Part III — Logic
Theorems with proof

Based on lectures by T. E. Forster
Notes taken by Dexter Chua

Lent 2017

This course is the sequel to the Part II courses in Set Theory and Logic and in Automata and Formal Languages lectured in 2015-6. (It is already being referred to informally as "Son of ST&L and Automata & Formal Languages"). Because of the advent of that second course this Part III course no longer covers elementary computability in the way that its predecessor ("Computability and Logic") did, and this is reflected in the change in title. It will say less about Set Theory than one would expect from a course entitled 'Logic'; this is because in Lent term Benedikt Löwe will be lecturing a course entitled 'Topics in Set Theory' and I do not wish to tread on his toes. Material likely to be covered include: advanced topics in first-order logic (Natural Deduction, Sequent Calculus, Cut-elimination, Interpolation, Skolemisation, Completeness and Undecidability of First-Order Logic, Curry-Howard, Possible world semantics, Gödel's Negative Interpretation, Generalised quantifiers. . .); Advanced Computability (λ-representability of computable functions, Tennenbaum's theorem, Friedberg-Muchnik, Baker-Gill-Solovay. . .); Model theory background (ultraproducts, Los's theorem, elementary embeddings, omitting types, categoricity, saturation, Ehrenfeucht-Mostowski theorem. . .); Logical combinatorics (Paris-Harrington, WQO and BQO theory at least as far as Kruskal's theorem on wellquasiorderings of trees. . .). This is a new syllabus and may change in the coming months. It is entirely in order for students to contact the lecturer for updates.

Pre-requisites

The obvious prerequisites from last year's Part II are Professor Johnstone's Set Theory and Logic and Dr Chiodo's Automata and Formal Languages, and I would like to assume that everybody coming to my lectures is on top of all the material lectured in those courses. This aspiration is less unreasonable than it may sound, since in 2016-7 both these courses are being lectured the term before this one, in Michaelmas; indeed supervisions for Part III students attending them can be arranged if needed: contact me or your director of studies. I am lecturing Part II Set Theory and Logic and I am even going to be issuing a "Sheet 5" for Set Theory and Logic, of material likely to be of interest to people who are thinking of pursuing this material at Part III. Attending these two Part II courses in Michaelmas is a course of action that may appeal particularly to students from outside Cambridge.

Contents

1 Proof theory and constructive logic

1.1 Natural deduction

1.2 Curry–Howard correspondence

Solutions.

(i) $\lambda f.\lambda x.\langle \mathrm{fst}(f)(\mathrm{fst}(x)), \mathrm{snd}(f)(\mathrm{snd}(x))\rangle$

(ii) $\lambda f.\lambda g.\lambda a.g(fa)$

(iii) $\lambda f.\lambda g.g(fg)$

(iv) $\lambda f.\lambda b.\lambda a.(fa)b$

(v) $\lambda f.\lambda x.f(\mathrm{fst}\, x)(\mathrm{snd}\, x)$

(vi) $\lambda f.\lambda a.\lambda b.f\langle b, a\rangle$

One can write out the corresponding trees explicitly. For example, (iii) can be done by

$$\dfrac{\dfrac{\dfrac{\dfrac{g : [A \to B]^1 \qquad f : [(A \to B) \to A]^2}{fg : A}\,{\scriptstyle \to\text{-elim}} \qquad g : [A \to B]^1}{g(fg)}\,{\scriptstyle \to\text{-elim}}}{\lambda g.g(fg) : (A \to B) \to B}\,{\scriptstyle \to\text{-int (1)}}}{\lambda f.\lambda g.g(fg) : (A \to B) \to A \to (A \to B) \to B}\,{\scriptstyle \to\text{-int (2)}}$$

Note that we always decorate assumptions with a single variable, say f, even if they are very complicated. For example, if we have an assumption $A \wedge B$, it might be tempting to decorate it as $\langle a, b\rangle$, but we do not. □

Proposition. We cannot prove $((A \to B) \to A) \to A$ in natural deduction without the law of excluded middle.

Proof. Suppose there were a lambda term $P : ((A \to B) \to A) \to A$.

We pick

$$B = \{0, 1\}, \quad A = \{0, 1, 2, 3, 4\}.$$

In this setting, any function $f : A \to B$ identifies a distinguished member of B, namely the one that is hit by more members of A. We know $B \subseteq A$, so this is an element in A. So we have a function $F : (A \to B) \to A$. Then $P(F)$ is a member of A. We claim that in fact $P(F) \in B$.

Indeed, we write $P(F) = a \in A$. Let π be a 3-cycle moving everything in $A \setminus B$ and fixing B. Then this induces an action on functions among A and B by conjugation. We have.

$$\pi(P(F)) = \pi(a).$$

But since P is given by a λ term, it cannot distinguish between the different memebers of $A \setminus B$. So we have

$$P(\pi(F)) = \pi(a).$$

We now claim that $\pi(F) = F$. By construction, $\pi(F) = \pi^{-1} \circ F \circ \pi$. Then for all $f : A \to B$, we have

$$\begin{aligned}\pi(F)(f) = (\pi^{-1} \circ f \circ \pi)(f) = (\pi^{-1} \circ F)(\pi(f))\\ = \pi^{-1}(F(\pi(f))) = \pi^{-1}(F(f)) = F(f).\end{aligned}$$

Noting that π fixes f, the only equality that isn't obvious from unravelling the definitions is $F(\pi(f)) = F(f)$. Indeed, we have $\pi(f) = \pi^{-1} \circ f \circ \pi = f \circ \pi$. But $F(f \circ \pi) = F(f)$ because our explicit construction of F depends only on the image of f. So $\pi(F) = F$. So this implies $a = \pi(a)$, which means $a \in B$. So we always have $P(F) \in B$.

