Class: T-Th 1-2:30 2-139
Tutorial: F 3:00 2-132
MCG 31

18.511 - Introduction to Mathematical Logic and Recursion Theory

9/12/89

Prof. Gerald Sacks 2-274
x3-4391
available Tu, Th afternoons
3-5 Tu: at logic seminar

Next meeting: Thursday 9/14 @ 1:00-2:30 4-145
18.511 will be combined with 18.515

Course content

Propositional Calculus
First Order Logic
- First order language
- formal systems
- provability
- structures (or models)
- truth (in a structure)
- Gödel's completeness theorem - makes connection between truth and provability

related material:
- compactness theorem
- applications to algebra

Recursion Theory
- definition of recursive function (recursive function is the same as a computable fn.)
- ⋮
- Gödel's incompleteness theorem - an application of recursive functions
- Gödel's second incompleteness theorem
- Church's theorem
- pure recursion theory; recursively enumerable sets

Set Theory - ordinals and cardinals

There will be no examination; instead will be graded on homework.

Recommended books:

Enderton, Mendelsohn } easier

Shoenfield – harder to read
– good collection of problems
– "marvel of terseness"
– very few backward refs.; assumes at any point you know everything presented before

---

9/14/89

18.515 and 18.511 will meet in the same room; 18.515 will have harder problems

Propositional Calculus (PC)

→ example of formal system

Formal Language

The atomic symbols (called "tokens" by computer people) of PC are:

(	left parenthesis	
)	right parenthesis	
$\wedge$	conjunction	propositional connectives
$\vee$	disjunction	
$\rightarrow$	implication	
$\leftrightarrow$	equivalence	
$\neg$	negation	

$A_0, A_1, A_2, \ldots$ (infinite list) propositional letters (or sometimes, propositional atoms)

There is an important distinction between

syntax	&	semantics
(grammar, punctuation, ...)		(meaning ...)
↑		↑
provability	⟺	truth

Well-formed formula (WFF) for PC
- Recursive definition (rules of generation)

Recursion (for us) is a method of definition

Induction is a method of proof

Recursive definition of WFF:

1) (A_i) is a WFF (for each prop. letter A_i)

2) if $\mathcal{F}$ and $\mathcal{G}$ are WFF's (note script letters), $(\mathcal{F} \wedge \mathcal{G})$, $(\mathcal{F} \vee \mathcal{G})$, $(\mathcal{F} \to \mathcal{G})$, $(\mathcal{F} \leftrightarrow \mathcal{G})$, and $(\neg \mathcal{F})$ are WFF's

(sometimes there is a 3rd clause, "rule of exclusion", that specifies that no others are WFF's -- the professor chooses not to have this clause)

e.g.: (A_1)
(A_2)
$((\neg(A_1)) \wedge (A_2))$

Homework problem #1
Claim: There exists an effective method for deciding whether or not an expression is a WFF. (Describe, in words, the algorithm.)

Due Sept. 21 In general, H.W. is due 1 wk. after given

We need axioms and rules in order to make explicit the notion of proof in PC. Let's defer this bit of syntax at the moment.

Semantics

truth function (or Boolean function)

truth values: T, F (sometimes ⊥ instead of F)

A truth function is simply any function whose arguments and value belong to {T, F}

i.e., that $f(x_1, \ldots, x_m)$ is a truth function means each $x_i \in \{T, F\}$ and each value of $f \in \{T, F\}$.

x_1	x_2	x_3	...	x_m	$f(x_1, \ldots, x_m)$
T	T	T		T	
F	T	T		⋮	
T	F	T			
F	F	T			
		F			
		F			
⋮	⋮	F			
		F			
		⋮		T	
				F	
				⋮	
F	F	F		F	

There are 2^{2^m} truth functions with m arguments

Sussman's course
= "real" computer science

A <u>propositional-connective</u> is a function C whose arguments and values are WFF's of PC and such that the truth value of $C(\mathcal{F}_1, \ldots, \mathcal{F}_n)$ is determined by the truth values of $\mathcal{F}_1, \ldots, \mathcal{F}_n$

Propositional connectives correspond to truth functions.

