which form an antichain. Can you get infinite antichains? Think about what happens if you have things like this made from ω pieces strung together. You don't get an infinite antichain! Yes, you *can* get infinite antichains, but in every infinite antichain there must be at least one total ordering of an uncountable set (so, in fact, infinitely many, if you think about it). This is corollary of a beautiful theorem of the late and much lamented Richard Laver. If you want to have a look at it (and it is *very* nice) then point your search engine at *Laver's proof of the Fraïssé conjecture*.

7. *Let α, β and γ be ordinals.*

   (i) Must we have $\alpha^{\beta+\gamma} = \alpha^\beta \cdot \alpha^\gamma$?

   (ii) Must we have $\alpha^{\beta^\gamma} = \alpha^{\beta\cdot\gamma}$?

   (iii) Must we have $(\alpha \cdot \beta)^\gamma = \alpha^\gamma \cdot \beta^\gamma$?

   Make sure you really understand ordinal exponentiation before you tackle this question . . . it's deceptively hard.

   The first is pretty obviously true, and you prove it by induction (on 'γ').

   It may be worth pointing out that the true equations concerning exponentiation also work for arbitrary linear order types and can be proved synthetically using the synthetic definition of ordinal exponentiation . . . which you haven't been given. So you will have to use induction!

   Part (ii) is true and you prove it by induction on 'γ'.

   Part (iii) is false; take $\alpha = \beta = 2$ and $\gamma = \omega$.

Exercise 5

"Let $\langle X, R\rangle$ be a wellfounded binary structure, with rank function ρ. Prove that

$$(\forall x \in X)(\forall \alpha < \rho(x))(\exists y \in X)(\rho(y) = \alpha).$$

You're obviously going to do this by induction; but is it by induction on R or on $<_{On}$?

You do it by induction on R. The assertion to prove for all $x \in X$ is that

$$(\forall \alpha < \rho(x))(\exists y \in t(R)\text{“}\{x\})(\rho(y) = \alpha) \qquad (**)$$

The rather strange-looking existential quantifier is saying that there is a y related to x by the transitive closure $t(R)$) such that ....

Suppose (**) holds for all z s.t. zRx, and let $\alpha < \rho(x)$. If $\rho(x)$ is successor, life is easy; if $\rho(x)$ is limit then $\alpha < \rho(z)$ for some z s.t. zRx. But then there is a witness to the '$\exists y \in t(R)$"x}) by induction hypothesis.

■

Exercise 6

Show that $\omega^{\omega_1} = \omega_1$.

Is ω_1 the least ordinal α such that $\omega^\alpha = \alpha$?

[You may use standard facts about ordinal arithmetic.]

ω^{ω_1} is of course $\sup\{\omega^\alpha : \alpha < \omega_1\}$ and we want this to be no more than ω_1. It's clearly no *less* than ω_1 because $\alpha \leq \omega^\alpha$ always and the α we are summing over are unbounded below ω_1; for it to be no *greater* than ω_1 we need ω^α to be countable whenever α is. If we try to do this by induction on α we have no problem at successor ordinals of course, co's we're just multiplying by ω, but at limit stages we are liable to find ourselves appealing to the principle that a union of countably many countable sets is countable. Why is ω^λ countable? Well, if λ is countable limit it is $\sup\langle\lambda_n : n \in \mathbb{N}\rangle$ and each (von Neumann ordinal) ω^{λ_n} is [a] countable [set] by induction hypothesis, so the (von Neumann ordinal) ω^λ is [a] countable [set] by countable-union-of-countable-sets-is-countable. This use of countable choice seems to be unavoidable.

However, if we use the synthetic definition of ordinal exponentiation we obtain a set (the set of all those functions from a wellordering of length α to $\mathbb{N}$ that take the value 0 at all but finitely many arguments) equipped with a natural wellordering that is of order type ω^α. This set can be shown to be countable, as follows. Each such function can be thought of as a finite set of ordered pairs of ordinals-below-α paired with naturals. There are countably many such pairs and therefore only countably many finite sets of such pairs.

I may yet be prodded into explaining why this second argument doesn't require Choice. I can imagine that it's not obvious!