But this means we have found a way of uniformly picking a distinguished element out of a two-membered set. Indeed, given any such set B, we pick any three random objects, and combine it with B to obtain A. Then we just apply $P(F)$. This is clearly nonsense. □

1.3 Possible world semantics

Lemma. Any formula with a natural deduction proof not using the rule for classical negation is true in all possible world models.

Proof. The hard case is implication. Suppose we have a natural deduction proof of $A \to B$. The last rule is a $\to$-introduction. So by the induction hypothesis, every world that believes A also believes B. Now let w be a world that believes all the other undischarged assumptions in $A \to B$. By persistence, every $w' \geq w$ believes similarly. So any $w' \geq w$ that believes A also believes B. So $w \vDash A \to B$. □

1.4 Negative interpretation

Lemma. Any formula built up from negated and doubly negated atomics by $\neg$, $\wedge$ and $\forall$ is stable.

Proof. By induction on formulae. The base case is immediate, using the fact that $\neg\neg\neg A \to \neg A$. This follows from the more general fact that

$$(((p \to q) \to q) \to q) \to p \to q.$$

It is less confusing to prove this in two steps, and we will write λ-terms for our proofs. First note that if we have $f : A \to B$, then we can obtain $f^T : (B \to q) \to A \to q$ for any q, using

$$f^T = \lambda g_{B\to q}.\lambda a_A.g(f(a)).$$

So it suffices to prove that

$$p \to (p \to q) \to q,$$

and the corresponding term is

$$\lambda x_p.\lambda g_{p\to q}.gx$$

We now proceed by induction.

- Now assume that we have proofs of $\neg\neg p \to p$ and $\neg\neg q \to q$. We want to prove $p \wedge q$ from $\neg\neg(p \wedge q)$. It suffices to prove $\neg\neg p$ and $\neg\neg q$ form $\neg\neg(p \wedge q)$, and we will just do the first one by symmetry.

  We suppose $\neg p$. Then we know $\neg(p \wedge q)$. But we know $\neg\neg(p \wedge q)$. So we obtain a contradiction. So we have proved that $\neg\neg p$.

- Note that we have

  $$\vdash \exists_x \neg\neg\varphi(x) \to \neg\neg\exists_x \varphi(x),$$

  but not the other way round. For universal quantification, we have

  $$\neg\neg\forall_x \varphi(x) \to \forall_x \neg\neg\varphi(x),$$

  but not the other way round. We can construct a proof as follows:

  $$
  \begin{prooftree}
  \AxiomC{$[\forall_x \varphi(x)]^1$}
  \RightLabel{\scriptsize $\forall$-elim}
  \UnaryInfC{$\varphi(a)$}
  \AxiomC{$[\neg\varphi(x)]^2$}
  \RightLabel{\scriptsize $\to$-elim}
  \BinaryInfC{$\to$}
  \RightLabel{\scriptsize $\to$-int (1)}
  \UnaryInfC{$\neg\forall_x \varphi(x)$}
  \AxiomC{$[\neg\neg\forall_x \varphi(x)]^3$}
  \RightLabel{\scriptsize $\to$-elim}
  \BinaryInfC{$\bot$}
  \RightLabel{\scriptsize $\to$-int (2)}
  \UnaryInfC{$\neg\neg\varphi(a)$}
  \RightLabel{\scriptsize $\forall$-int}
  \UnaryInfC{$\neg\neg\forall_x \varphi(x)$}
  \RightLabel{\scriptsize $\to$-int (3)}
  \UnaryInfC{$\neg\neg\forall_x F(x) \to \forall_x \neg\neg F(x)$}
  \end{prooftree}
  $$

  We now want to show that if φ is stable, then $\forall_x \varphi(x)$ is stable. In other words, we want

  $$\neg\neg\forall_x \varphi^*(x) \to \forall_x \varphi^*(x).$$

  But form $\neg\neg\forall_x \varphi^*(x)$, we can deduce $\forall_x \neg\neg\varphi^*(x)$, which implies $\forall_x \varphi^*(x)$.

So every formula in the range of the negative interpretation is stable. Every stable formula is equivalent to its double negation (classically). Every formula is classically equivalent to a stable formula. □

1.5 Constructive mathematics

2 Model theory

2.1 Universal theories

Lemma. Let T be a consistent theory, and let $T_\forall$ be the set of all universal consequences of T, i.e. all things provable from T that are of the form ($*$). Let $\mathcal{M}$ be a model of $T_\forall$. Then $T \cup D(\mathcal{M})$ is also consistent.

Proof. Suppose $T \cup D(\mathcal{M})$ is not consistent. Then there is an inconsistency that can be derived from finitely many of the new axioms. Call this finite conjunction ψ. Then we have a proof of $\neg\psi$ from T. But T knows nothing about the constants we added to T. So we know $T \vdash \forall_{\mathbf{x}} \neg\psi$. This is a universal consequence of T that $\mathcal{M}$ does not satisfy, and this is a contradiction. □

Theorem. A theory T is universal if and only if every substructure of a model of T is a model of T.

Proof. $\Rightarrow$ is easy. For $\Rightarrow$, suppose T is a theory such that every substructure of a model of T is still a model of T.

Let $\mathcal{M}$ be an arbitrary model of $T_\forall$. Then $T \cup D(\mathcal{M})$ is consistent. So it must have a model, say $\mathcal{M}^*$, and this is in particular a model of T. Moreover, $\mathcal{M}$ is a submodel of $\mathcal{M}^*$. So $\mathcal{M}$ is a model of T.

So any model of $T_\forall$ is also a model of T, and the converse is clearly true. So we know $T_\forall$ is equivalent to T. □

2.2 Products

Proposition. Products preserve (universal) Horn formulae.