---

a WFF has a truth value determined by the truth values of the atomic letters occurring in it as follows:

A <u>valuation</u> V is an assignment of a truth value to each A_i

(i.e., V is a function whose domain is $\{A_0, A_1, A_2, \ldots\}$ -- there are as many valuations as there are real numbers -- and whose values belong to $\{T, F\}$.)

Each V gives rise to a truth value $V(\mathcal{F})$ for every WFF $\mathcal{F}$.

Recursive definition of $V(\mathcal{F})$.

1) $V((A_i)) = V(A_i)$
2) $V(((\mathcal{F}_1) \wedge (\mathcal{F}_2))) = T$ if $V((\mathcal{F}_1)) = V((\mathcal{F}_2)) = T$
   $= F$ otherwise
3) $V(((\mathcal{F}_1) \vee (\mathcal{F}_2))) = T$ if $V((\mathcal{F}_1)) = T$ or $V((\mathcal{F}_2)) = T$
   $= F$ otherwise
4) $V((\neg\mathcal{F})) = T$ if $V(\mathcal{F}) = F$
   $= F$ otherwise
5) $V((\mathcal{F} \to \mathcal{G})) = T$ if $V(\mathcal{F}) = F$ or $V(\mathcal{G}) = T$
   $= F$ otherwise
6) $V((\mathcal{F} \leftrightarrow \mathcal{G})) = T$ if $V(\mathcal{F}) = V(\mathcal{G})$
   $= F$ otherwise

A propositional connective is a function C whose arguments and values are WFF's and s.t. the truth value of C is determined by the truth values of its arguments.

A set S of propositional connectives is said to be complete if all propositional connectives can be generated from S.

example: $\{\neg, \wedge\}$ is complete
$\{\vee, \wedge\}$ is not complete

$\mathcal{F}$ is called a tautology if $V(\mathcal{F}) = T$ for all V.

A_1	$((A_1) \vee (\neg (A_1)))$
T	T
F	T

"Tautology" is an effectively decidable notion (i.e., just evaluate all entries of the truth table)

Famous associated problem: NP-completeness of the decision procedure

[redacted]

Student: Mike Parker
Ashdown 315 B
225-9738

9/19/89

Michael Picard
-teaching assistant
20D-213 x3-2690
787-4767

available:
20E-201 M, F
11:30 - 12:30

Example (of tautology)

$\mathcal{F}$ is $((\neg((A)\vee(B)))\rightarrow((\neg(A))\wedge(\neg(B))))$

A	B	$\neg((A)\vee(B))$	$\mathcal{F}$
T	T	F	T
F	T	F	T
T	F	F	T
F	F	T	T

Axioms and rules for PC

Axioms must be sound
(soundness for PC means a tautology)

Axiom scheme

$((A_0)\rightarrow(A_0))$ would be an axiom
$(\mathcal{F}\rightarrow\mathcal{F})$ would be an axiom scheme, where $\mathcal{F}$ is a WFF

Example of rule:

$$\frac{\mathcal{F}\rightarrow\mathcal{G} \quad \mathcal{G}\rightarrow\mathcal{H}}{\mathcal{F}\rightarrow\mathcal{H}}$$

soundness: if WFF's above the line are tautologies, then the WFF below the line is a tautology

(General) rule R $\quad \dfrac{\mathcal{F}_1, \ldots, \mathcal{F}_n}{\mathcal{G}}$

rule R is sound if for every truth valuation V if $V(\mathcal{F}_i) = T$ for all $i \leq n$, then $V(\mathcal{G}) = T$.

Let APC be a finite set of rules and axioms for PC.

$\Gamma \vdash \mathcal{F}$ — gamma, yield symbol

(Γ is a set of WFF's)

means there is a sequence of $\mathcal{F}_0, \mathcal{F}_1, \ldots, \mathcal{F}_n$ such that for all $i \leq n$,

$\mathcal{F}_i \in \Gamma$

or $\mathcal{F}_i$ is an axiom (of APC)

or $\mathcal{F}_i$ is the result of a rule (of APC) applied to formulas occurring in the sequence $\mathcal{F}_0, \ldots, \mathcal{F}_n$ occurring before $\mathcal{F}_i$

and such that $\mathcal{F}_n$ is $\mathcal{F}_i$ (?)