Exercise 20

PTJ comments:

[*The original question worked with ω-continuous functions, for which one has a much easier proof of the existence of fixed points, but the question itself becomes harder because you have to verify that every function in sight is ω-continuous. As it stands, it should be pretty easy, except for the proof that m is order-preserving (needed to show that f is order-preserving): for this, observe that if $x_1 \leq x_2$ then $m(x_2)$ is a 'post-fixed point' of g_{x_1} (that is, $m(x_2) \geq g_{x_1}(m(x_2))$), and so $\{y \in Q : y \leq m(x_2)\}$ is a 'closed set' in the sense used in the construction of the least fixed point $m(x_1)$ of g_{x_1}.*]

And my discussion...

1. Given $x \in P$, suppose $y_1 \leq y_2 \in Q$. Then $\langle x, y_1\rangle \leq \langle x, y_2\rangle$ so $h(\langle x, y_1\rangle) \leq h(\langle x, y_2\rangle)$ so $g_x(y_1) = h_2(\langle x, y_1\rangle) \leq h_2(\langle x, y_2\rangle) = g_x(y_2)$, so g_x is order-preserving.

2. m is order-preserving. *Proof:*

   Suppose $x_1 \leq x_2 \in P$. Set $Y = \{y \in Q : y \leq m(x_2)\}$. For $y \in Y$ we have $g_{x_1}(y) = h_2(\langle x_1, y\rangle) \leq h_2(\langle x_2, y\rangle) = m(x_2)$ so g_{x_1} acts on Y.

   Now if $C \subseteq Y$ is a chain then its sup is below $m(x_2)$ so Y is chain-complete, whence $g_{x_1} \restriction Y$ has a fixed point $y_0 \in Y$ with $m(x_1) \leq y_0 \leq m(x_2)$ and m is order-preserving.

   Now suppose $x_1 \leq x_2 \in P$ again. Then $\langle x_1, m(x_1)\rangle \leq \langle x_1, m(x_1)\rangle$. So $f(x_1) \leq f(x_2)$ and f is order-preserving.

3. $h(x_0, m(x_0)) = \langle f(x_0), g_{x_0}(m(x_0))\rangle = \langle x_0, m(x_0)\rangle$ so $\langle x_0, m(x_0)\rangle$ is a fixed point of h. Let $\langle x, y\rangle$ be the least fixed point of h. Then $g_x(y) = y$ so $y \geq m(x)$.

4. Let $Z = \{\langle a, b\rangle \in P \times Q : \langle a, b\rangle \leq \langle x, m(x))\rangle\}$

   For $\langle a, b\rangle \in X$:

   $h(a, b) \leq h(x, m(x)) \leq \langle h_1(x, y), h_2(x, m(x))\rangle = \langle x, m(x)\rangle$ so h acts on Z. Furthermore, Z is chain-complete and has a least element, similar to claim above. So h has a fixed point $\langle x', y'\rangle \in Z$. Now $\langle x, y\rangle \leq \langle x', y'\rangle \leq \langle x, m(x)\rangle$. But $\langle x, y\rangle \geq \langle x, m(x)\rangle$ so $\langle x, y\rangle = \langle x, m(x)\rangle$.

   So x is a fixed point for f, whence $x \geq x_0$. But m is order-preserving so $y = m(x) \geq m(x_0)$. So $\langle x, y\rangle \geq \langle x_0, m(x_0)\rangle$ and $\langle x_0, m(x_0)\rangle$ is the least fixed point of h.

Bibliography

[1] Jeremy Avigad and Erich H. Reck, "Clarifying the nature of the infinite": the development of metamathematics and proof theory, Carnegie-Mellon Technical Report CMU-PHIL-120, 2001. Also available at http://www.andrew.cmu.edu/user/avigad/Papers/infinite.pdf

[2] N. Bourbaki, Sur le theorème de Zorn, Arch. Math. **2** (1950), 434–437.

[3] Buchholz, W. and Wainer S. Provably computable functions and the fast-growing hierarchy. Logic and Combinatorics, AMS Contemporary Mathematics **65** (1985) pp 179-198.

[4] See http://en.wikipedia.org/wiki/Carlson's_theorem

[5] Elwyn R. Berlekamp, John H. Conway, and Richard K. Guy "Winning Ways for Your Mathematical Plays" (Academic Press, 1982) available at https://annarchive.com/files/Winning%20Ways%20for%20Your%20Mathematical%20Plays%20V1.pdf

[6] John Doner and Alfred Tarski. An Extended Arithmetic of ordinal numbers. Fundamenta Mathematicæ **LXV**(1969) 95–127. Also on http://www.math.ucsb.edu/~doner/articles/.