Proof. Suppose every factor

$$A_i \vDash \forall_{\mathbf{x}} \bigwedge \varphi_i(\mathbf{x}) \to \chi(\mathbf{x}).$$

We want to show that the product believes in the same statement. So let $(f_1, \cdots, f_k)$ be a tuple in the product of the right length satisfying the antecedent, i.e. for each $n \in I$, we have

$$A_n \vDash \varphi_i(f_1(n), \cdots, f_k(n))$$

for each i, But then by assumption,

$$A_n \vDash \chi(f_1(n), \cdots, f_k(n))$$

for all n. So the product also believes in $\varphi_j(f_1, \cdots, f_n)$. So we are done. □

Theorem (Łoś theorem)**.** Let $\{A_i : i \in I\}$ be a family of structures of the same (first-order) signature, and $\mathcal{U} \subseteq P(I)$ an ultrafilter. Then

$$\prod_{i \in I} A_i/\mathcal{U} \vDash \varphi \Longleftrightarrow \{i : A_i \vDash \varphi\} \in \mathcal{U}.$$

In particular, if A_i are all models of some theory, then so is $\prod A_i/\mathcal{U}$.

Lemma. Let F be a filter on I. Then the following are equivalent:

(i) F is an ultrafilter.

(ii) For $X \subseteq I$, either $X \in F$ or $I \setminus X \in F$ ("F is prime").

(iii) If $X, Y \subseteq I$ and $X \cup Y \in I$, then $X \in I$ or $Y \in I$.

Theorem (Compactness theorem)**.** Let T be a theory in first order logic such that every finite subset has a model. Then T has a model.

Proof. Let Δ be such a theory. Let $S = \mathcal{P}_{\aleph_0}(\Delta)$ be the set of all finite subsets of Δ. For each $s \in S$, we pick a model $\mathcal{M}_s$ of s.

Given $s \in S$, we define

$$X_s = \{t \in S : s \subseteq t\}.$$

We notice that $\{X_s : s \in S\}$ generate a proper filter on S. We extend this to ultrafilter $\mathcal{U}$ by Zorn's lemma. Then we claim that

$$\prod_{s \in S} \mathcal{M}_s / \mathcal{U} \vDash \Delta.$$

Indeed, for any $\varphi \in \Delta$, we have

$$\{s : \mathcal{M}_s \vDash \varphi\} \supseteq X_{\{\varphi\}} \in \mathcal{U}.$$ □

2.3 Ehrenfeucht–Mostowski theorem

Proposition. Monadic first-order logic is decidable.

Proof. Consider any formula φ. Suppose it involves the one-place predicates $p_1, \ldots, p_n$. Given any structure $\mathcal{M}$, we consider the quotient of $\mathcal{M}$ by

$$x \sim y \Leftrightarrow p_i(x) = p_i(y) \text{ for all i}.$$

Then there are at most 2^n things in the quotient.

Then given any transversal of the quotient, we only have to check if the formula holds for this transversal, and this is finite. So we can decide. □

Theorem (Ehrenfeucht–Mostowski theorem (1956))**.** Let $\langle I, \leq \rangle$ be a total order, and let T be a theory with infinite models. Suppose we have a unary predicate P and a 2-ary relation $\preccurlyeq \in \mathcal{L}(T)$ such that

$$T \vdash \preccurlyeq \text{ is a total order on } \{x : P(x)\}.$$

Then T has a model $\mathcal{M}$ with a copy of I as a sub-order of $\preccurlyeq$, and the copy of I is a set of indiscernibles. Moreover, we can pick $\mathcal{M}$ such that every order-automorphism of $\langle I, \leq \rangle$ extends to an automorphism of $\mathcal{M}$.

Proof. Let T and $\langle I, \leq \rangle$ be as in the statement of the theorem. We add to $\mathcal{L}(T)$ names for every element of I, say $\{c_i : i \in I\}$. We add axioms that says $P(c_i)$ and $c_i \preccurlyeq c_j$ whenever $i < j$. We will thereby confuse the orders $\leq$ and $\preccurlyeq$, partly because $\leq$ is much easier to type. We call this theory T^*.

Now we add to T^* new axioms to say that the c_i form a set of indiscernibles. So we are adding axioms like

$$\varphi(c_i, c_j) \Leftrightarrow \varphi(c_{i'}, c_{j'}) \qquad (*)$$

for all $i < j$ and $i' < j'$. We do this simultaneously for all $\varphi \in \mathcal{L}(T)$ and all tuples of the appropriate length. We call this theory T^I, and it will say that $\langle I, \leq \rangle$ forms a set of indiscernibles. The next stage is, of course, to prove that T^I is consistent.

Consider any finite fragment T' of T^I. We want to show that T' is consistent. By finiteness, T' only mentions finitely many constants, say $c_1 < \cdots < c_K$, and only involve finitely many axioms of the form $(*)$. Denote those predicates as $\varphi_1, \cdots, \varphi_n$. We let N be the supremum of the arities of the φ_i.

Pick an infinite model $\mathcal{M}$ of T. We write

$$\mathcal{M}^{[N]} = \{A \subseteq \mathcal{M} : |A| = N\},$$

For each φ_i, we partition $\mathcal{M}^{[N]}$ as follows — given any collection $\{a_k\}_{k=1}^N$, we use the order relation $\preccurlyeq$ to order them, so we suppose $a_k \preccurlyeq a_{k+1}$. If φ_i has arity $m \leq N$, then we can check whether $\varphi_i(a_1, \cdots, a_m)$ holds, and the truth value gives us a partition of $\mathcal{M}^{[N]}$ into 2 bits.