Suppose $\dfrac{\mathcal{F}, \mathcal{F} \to \mathcal{G}}{\mathcal{G}}$ (modus ponens)

Suppose $(\mathcal{F} \to (\mathcal{G} \to \mathcal{F}))$ is an axiom

Let $\Gamma = \{(A_0)\}$

1. (A_0) — $\in \Gamma$
2. $((A_0) \to ((A_1) \to (A_0)))$ — axiom
3. $((A_1) \to (A_0))$ — rule

$\{(A_0)\} \vdash ((A_1) \to (A_0))$

Yield symbol $\vdash$ is a syntactical device. What is its smantical counterpart?

$\Gamma \models \mathcal{F}$ is the <u>smantical</u> counterpart of $\Gamma \vdash \mathcal{F}$

↑ satifaction symbol (Tarski)
("not a good choice of name" – professor)

$\Gamma \models \mathcal{F}$ means for every truth valuation V: if V makes every member of Γ true, then V makes $\mathcal{F}$ true.

We will eventually prove this metatheorem:

$$\boxed{\begin{array}{c} \Gamma \vdash \mathcal{F} \\ \text{iff} \\ \Gamma \models \mathcal{F} \end{array}}$$

Letting Γ be infinite makes this difficult to prove.

$\phi \vdash \mathcal{F}$ abbrev: $\vdash \mathcal{F}$ means $\mathcal{F}$ is provable (APC)
$\phi \models \mathcal{F}$ abbrev: $\models \mathcal{F}$ means $\mathcal{F}$ is a tautology

↑ empty set

Compactness Theorem: Suppose for each finite $\Gamma_0 \subseteq \Gamma$ (Γ may be infinite, even uncountable), there is a valuation V such that V makes every member of Γ_0 true. Then there exists a V that makes every member of Γ true.

Proof. Let Γ be $\mathcal{F}_0, \mathcal{F}_1, \mathcal{F}_2, \ldots$ (countable for simplicity in this proof)

We define by recursion a sequence $B_0, B_1, B_2, \ldots$ (Each B_i will be either (A_i) or $(\neg(A_i))$.)

Basis Step ($n=0$) ↓

Fix $n \geq 0$. Suppose $B_0, \ldots, B_{n-1}$ have already been defined so that for each finite subset $H \subseteq \Gamma \cup \{B_0, \ldots, B_{n-1}\}$ there is a V that makes all members of H true.

$H \subseteq \Gamma$

either $\Gamma \cup \{(A_0)\}$ or $\Gamma \cup \{(\neg(A_0))\}$ has f.c.p.

Claim: either $\Gamma \cup \{B_0, \ldots, B_{n-1}, (A_n)\}$ or $\Gamma \cup \{B_0, \ldots, B_{n-1}, (\neg(A_n))\}$ has the "finite consistency property"

a set Δ of WFF's has the finite consistency property if for each $\Delta_0 \subseteq \Delta$, there is a V such that V makes all of Δ_0 true.

Proof of claim: Suppose not.

$\Gamma_0 \cup \{(A_0)\}$

$\exists$ finite $\Gamma_0 \subseteq \Gamma$ s.t. $\Gamma_0 \cup \{B_0, \ldots, B_{n-1}, (A_n)\}$ cannot be made true by any V.

$\Gamma_0 \cup \{(\neg(A_0))\}$

$\exists$ finite $\Gamma_1 \subseteq \Gamma$ s.t. $\Gamma_1 \cup \{B_0, \ldots, B_{n-1}, (\neg(A_n))\}$ cannot be made true by any V.