[7] Ehrenfeucht, A. "Polynomial functions with exponentiation are wellordered" *Algebra universalis* **3** December 1973, Issue 1, pp 261–262

[8] Fairtlough, M and Wainer, S. Hierarchies of Provably Recursive Functions: chapter III of Handbook of Proof Theory (S.Buss Ed) Elsevier (1995) pp 148-205.

[9] Torkel Franzen, Inexhaustibility: A Non-Exhaustive Treatment, Lecture Notes in Logic **16**, A. K. Peters, Ltd., 2004.

[10] Solomon Feferman, Highlights in proof theory, in Proof Theory, eds. V. F. Hendricks et al, Kluwer, Dordrecht (2000), pp. 11-31. Also available at http://math.stanford.edu/~feferman/papers.html

[11] Solomon Feferman, Proof theory since 1960, prepared for the Encyclopedia of Philosophy Supplement, Macmillan Publishing Co., New York. Also available at http://math.stanford.edu/~feferman/papers.html

[12] Geza Fodor, Eine Bemerkung zur Theorie der regressiven Funktionen, Acta Scientiarum Mathematicarum, Szeged, **17** (1956), pp. 139–142.

[13] Gerhard Gentzen, Die Widerspruchfreiheit der reinen Zahlentheorie, Mathematische Annalen **112** (1936), 493-565. Translated as "The consistency of arithmetic" in M. E. Szabo ed., The Collected Works of Gerhard Gentzen, North-Holland, Amsterdam, 1969.

[14] R. Goodstein, On the restricted ordinal theorem, Journal of Symbolic Logic, **9** (1944), 33-41.

[15] Hardy, G. H. Quarterly J. of Pure and Applied Mathematics. **35** (1903) 87-94.

[16] A Joyal and E Moerdijk Algebraic set theory. LMS lecture notes series **220** CUP 1995

[17] L. Kirby and J. Paris, Accessible independence results for Peano arithmetic, Bull. London. Math. Soc. **14** (1982), 285–93.

[18] Hilbert Levitz "An ordinal bound for the set of polynomial functions with exponentiation". *Algebra universalis* **8** (1978) 233–243

[19] Eliot Mendelson, Introduction to Mathematical Logic Van Nostrand, various editions.

[20] W.V. Quine Set Theory and its Logic. Harvard

[21] by D. Richardson "Solution of the identity problem for integral exponential functions" Zeilschr. f. math. Logik und Grundlagen d. Math. **15**, S. 333-340 (1969)

[22] Diana Schmidt. "Built-up Systems of Fundamental Sequences and Hierarchies of Number-Theoretic Functions". Arch. Math. Logik. **18** (1976) pp 47–53.

[23] H. Simmons A Comparison of Two Systems of Ordinal Notation, Arch. Math. Logic **43** (2004) pp 65–83.

[24] C. Smorynski Some rapidly growing functions, Mathematical intelligencer **2** pp 149-154

[25] C. Smorynski Varieties of arboreal experience, Mathematical Intelligencer **4** (1982) pp 182-189.

[26] Alan M. Turing, Systems of logic defined by ordinals, Proc. London Math. Soc., Series 2, **45** (1939), 161–228.

[27] Wainer, S. [1996] Basic Proof Theory with Applications to Computation. Leeds preprint series **18**.

[28] Wikipedia, Ordinal numbers, `http://en.wikipedia.org/wiki/Ordinal_number` Ordinal arithmetic, `http://en.wikipedia.org/wiki/Ordinal_arithmetic` Large countable ordinals, `http://en.wikipedia.org/wiki/Large_countable_ordinals`

[29] E. Witt, Beweisstudien zum Satz von M. Zorn, Math. Nachr. **4** (1951), 434–438.

13.1 Stuff to fit in

Any system $\mathcal{F}$ of fundamental sequences for an initial segment Γ of the second number class will give a bijection between Γ and $\mathbb{N}$. If $\mathcal{F}$ is nice then the bijection should send every fundamental sequence in $\mathcal{F}$ to a strictly increasing sequence $\mathbb{N} \to \Gamma$. Is it always the case that, given Γ and $\mathcal{F}$ there is a bijection $\mathbb{N} \longleftrightarrow \Gamma$ according to which every fundamental sequence is increasing?