If we do this for all φ_i, then we have finitely partitioned $\mathcal{M}^{[N]}$. By Ramsey's theorem, this has an infinite monochromatic subset, i.e. a subset such that any two collection of N members fall in the same partition. We pick elements $c_1, \cdots, c_K, \cdots, c_{K+N}$, in increasing order (under $\preccurlyeq$). We claim that picking the $c_1, \cdots, c_K$ to be our constants satisfy the axioms of T'.

Indeed, given any φ_i mentioned in T' with arity $m < N$, and sequences $c_{\ell_1} < \cdots < c_{\ell_m}$ and $c_{\ell'_1} < \cdots < c_{\ell'_m}$, we can extend these sequences on the right by adding more of those c_i. Then by our choice of the colouring, we know

$$\varphi_i(c_{\ell_1}, \cdots, c_{\ell_m}) \Leftrightarrow \varphi_i(c_{\ell'_1}, \cdots, _{\ell'_m}).$$

So we know T' is consistent. So T^I is consistent. So we can just take a model of T^I, and the Skolem hull of the indiscernibles is the model desired. □

2.4 The omitting type theorem

Theorem (Omitting type theorem)**.** Let T be a first-order theory, and Σ an n-type. If

$$T \vdash \forall_x \neg\varphi(x)$$

whenever φ locally realizes Σ, then T has a model omitting Σ.

Theorem. Let T be a propositional theory, and $\Sigma \subseteq \mathcal{L}(T)$ a type (with $n = 0$). If T locally omits Σ, then there is a T-valuation that omits Σ.

Proof. Suppose there is no T-valuation omitting Σ. By the completeness theorem, we know everything in Σ is a theorem of T. So T can't locally omit Σ. □

Theorem. Let T be a propositional theory, and for each $i \in \mathbb{N}$, we let $\Sigma_i \subseteq \mathcal{L}(T)$ be types for each $i \in \mathbb{N}$. If T locally omits each Σ_i, then there is a T-valuation omitting all Σ_i.

Proof. We will show that whenever $T \cup \{\neg A_1, \cdots, \neg A_i\}$ is consistent, where $A_n \in \Sigma_n$ for $n \leq i$, then we can find $A_{n+1} \in \Sigma_{n+1}$ such that

$$T \cup \{\neg A_1, \cdots, \neg A_n, \neg A_{n+1}\}$$

is consistent.

Suppose we can't do this. Then we know that

$$T \vdash \left(\bigwedge_{1 \leq j \leq n} \neg A_j \right) \to A_{n+1},$$

for every $A_{n+1} \in \Sigma_{n+1}$. But by assumption, T locally omits Σ_{i+1}. This implies

$$T \vdash \neg \left(\bigwedge_{1 \leq j \leq n} \neg A_j \right),$$

contradicting the inductive hypothesis that $T \cup \{\neg A_1, \cdots, \neg A_i\}$ is consistent.

Thus by compactness, we know $T \cup \{\neg A_1, \neg A_2, \cdots\}$ is consistent, and a model of this would give us a model of T omitting all those types. □

Proof. Let T be a first order theory (in a countable language) locally omitting Σ. For simplicity, we suppose Σ is a 1-type. We want to find a model omitting Σ. Suppose T locally omits Σ, and let $\{c_i : i \in \mathbb{N}\}$ be a countable set of new constant symbols. Let $\langle \varphi_i : i \in \mathbb{N} \rangle$ be an enumeration of the sentences of $\mathcal{L}(T)$. We will construct an increasing sequence $\{T_i : i \in \mathbb{N}\}$ of finite extensions of T such that for each $m \in \mathbb{N}$,

(0) T_{m+1} is consistent.

(i) T_{m+1} decides φ_n for $n \leq m$, i.e. $T_{m+1} \vdash \varphi_n$ or $T_{m+1} \vdash \neg\varphi_n$.

(ii) If φ_m is $\exists_x \psi(x)$ and $\varphi_m \in T_{m+1}$, then $\psi(c_p) \in T_{m+1}$, where c_p is the first constant not occurring in T_m or φ_m.

(iii) There is a formula $\sigma(x) \in \Sigma$ such that $\neg\sigma(c_m) \in T_{m+1}$.

We will construct this sequence by recursion. Given T_m, we construct T_{m+1} as follows: think of T_m as $T \cup \{\theta_1, \cdots, \theta_r\}$, and let

$$\Theta = \bigwedge_{j \leq r} \theta_j.$$

We let $\{c_1, \cdots, c_N\}$ be the constants that have appeared in Θ, and let

$$\Theta(\mathbf{x})$$

be the result of replacing c_i with x_i in θ. Then clearly, $\Theta(\mathbf{x})$ is consistent with T. Since T locally omits Σ, we know there exists some $\sigma(x) \in \Sigma$ such that

$$\Theta \wedge \neg\sigma(x_m)$$

is consistent with T. We put $\neg\sigma(c_m)$ into T_{m+1}, and this takes care of (iii).

If φ_m is consistent with $T_m \cup \{\neg\sigma(c_m)\}$, then put it into T_{m+1}. Otherwise, put in $\neg\varphi_m$. This takes care of (i).

If φ_m is $\exists_x \psi(x)$ and it's consistent with $T_m \cup \{\neg\sigma(c_m)\}$, we put $\psi(c_m)$ into T_{m+1}. This takes care of (ii).

Now consider

$$T^* = \bigcup_{n \in \mathbb{N}} T_n$$

Then T^* is complete by construction, and is complete by compactness.