$\Gamma_0 \cup \Gamma_1$

But $\exists$ V that makes $\Gamma_0 \cup \Gamma_1 \cup \{B_0, \ldots, B_{n-1}\}$ true. For this V, either

$V((A_n)) = T \therefore$ V makes $\Gamma_0 \cup \{B_0, \ldots, B_{n-1}, (A_n)\}$ true

or $V((\neg(A_n))) = T \therefore$ V " $\Gamma_1 \cup \{B_0, \ldots, B_{n-1}, (\neg(A_n))\}$ true

So the recursive def. of $B_0, B_1, B_2, \ldots$ is complete: each B_i is either (A_i) or $(\neg(A_i))$.

$T \cup \{B_0, \ldots, B_n\}$ has the finite consistency property, for each n.

Follows that

$T \cup \{B_0, B_1, B_2, \ldots\}$ has finite consistency property

Define $V(A_i) = T$ if B_i is (A_i)
$= F$ if B_i is $(\neg(A_i))$

Final claim: V makes all of T true.

Suppose $\mathcal{F} \in T$. Must show that $V(\mathcal{F}) = T$.

Suppose the atomic letters of $\mathcal{F}$ are included in $A_0, A_1, \ldots, A_j$

Know that $T \cup \{B_0, \ldots, B_j\}$ has finite consistency property: $\exists$ valuation W s.t. for $\{\mathcal{F}, B_0, B_1, \ldots, B_j\}$

$$W(\mathcal{F}) = W(B_i) = T \quad (i \leq j)$$

Must show $V(A_i) = W(A_i)$ $(i \leq m)$ (j?)

Then $V(\mathcal{F}) = W(\mathcal{F}) = T$

$W(B_i) = T$.

if B_i is (A_i), then $W(A_i) = T$.
if B_i is $(\neg(A_i))$, then $W(A_i) = F$. } matches

Next time: Application: coloring maps (Paul Erdos)
4-color theorem
Would 4 colors suffice for ∞ map?
Compactness says it will.

9/21/89 Review of compactness theorem

Γ is <u>satisfiable</u> if $\exists\ V$ s.t. for all $\mathcal{F} \in \Gamma$, $V(\mathcal{F}) = T$.

Γ is <u>finitely satisfiable</u> if for each finite $\Gamma_0 \subseteq \Gamma$, $\exists\ V$ s.t. for all $\mathcal{F} \in \Gamma_0$, $V(\mathcal{F}) = T$.

Compactness Theorem: If Γ is finitely satisfiable, then Γ is satisfiable.

Extension Lemma. If Γ is finitely satisfiable, then either $\Gamma \cup \{\mathcal{F}\}$ or $\Gamma \cup \{\sim\mathcal{F}\}$ is finitely satisfiable.

Proof (of ext. lemma) Suppose not.

$\Gamma \cup \{\mathcal{F}\}$ is not f.s. $\quad$ $\Gamma \cup \{\sim\mathcal{F}\}$ is not f.s.

$\downarrow$ $\quad$ $\downarrow$

$\exists$ finite $\Gamma_0 \subseteq \Gamma$ s.t. $\Gamma_0 \cup \{\mathcal{F}\}$ is not sat. $\quad$ $\exists$ finite $\Gamma_1 \subseteq \Gamma$ s.t. $\Gamma_1 \cup \{\sim\mathcal{F}\}$ is not sat.

$\Gamma_0 \cup \Gamma_1$ is a finite subset of Γ.

$\Gamma_0 \cup \Gamma_1$ is sat. $\exists\ V$ s.t. for all $\mathcal{G} \in \Gamma_0 \cup \Gamma_1$, $V(\mathcal{G}) = T$.

If $V(\mathcal{F}) = T$, then V makes all of $\Gamma_0 \cup \{\mathcal{F}\}$ true. Hence $\Gamma_0 \cup \{\mathcal{F}\}$ is sat.

If $V(\mathcal{F}) = F$ then V makes all of $\Gamma_1 \cup \{\sim\mathcal{F}\}$ true. Hence $\Gamma_1 \cup \{\sim\mathcal{F}\}$ is sat.

Proof of Compactness: Suppose Γ is f.s.