Let's try. We have countably many fundamental sequences from $\mathcal{F}$. All we have to do is interleave them. Doesn't that do it? It does if the fundamental sequences provide a partition of Γ. They don't, at least not straightforwardly. ω is the first member of a fundamental sequence for $\omega \cdot 2$ and also the first member of a fundamental sequence for ω^2. We'd better check that there is a safe way of excluding the double counting.

Here's how. You enumerate all the limit ordinals in Γ in order-type ω and line up all the fundamental sequences. You the delete from any fundamental sequence any ordinal that appears in an earlier sequence. Assuming that the intersection of the ranges of two fundamental sequences is of size 1 at most this ensures that there is no double counting. Is everything covered? Yes, every successor ordinal gets hit beco's every successor ordinal is in some interval $(\lambda, \lambda + \omega)$ and that of course is a fundamental sequence. But actually it doesn't matter if not everything is covered. If there are things not in the union of all the fundamental sequences then you just order them in otype ω and interleave them like all the others.

So we have proved:

REMARK 24 *For every initial segment Γ of the second number class and every system $\mathcal{F}$ of fundamental sequences for Γ there is a bijection between Γ and $\mathbb{N}$ which turns every fundamental sequence into a strictly increasing sequence of naturals.*

Can we do it the other way round? Given Γ and an enumeration of it can we find $\mathcal{F}$ so that all fundamental sequences in $\mathcal{F}$ are increasing sequences? This is even easier. Given Γ and the bijection $\Gamma \longleftrightarrow \mathbb{N}$ we build $\mathcal{F}$ with complete freedom. You want a fundamental sequence for α? There are infinitely many ordinals less than it. You then procede as in the proof that every countable limit ordinal has cofinality ω. So you can do it for all α independently and simultaneously. But of course there is no guarantee that the fundamental sequences you obtain will be disjoint. To do that you have to enumerate the limit ordinals in Γ in otype ω and make sure you don't re-use anything.

Harold's ever-increasing functionals

$$Sn = n + 1$$

$$Jfn = f^{n+1}1$$

$$KJfn = J^{n+1}f1$$

$$LKJfn = K^{n+1}Jf1$$

(i) $\aleph_1 \leq 2^{\aleph_0}$ cannot be done without (at least some) choice.

(ii) Second number class cannot be injected into $\langle \mathbb{R}, <_{\mathbb{R}} \rangle$ *at all*! even *with* Choice.

Recall the discussion earlier of the various injections of proper initial segments of the second number class into $\mathbb{R}$; how the destinations of ω do *not* form a nice descending sequence.

Which of these two lies behind the Schmidt conditions?

LEMMA 14 *The ordinals $\leq \alpha$ are totally ordered by $\leq$.*

Proof:

details here

We do this by induction on α. The base case is immediate; the succ case is just like the inductive proof that $<_{\mathbb{N}}$ is a total order. For the limit case we exploit $(\forall\alpha)(\forall S \subset On)((\alpha < \mathtt{sup}(s)) \rightarrow (\exists\beta \in S)(\alpha \leq \beta))$.

If $\alpha_1 \leq \mathtt{sup}(S)$ and $\alpha_2 \leq \mathtt{sup}(S)$ then there is $\beta \in S$ with $\alpha_1 \leq \beta$ and $\alpha_2 \leq \beta$. (Indeed, by lemma 2, β can be taken to be $\alpha_1 + \alpha_2$ or $\alpha_2 + \alpha_1$.) But then α_1 and α_2 are comparable by induction hypothesis.

■

COROLLARY 5 *$<_{On}$ is a wellorder.*

Proof:

It's wellfounded because it is the engendering relation of a rectype. To show it's a total order consider two arbitrary ordinals α and β. By lemma 2, α and β are both $\leq \alpha + \beta$. Then by lemma 14 the ordinals below $\alpha + \beta$ are totally ordered. ■

This proof of corollary 5 is mine, though it may well have been anticipated. If so, I hope my readers will tell me. There is a proof concealed in the papers of Bourbaki [2] and Witt [29] (See Appendix 1).

> *It now seems to me that one can give a much shorter proof that $<$ is a total order. We know it is wellfounded. Consider a minimal member α_1 of $X = \{\alpha : (\exists\beta)(\alpha \neq \beta \not> \alpha \not> \beta)\}$, and then a minimal member α_2 of $\{\alpha : \alpha \neq \alpha_1 \not> \alpha \not> \alpha_1\}$. Thus α_1 and α_2 are incomparable minimal elements of X. The ordinals below α_1 form a chain A_1 and the ordinals below α_2 form a chain A_2. Now these must be the same chain, so we call it A. If A has a top element – α, say – then α_1 and α_2 must both be* succ(α). If not, they must both be sup(A). Either way, they are the same.