Consider an arbitrary countable model of T^*, and the submodel generated by the constants in C. This is a model of $T^* \supseteq T$ and condition (iii) ensures that it omits Σ. □

3 Computability theory

3.1 Computability

Proposition. There exists primitive recursion functions $\mathsf{pair} : \mathbb{N}^2 \to \mathbb{N}$ and $\mathsf{unpair} : \mathbb{N} \to \mathbb{N}^2$ such that

$$\mathsf{unpair}(\mathsf{pair}(x, y)) = (x, y)$$

for all $x, y \in \mathbb{N}$.

Proof. We can define the pairing function by

$$\mathsf{pair}(x, y) = \binom{x + y + 1}{2} + y.$$

The unpairing function can be shown to be primitive recursive, but is more messy. □

Corollary. There exists $\mathsf{cons} : \mathbb{N} \to \mathbb{N}, \mathsf{head} : \mathbb{N} \to \mathbb{N}$ and $\mathsf{tail} : \mathbb{N} \to \mathbb{N}$ such that

$$\mathsf{cons}(\mathsf{head}\ x, \mathsf{tail}\ x) = x$$

Proof. Take $\mathsf{cons} = \mathsf{pair}$; head to be the first projection of the unpairing and tail to be a second projection. □

Proposition. The Ackermann function is well-defined.

Proof. To see this, note that computing $A(m + 1, n + 1)$ requires knowledge of the values of $A(m + 1, n)$, and $A(m, A(m + 1, n))$.

Consider $\mathbb{N} \times \mathbb{N}$ ordered lexicographically. Then computing $A(m + 1, n + 1)$ requires knowledge of the values of A at pairs lying below $\langle m + 1, n + 1\rangle$ in this order. Since the lexicographic order of $\mathbb{N} \times \mathbb{N}$ is well-ordered (it has order type $\omega \times \omega$), by transfinite induction, we know A is well-defined. □

Theorem. The function $n \mapsto A(n, n)$ dominates all primitive recursive functions.

3.2 Decidable and semi-decidable sets

Proposition. A set $X \subseteq \mathbb{N}^k$ is semi-decidable iff it is a projection of a decidable subset of $\mathbb{N}^{k+1}$.

Proof. ($\Leftarrow$) Let $Y \subseteq \mathbb{N}^{k+1}$ be such that $\mathsf{proj}_k Y = X$, where proj_k here denotes the projection to the first k factors. Since Y is decidable, there is a computable function $f : \mathbb{N} \to \mathbb{N}^{k+1}$ such that $\operatorname{im} f = Y$. Then $\operatorname{im}(\mathsf{proj}_k \circ f) = X$. So X is the image of a computable function.

($\Rightarrow$) Suppose X is semi-decidable. So $X = \operatorname{dom}(\{m\})$ for some $m \in \mathbb{N}$, i.e. $X = \{n : \{m\}(n)\downarrow\}$. Then we can pick

$$Y = \{(\mathbf{x}, t) \mid \{m\}(\mathbf{x}) \text{ halts in } t \text{ steps}\}.$$ □

Theorem (Turing)**.** The halting set is semi-decidable but not decidable.

Proof. Suppose not, and $\mathcal{M}$ is a machine with two inputs such that for all p, i, we have

$$\mathcal{M}(p, i) = \begin{cases} \text{yes} & \{p\}(i) \downarrow \\ \text{no} & \{p\}(i) \uparrow \end{cases}.$$

If there were such a machine, then we could do some "wrapping" — if the output is "yes", we intercept this, and pretend we are still running. If the output is "no", then we halt. Call this $\mathcal{M}'$. From this, we construct $\mathcal{M}''(n) = \mathcal{M}'(n, n)$. Suppose this machine is coded by m.

Now does $\{m\}(m)$ halt? Suppose it does. Then $\mathcal{M}(m, m) = \text{yes}$, and hence $\mathcal{M}'(m, m)$ does not halt. This means $m(m)$ doesn't halt, which is a contradiction.

Conversely, if $m(m)$ does not halt, then $\mathcal{M}'(m, m)$ says no. Thus, $m(m)$ halts. This is again a contradiction!

So $\mathcal{M}$ cannot exist. □

Theorem (*smn* theorem)**.** There is a total computable function s of two variables such that for all e, we have

$$\{e\}(b, a) = \{s(e, b)\}(a).$$

Similarly, we can find such an s for any tuples $\mathbf{b}$ and $\mathbf{a}$.

Proof. We can certainly write a program that does this. □

Theorem (Fixed point theorem)**.** Let $h : \mathbb{N} \to \mathbb{N}$ be total computable. Then there is an $n \in \mathbb{N}$ such that $\{n\} = \{h(n)\}$ (as functions).

Proof. Consider the map

$$\langle e, x\rangle \mapsto \{h(s(e, e))\}(x).$$

This is clearly computable, and is computed by a machine numbered a, say. We then pick $n = s(a, a)$. Then we have

$$\{n\}(x) = \{s(a, a)\}(x) = \{a\}(a, x) = \{h(s(a, a))\}(x) = \{h(n)\}(x).$$ □

Theorem (Rice's theorem)**.** Let A be a non-empty proper subset of the set of all computable functions $\mathbb{N} \to \mathbb{N}$. Then $\{n : \{n\} \in A\}$ is not decidable.

Proof. We fix an A. Suppose not. We let χ be the (total) characteristic function of $\{n : \{n\} \in A\}$. By assumption, χ is computable. We find naturals a, b such that $\{a\} \in A$ and $\{b\} \not\in A$. Then by the hypothesis, the following is computable:

$$g(n) = \begin{cases} b & \{n\} \in A \\ a & \text{otherwise} \end{cases}.$$

The key point is that this is the wrong way round. We return something in A if the graph of $\{n\}$ is *not* in A. Now by the fixed point theorem, there is some $n \in \mathbb{N}$ such that

$$\{n\} = \{g(n)\}.$$

We now ask ourselves — do we have $\{n\} \in A$? If so, then we also have $\{g(n)\} \in A$. But these separately imply $g(n) = b$ and $g(g(n)) = b$ respectively. This implies $g(b) = b$, which is not possible.