Let $\mathcal{F}_0, \mathcal{F}_1, \mathcal{F}_2, \ldots$ be a list of all WFF's

Define by recursion $\Gamma_0, \Gamma_1, \Gamma_2, \ldots$

Let $\Gamma_0 = \Gamma$

Assume $\Gamma_0, \ldots, \Gamma_n$ have been defined
Assume $\Gamma_0 \subseteq \Gamma_1 \subseteq \ldots \subseteq \Gamma_n$
Assume Γ_n is finitely sat.

By ext. lemma, either $\Gamma_n \cup \{\mathcal{F}_n\}$ or $\Gamma_n \cup \{\sim\mathcal{F}_n\}$ is f.s.

Let $\Gamma_{n+1} = \Gamma_n \cup \{\mathcal{F}_n\}$ if $\Gamma_n \cup \{\mathcal{F}_n\}$ is f.s.

Otherwise let $\Gamma_{n+1} = \Gamma_n \cup \{\sim\mathcal{F}_n\}$

then $\Gamma_0 \subseteq \Gamma_1 \subseteq \ldots \subseteq \Gamma_n \subseteq \Gamma_{n+1}$

Γ_{n+1} is f.s.

Let $\Gamma_\infty = \bigcup_n \Gamma_n$

Γ_∞ is f.s. because each finite $\Gamma_0 \subseteq \Gamma_\infty$ is contained in some Γ_n.

(Γ_∞ is called a <u>maximal</u> f.s. set)

(because for all $\mathcal{F}$, either $\mathcal{F} \in \Gamma_\infty$ or $(\neg\mathcal{F}) \in \Gamma_\infty$)

Define $V(A_i) = T$ if $(A_i) \in \Gamma_\infty$
$\qquad F$ if $(\neg(A_i)) \in \Gamma_\infty$

Final claim: For all $\mathcal{F} \in \Gamma_\infty$, $V(\mathcal{F}) = T$.

Let $A_0, A_1, \ldots, A_n$ be the atomic letters of $\mathcal{F}$.

For $i \leq n$, let $B_i = (A_i)$ if $V(A_i) = T$
$\qquad (\neg(A_i))$ if $V(A_i) = F$

$\therefore B_i \in \Gamma_\infty$

$\{B_0, \ldots, B_n\}$ is a finite subset of Γ_ω

$\exists\ W \quad W(B_i) = T \ (i \leq n), \quad W(\mathcal{F}) = T$

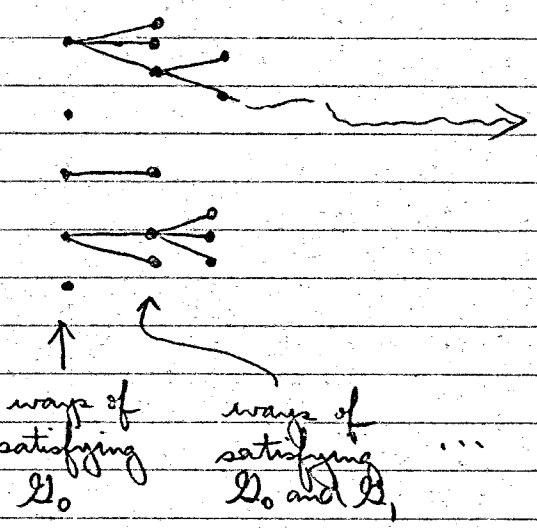
(by definition because Γ_ω is finitely satisfiable)

$W(A_i) = V(A_i) \quad (i \leq n)$

$W(\mathcal{F}) = V(\mathcal{F})$ because if two valuations agree on the atomic letters, they agree on any formula built from the atomic letters.

Since $W(\mathcal{F}) = T$, $\quad V(\mathcal{F}) = T$. (end)

Let $T = \{\mathcal{D}_0, \mathcal{D}_1, \mathcal{D}_2, \ldots\}$



We have really proven a theorem about trees.

A tree begins with an initial node. Each node has some (or none) immediate successors.

A tree is finitely branching if each node has finitely many immediate successors.

Every node on a tree is either the initial node or the successor of some node on the tree.