Quite how useful this fact is when dealing with an arbitrary ordinal β will depend on β. After all, if $\beta = \omega^\beta$ then – if we run the algorithm with ω and β – all Cantor's normal form theorem will tell us is that this is, indeed, the case. Ordinals β s.t. $\beta = \omega^\beta$ are around in plenty. They are called ϵ-*numbers*. They are moderately important because if β is an ϵ-number then the ordinals below β are closed under exponentiation. The smallest ϵ-number is called 'ϵ_0'. For the moment what concerns us about ϵ_0 is that if we look at the proof of Cantor's Normal Form theorem in the case where β is an ordinal below ϵ_0 and $\alpha = \omega$ the result is something sensible. This is because, ϵ_0 being the *least*

fixed point of $\alpha \mapsto \omega^\alpha$, if we apply the technique of remark 3 to some $\alpha < \epsilon_0$ the output of this process must be an expression containing ordinals below α.

Now we must ask a very mathematical question, one that might have occurred to you already. On what features of multiplication, exponentiation and addition does this construction actually rely? Suppose we have a family $\langle f_i : i \in On \rangle$ of functions of two arguments defined in the manner of definition 8 so that

$$f_{n+1}(\alpha, \gamma + 1) = f_n(f_{n+1}(\alpha, \gamma), \alpha). \tag{13.1}$$

(and we require $\gamma \mapsto f_{n+1}(\alpha, \gamma)$ to be continuous at limit γ. We'll worry later about what to do when the subscript is limit!).

Suppose we want to express a given β in terms of a given α and n. What do we need? We want the various f_n to be normal in at least one argument. That is to say, for each n and every ζ, the function $\tau \mapsto f_n(\zeta, \tau)$ must be normal. That way we can be sure – to return to our given β, α and n – that there is a *last* γ so that

$$f_n(\alpha, \gamma) \leq \beta$$

which is to say, there is a γ so that

$$f_n(\alpha, \gamma) \leq \beta < f_n(\alpha, \gamma + 1)$$

Of course if $f_n(\alpha, \gamma) = \beta$ we stop. Otherwise we have

$$f_n(\alpha, \gamma) < \beta < f_n(\alpha, \gamma + 1) = f_{n-1}(f_n(\alpha, \gamma), \alpha)$$

Now, by normality of $\zeta \mapsto f_{n-1}((f_n(\alpha, \gamma), \zeta)$, there will be a last δ such that

$$f_{n-1}((f_n(\alpha, \gamma), \delta) \leq \beta$$

and we repeat the process.

Notice that addition, multiplication and exponentiation are related as successive members of precisely this kind of sequence of functions:

$$f_0(\alpha, \beta) := \alpha + 1$$

$$f_1(\alpha, \beta) := \alpha + \beta$$

$$f_2(\alpha, \beta) := \alpha \cdot \beta$$

$$f_3(\alpha, \beta) := \alpha^\beta$$

So the definitions from definition 8 give rise to a system of ordinal notations.

The following old tripos question (which had an afterlife on PTJ's example sheet 4 for Part II Set theory and Logic) can be profitably reviewed here.

EXERCISE 20 *(Tripos IIA 1995 Paper 4 question 8, modified).*

Let $\mathcal{P} = \langle P, \leq \rangle$ and $\mathcal{Q} = \langle Q, \leq \rangle$ be chain-complete posets with least elements, and let $h : \mathcal{P} \times \mathcal{Q} \to \mathcal{P} \times \mathcal{Q}$ be a map which is order-preserving with respect to the pointwise product ordering. Let the two components of the ordered pair $h(x, y)$ be $h_1(x, y)$ and $h_2(x, y)$ respectively.

1. *Show that, for each fixed $x \in P$, the mapping $g_x : Q \to Q$ defined by $g_x(y) = h_2(x, y)$ is order-preserving. Let $m(x)$ be its least fixed point.*

2. *Show that the map $f : P \to P$ defined by $f(x) = h_1(x, m(x))$ is order-preserving. Let x_0 be its least fixed point.*

3. *Show that $\langle x_0, m(x_0) \rangle$ is the least fixed point of h.*