Similarly, if $\{n\} \not\in A$, then $\{g(n)\} \not\in A$. These again separately imply $g(n) = a$ and $g(g(n)) = a$. So we find $g(a) = a$, which is again a contradiction. □

Corollary. It is impossible to grade programming homework.

3.3 Computability elsewhere

3.4 Logic

Theorem (Craig's theorem)**.** Every first-order theory with a semi-decidable set of axioms has a decidable set of axioms.

Proof. By assumption, there is a total computable function f such that the axioms of the theory are exactly $\{f(n) : n \in \mathbb{N}\}$. We write the nth axiom as φ_n.

The idea is to give an alternative axiom that says the same thing as φ_n, but from the form of the new axiom itself, we can deduce the value of n, and so we can compute $f(n)$ to see if they agree. There are many possible ways to do this. For example, we can say that we add n many useless brackets around φ_n and take it as the new axiom.

Alternatively, without silly bracketing, we can take the nth axiom to be

$$\phi_n = \left(\bigwedge_{i<n} \varphi_i\right) \to \varphi_n.$$

Then given any statement ψ, we can just keep computing $f(1), f(2), \cdots$, and then if $\psi = \phi_n$, then we will figure in finite time. Otherwise, we will, in finite time, see that ψ doesn't look like $f(1) \wedge f(2) \wedge \cdots$, and thus deduce it is not an axiom. □

Theorem (Tennenbaum's theorem)**.** For any countable non-standard model of true arithmetic, the graph of $+$ and $\times$ cannot be decidable.

Theorem. The set of Gödel numbers of machines that compute total functions is not semi-decidable.

Proof. Suppose it were. Then there is a computable total function $f : \mathbb{N} \to \mathbb{N}$ such that every computable total function is $\{f(n)\}$ for some n. Now consider the function

$$g(n) = \{f(n)\}(n) + 1.$$

This is a total computable function! But it is not $\{f(n)\}$ for any n, because it differs from $\{f(n)\}$ at n. □

Theorem (Gödel's incompleteness theorem)**.** Let T be a recursively axiomatized theory of arithmetic, i.e. the set of axioms is semi-decidable (hence decidable). Suppose T is sufficiently strong to talk about computability of functions (e.g. Peano arithmetic is). Then there is some proposition true in $\mathbb{N}$ that cannot be proven in T.

Proof. We know the set of theorems of T is semi-decidable. So $\{n : T \vdash \{n\} \text{ is a total function}\}$ is semi-decidable. So there must be some total function such that T does not prove it is total. In other words, T is not complete! □

Theorem (Ramsey's theorem)**.** We write $\mathbb{N}^{(k)}$ for the set of all subsets of $\mathbb{N}$ of size k. Suppose we partition $\mathbb{N}^{(k)}$ in m many distinct pieces. Then there exists some infinite $X \subseteq \mathbb{N}$ such that X is monochromatic, i.e. $X^{(k)} \subseteq \mathbb{N}^{(k)}$ lie entirely within a partition.

Theorem (Jockusch)**.** There exists a decidable partition of $\mathbb{N}^{(3)}$ into two pieces with no infinite decidable monochromatic set.

Proof. We define a partition $\rho : \mathbb{N}^{(3)} \to \{0, 1\}$ as follows. Given $x < y < z$, we define $\rho(\{x, y, z\})$ to be 0 if for any $p, d < x$, we have "$\{p\}(d)$ halts in y steps iff $\{p\}(d)$ halts in z steps", and 1 otherwise. This is a rather weird colouring, but let's see what it gives us.

We first note that there can be no monochromatic set coloured 1, as given any x, for sufficiently large y and z, we must have $\{p\}(d)$ halts in y steps iff $\{p\}(d)$ halts in z steps.

We claim that an infinite decidable monochromatic set A for 0 will solve the halting problem. Indeed, if we want to know if $\{p\}$ halts on d, then we pick some $x \in A$ such that $p, d < x$. Then pick some $y \in A$ such that $y > x$. Then by construction of ρ, if $\{p\}(d)$ halts at all, then it must halt in x steps, and we can just check this.

Thus, there cannot be an infinite decidable monochromatic set for this partition. □

3.5 Computability by λ-calculus

Theorem. Every λ expression can be reduced to at most one β-normal form. Moreover, there exists a reduction strategy such that whenever a λ expression can be reduced to a β-normal form, then it will be reduced to it via this reduction strategy.

This magic reduction strategy is just to always perform β-reduction on the leftmost thing possible.

Theorem. For any g, we have

$$\mathsf{Y}\ g \rightsquigarrow g\ (\mathsf{Y}\ g).$$

Proof.

$$\begin{aligned}
\mathsf{Y}\ g &\rightsquigarrow \lambda f.\Big[(\lambda x.f(x\ x))(\lambda x.f(x\ x))\Big]\ g\\
&\rightsquigarrow (\lambda x.(g(x\ x)))(\lambda x.g(x\ x))\\
&\rightsquigarrow g\Big((\lambda x.(g(x\ x)))(\lambda x.g(x\ x))\Big)
\end{aligned}$$

□

3.6 Reducibility

Proposition. Let $A \subseteq \mathbb{N}$. Then $A \leq_m \mathbb{K}$ iff A is semi-decidable.

Proposition. $(\mathbb{N} \setminus \mathbb{K}) \leq_M A$ iff A is productive.