König's Lemma: If T is finitely branching and has arbitrarily many finite paths, then T has an infinite path.

Skeleton of Compactness Theorem:

Hypothesis $\forall_n \exists V$ weaker

Conclusion $\exists V \forall_n$ stronger

4-color map problem

Specification of map M:

Countries: $C_0, C_1, C_2, \ldots$

Borders: C_i and C_j have a common border

$i \neq j$ ⋮

a coloring of M.

Let's have 4 colors: K_1, K_2, K_3, K_4

C_i has color K_m $(1 \leq m \leq 4)$

If C_i and C_j have a common border, then they have different colors.

HW problem #2 Erdos: If each finite subm$_0$ of M has a coloring, then M has a coloring.

Hint: Use compactness theorem (4 colors instead of 2 truth values) or use Konigs lemma

---

Truth functional completeness

A set S of propositional connectives is said to be complete if every connective is expressible in terms of those in S.

Specify a prop. connective by a truth table.

x	y	z	$c(x,y,z)$
T	T	T	T ✓
F	T	T	F
T	F	T	T ✓
F	F	T	T ✓
T	T	F	F
F	T	F	F
T	F	F	F
F	F	F	F

← each entry of c is T or F

Claim: $\{\neg, \wedge, \vee\}$ is complete

Use A_0, A_1, A_2 in example above

$$((A_0) \wedge (A_1) \wedge (A_2)) \vee ((A_0) \wedge (\neg(A_1)) \wedge (A_2)) \vee ((\neg(A_0)) \wedge (\neg(A_1)) \wedge (A_2))$$

has same t.t. as example above.

$(\mathcal{F} \wedge \mathcal{G} \wedge \mathcal{H})$ means $((\mathcal{F} \wedge \mathcal{G}) \wedge \mathcal{H})$ (associativity)

HW #3: (a) show $\{\neg, \wedge\}$ is complete

(b) show $\{\vee, \wedge\}$ is not complete (show you can't express negation in terms of $\vee$, $\wedge$)

(c) find a single binary connective that is complete.

9/26/89

Corollaries of Compactness

$\Gamma \vdash \mathcal{F}$ iff $\Gamma \models \mathcal{F}$

pf of $\Rightarrow$

$\Gamma \vdash \mathcal{F}$ ⇓ (redundant) $\Gamma_0 \vdash \mathcal{F}$ ⇓ $V(\Gamma)=T \Rightarrow V(\mathcal{F})=T$ ⇓ $\Gamma \models \mathcal{F}$

Assumption: $\Gamma \vdash \mathcal{F}$

so there is a finite $\Gamma_0 \subseteq \Gamma$ s.t. $\Gamma_0 \vdash \mathcal{F}$, because a deduction is finite } (not relevant to proof)

Let V make all of Γ true; show $V(\mathcal{F})=T$

Let $\mathcal{F}_0, \mathcal{F}_1, \ldots, \mathcal{F}_n$ be a deduction of $\mathcal{F}$ from Γ_0

Know $\mathcal{F}_n$ is $\mathcal{F}$

$(i \leq n)$ $\mathcal{F}_i$ is an axiom or $\mathcal{F}_i \in \Gamma_0$ or $\mathcal{F}_i$ is the result of a rule applied to some $\mathcal{F}_j \in \Gamma_0$ $(j<i)$.

Show by induction: $V(\mathcal{F}_i)=T$

① $\mathcal{F}_i$ is an axiom, hence a tautology, so $V(\mathcal{F}_i)=T$

② $\mathcal{F}_i \in \Gamma_0 \Rightarrow V(\mathcal{F}_i)=T$

③ If $\mathcal{F}_i$ is a result of rule R applied to some $\mathcal{F}_j$'s $(j<i)$ then by induction hypothesis, $V(\mathcal{F}_j)$ $(j<i)$ $=T$, and so $V(\mathcal{F}_i)=T$, since R "preserves truth" (by definition of a rule)

pf of $\Leftarrow$

① $\Gamma \vDash \mathcal{F}$

suppose $\Gamma \vDash \mathcal{F}$ ("semantically implies")

show $\Gamma \vdash \mathcal{F}$ ("yields")