Theorem (Friedberg–Muchnik)**.** There exists two $A, B \subseteq \mathbb{N}$ such that $A \not\leq B \not\leq A$. Moreover, A and B are both semi-decidable.

Proof. We will obtain the sets A and B as

$$A = \bigcup_{n<\omega} A_n, \quad B = \bigcup_{n<\omega} B_n,$$

where A_n and B_n are finite (and in particular decidable) and nested, i.e. $i < j$ implies $A_i \subseteq A_j$ and $B_i \subseteq B_j$.

We introduce a bit of notation. As mentioned, if we allow our programs to access the oracle B, then our "programming language" will allow consultation of B. Then in this new language, we can again assign Gödel numbers to programs, and we write $\{e\}^B$ for the program whose Gödel number is e. Instead of inventing a new language for each B, we invent a language that allows calling an "oracle", without specifying what it is. We can then plug in different sets and run.

Our objective is to pick A, B such that

$$\chi_A \neq \{e\}^B$$
$$\chi_B \neq \{e\}^A$$

for all e. Here we are taking χ_A to be the total version, i.e.

$$\chi_A(x) = \begin{cases} 1 & x \in A \\ 0 & x \notin A \end{cases}.$$

The idea is, of course, to choose A_m such that it prevents χ_A from being $\{m\}^B$, and vice versa. But this is tricky, because when we try to pick A_m, we don't know the whole of B yet.

It helps to spell out more explicitly what we want to achieve. We want to find some $n_i, m_i \in \mathbb{N}$ such that for each i, we have

$$\chi_A(n^{(i)}) \neq \{i\}^B(n^{(i)})$$
$$\chi_B(m^{(i)}) \neq \{i\}^A(m^{(i)})$$

These n_i and m_i are the *witness* to the functions being not equal.

We now begin by producing infinite lists

$$N_i = \{n_1^{(i)}, n_2^{(i)}, \cdots\}$$
$$M_i = \{m_1^{(i)}, m_2^{(i)}, \cdots\}$$

of "candidate witnesses". We will assume all of these are disjoint. For reasons that will become clear later, we assign some "priorities" to these sets, say

$$N_1 > M_1 > N_2 > M_2 > N_3 > N_3 > \cdots.$$

We begin by picking

$$A_0 = B_0 = \emptyset.$$

Suppose at the tth iteration of the process, we have managed to produce A_{t-1} and B_{t-1}. We now look at $N_1, \ldots, N_t$ and $M_1, \cdots, M_t$. If they have managed to found a witness, then we leave them alone. Otherwise, suppose N_i hasn't found a witness yet. Then we run $\{i\}^{B_{t-1}}(n_1^{(i)})$ for t many time steps. We consider the various possibilities:

- Let n be the first remaining element of N_i. If $\{i\}^{B_{t-1}}(n)$ halts within t steps and returns 0, then we put n into A_t, and then pick this as the desired witness. We now look at all members of B_{t-1} our computation of $\{i\}^{B_{t-1}}$ has queried. We *remove* all of these from all sets of lower priority than N_i.

– Otherwise, do nothing, and move on with life.

Now the problem, of course, is that whenever we add things into A_t or B_t, it might have changed the results of some previous computations. Suppose we originally found that $\{10\}^{B_4}(32) = 0$, and therefore put 32 into A_5 as a witness. But later, we found that $\{3\}^{A_{23}}(70) = 0$, and so we put 70 into B_{24}. But if the computation of $\{10\}^{B_4}(32)$ relied on the fact that $70 \notin B_4$, then we might have

$$\{10\}^{B_{24}}(32) \neq 0,$$

and now our witness is "injured". When this happens, we forget the fact that we picked 32 as a witness, and then pretend N_{10} hasn't managed to find a witness after all.

Fortunately, this can only happen because M_3 is of higher priority than N_{10}, and thus 70 was not forbidden from being a witness of M_3. Since there are only finitely many things of higher priorities, our witness can be injured only finitely many times, and we will eventually be stabilized.

We are almost done. After all this process, we take the union and get A and B. If, say, $\{i\}^A$ has a witness, then we are happy. What if it does not? Suppose $\{i\}^A$ is some characteristic function, and m is the first element in the list of witnesses. Then since the lists of candidate witnesses are disjoint, we know $m \notin B$. So it suffices to show that $\{i\}^A(m) \neq 0$. But if $\{i\}^A(m) = 0$, then since this computation only involves finitely many values of A, eventually, the membership of these things in A would have stabilized. So we would have $\{i\}^A(m) = 0$ long ago, and made m a witness.

□

4 Well-quasi-orderings

Axiom (Axiom of dependent choice)**.** Let X be a set an R a relation on X. The *axiom of dependent choice* says if for all $x \in X$, there exists $y \in X$ such that $R(x, y)$, then we can find a sequence $x_1, x_2, \cdots$ such that $R(x_i, x_{i+1})$ for all $i \in \mathbb{N}$.

Lemma. If $\langle X, \leq_X \rangle$ is a well-founded quasi-order, then so is $X^{<\omega}$ and Trees(X).

Proposition. Let $\langle X, \leq$ be a quasi-order. Then the following are equivalent:

(i) $\langle X, \leq \rangle$ is a well-quasi-order.

(ii) There is no infinite decreasing sequence and no infinite anti-chain.

(iii) Whenever we have any sequence $x_i \in X$ whatsoever, we can find $i < j$ such that $x_i \leq x_j$.

Proof.

- (i) $\Rightarrow$ (ii): We just showed this.
- (iii) $\Rightarrow$ (i): Suppose $X_1, X_2, X_3, \cdots$ is a strictly decreasing chain in $\mathcal{P}(X)$. Then by definition, we can pick $x_i \in X_i$ such that x_i is not $\leq$ anything in X_{i+1}. Now for any $j > i$, we know $x_i \not\leq x_j$, because x_j is $\leq$ something in X_{i+1}. So we have found a sequence $\{x_i\}$ such that $x_i \not\leq x_j$ for all $i < j$.
- (iii) $\Rightarrow$ (ii) is clear.
- (ii) $\Rightarrow$ (iii), we show that whenever x_i is a sequence without $i < j$ such that $x_i \leq x_j$, then it either contains an infinite anti-chain, or an infinite descending chain.

  To do so, we two-colour [$\mathbb{N}$] by

  $$X(\{i < j\}) = \begin{cases} 0 & x_i > x_j \\ 1 & \text{otherwise} \end{cases}$$

  By Ramsey's theorem, this has an infinite monochromatic set. If we have an infinite monochromatic set of colour 0, then this is a descending chain. Otherwise, if it is of colour 1, then together with our hypothesis, we know $\{x_i\}$ is an anti-chain. □

Lemma. Let $\langle X, \leq \rangle$ be a well-founded quasi-order that is not a WQO. Then it has a minimal bad sequence.

Proof. Just pick each x_i according to the requirement in the definition. Such an x_i can always be found because $\langle X, \leq \rangle$ is well-founded. □

Lemma (Minimal bad sequence lemma)**.** Let $\langle X, \leq \rangle$ be a quasi-order and $B = \{b_i\}$ a minimal bad sequence. Let

$$X' = \{x \in X : \exists_{n \in \mathbb{N}} x < b_n\}.$$

Then $\langle X', \leq \rangle$ is a WQO.

Proof. Suppose $\{s_i\}$ is a bad sequence in X'. We prove by induction that nothing in $\{s_i\}$ is below b_n, which gives a contradiction.

Suppose $s_i < b_0$ for some i. Then $s_i, s_{i+1}, s_{i+2}, \cdots$ is a bad sequence, whose first element is less than b_0. This then contradicts the minimality of B.

For the induction step, suppose nothing in S is strictly less than $b_0, \cdots, b_n$. Suppose, for contradiction, that $s_i < b_{n+1}$. Now consider the sequence

$$b_0, \cdots, b_n, s_i, s_{i+1}, s_{i+2}, \cdots.$$

By minimality of B, we know this cannot be a bad sequence. This implies there is some n, m such that the nth element of the sequence is less than the mth element. But they can't be both from the $\{b_k\}$ or both from then $\{s_k\}$. This implies there is some $b_j \leq s_k$ with $j \leq n$ and $k \geq i+1$.

Consider s_k. Since $s_k \in X'$, it must be $\leq b_m$ for some m. Moreover, by induction hypothesis, we must have $m > n$. Then by transitivity, we have $b_j \leq b_m$, contradicting the fact that B is bad. □

Lemma (Perfect subsequence lemma)**.** Let $\langle X, \leq\rangle$ be a WQO. Then every sequence $\{x_n\}$ in X has a *perfect subsequence*, i.e. an infinite subset $A \subseteq \mathbb{N}$ such that for all $i < j \in A$, we have $f(i) \leq f(j)$.

Proof. We apply Ramsey's theorem. We two-colour $[\mathbb{N}]^2$ by

$$c(i<j) = \begin{cases} \text{red} & f(i) \leq f(j) \\ \text{blue} & f(i) \not\leq f(j) \end{cases}$$

Then Ramsey's theorem gives us an infinite monochromatic set. But we cannot have an infinite monochromatic blue set, as this will give a bad sequence. So there is a monochromatic red set, which is a perfect subsequence. □

Lemma (Higman's lemma)**.** Let $\langle X, \leq_X\rangle$ be a WQO. Then $\langle X^{<\omega}, \leq_s\rangle$ is a WQO.

Proof. We already know that $X^{<\omega}$ is well-founded. Suppose it is not a WQO. Then there is a minimal bad sequence $\{x_i\}$ of X-lists under $\leq_s$.

Now consider the sequence $\{\mathsf{head}(x_i)\}$. By the perfect subsequence lemma, after removing some elements in the sequence, we may wlog this is a perfect sequence.

Now consider the sequence $\{\mathsf{tail}(x_i)\}$. Now note that $\mathsf{tail}(x_i) < x_i$ for each i (here it is crucial that lists are finite). Thus, using the notation in the minimal bad sequence lemma, we know $\mathsf{tail}(x_i) \in X'$ for all i.

But X' is a well quasi-order. So we can find some $i < j$ such that $\mathsf{tail}(x_i) \leq \mathsf{tail}(x_j)$. But also $\mathsf{head}(x_i) \leq \mathsf{head}(x_j)$ by assumption. So $x_i \leq x_j$, and this is a contradiction. □

Theorem (Kruskal's theorem)**.** Let $\langle X, \leq_X\rangle$ be a WQO. Then $\langle \text{Trees}(X), \leq_s\rangle$ is a WQO.

Proof. We already know that Trees(X) is well-founded. Suppose it is not a WQO. Then we can pick a minimal bad sequence $\{x_i\}$ of trees.

As before, we may wlog $\{\text{root}(x_i)\}$ is a perfect sequence. Consider

$$Y = \{T : T \in \text{children}(x_i) \text{ for some } i\}.$$

Then $Y \subseteq X'$. So Y is a WQO, and hence by Higman's lemma, $Y^{<\omega}$ is a WQO. So there exists some i, j such that $\text{children}(x_i) \leq \text{children}(x_j)$. But by perfectness, we have $\text{root}(x_i) \leq \text{root}(x_j)$. So by definition of the ordering, $x_i \leq x_j$. □

Proposition (Friedman's finite form)**.** For all $k \in \mathbb{N}$, the statement $P(k)$ is true.