We must show there is a deduction

Sublemma: If $\Gamma \vDash \mathcal{F}$, then there exists a finite $\Gamma_0 \subseteq \Gamma$ s.t. $\Gamma_0 \vDash \mathcal{F}$

Pf. Suppose not. Then for each finite $\Gamma_0 \subseteq \Gamma$ there is a V that makes Γ_0 true, and $\mathcal{F}$ false: $(\neg \mathcal{F})$ true

By compactness theorem, there is a V that makes all of Γ true and $\mathcal{F}$ false (contradiction).

② $\Gamma_0 \vDash \mathcal{F}$

$\therefore \exists$ finite $\Gamma_0 \subseteq \Gamma$ s.t. $\Gamma_0 \vDash \mathcal{F}$

Show $\Gamma_0 \vdash \mathcal{F}$

⇓ (def.)

---

③ $\{\mathcal{G}_0, \ldots, \mathcal{G}_m\} \vDash \mathcal{F}$ $\quad \Gamma_0 \vDash \mathcal{F} \quad \Gamma_0 = \{\mathcal{G}_0, \mathcal{G}_1, \ldots, \mathcal{G}_m\}$

$\mathcal{G}_0, \ldots, \mathcal{G}_m \vDash \mathcal{F}$

must show:

④ $\vDash \underbrace{(\mathcal{G}_0 \wedge \ldots \wedge \mathcal{G}_m)}_{H} \rightarrow \mathcal{F}$ $\quad \vDash (\mathcal{G}_0 \,\&\, \mathcal{G}_1 \,\&\, \ldots \,\&\, \mathcal{G}_m) \rightarrow \mathcal{F}$

if $V(\mathcal{G}_0 \wedge \ldots \wedge \mathcal{G}_m) = F$, then $V(H) = T$

if $V(\mathcal{G}_0 \wedge \ldots \wedge \mathcal{G}_m) = T$, then $V(\mathcal{G}_i) = T$ (each i),

so $V(\mathcal{F}) = T$

$\therefore T \rightarrow T$ yields T $\therefore H$ is tautology

Completeness (for PC): If $\mathcal{F}$ is a tautology, then $\vdash \mathcal{F}$.

$\mathcal{F}$ ⇕ $\models \mathcal{F}$ / $\emptyset \models \mathcal{F}$

last part of proof: $\vdash (\mathcal{G} \to \mathcal{F})$ ⇓ $\mathcal{G} \vdash \mathcal{F}$

Suppose $\vdash (\mathcal{G} \to \mathcal{F})$

? $\mathcal{G} \vdash \mathcal{F}$

Sublemma: If $\vdash (\mathcal{G} \to \mathcal{F})$, then $\mathcal{G} \vdash \mathcal{F}$

proof.

⋮ } proof of $\mathcal{G} \to \mathcal{F}$

$\mathcal{G} \to \mathcal{F}$

$\mathcal{G}$

$\mathcal{F}$ by modus ponens

→ Suppose $\mathcal{F}$ is in conjunctive normal form.
(conjunction of disjunctions of atomic letters or their negations)

$(A \vee B \vee \neg C) \wedge (B \vee C \vee \neg D)$

$\mathcal{F}$ is $\mathcal{C}_0 \wedge \mathcal{C}_1 \wedge \cdots \wedge \mathcal{C}_k$

$\mathcal{C}_i$ is a disjunction of atomic letters or their negations.

associate from the left when written with no parentheses:
$\mathcal{F}_0 \wedge \mathcal{F}_1 \wedge \mathcal{F}_2$ means $((\mathcal{F}_0 \wedge \mathcal{F}_1) \wedge (\mathcal{F}_2))$

Each $\mathcal{C}_i$ is a tautology, because $\mathcal{F}$ is.

Suppose we knew how to do completeness for formulas like $\mathcal{C}_i$.

$\vdash \mathcal{C}_0, \ldots, \vdash \mathcal{C}_k$

Add the rule; $\wedge$-introduction

rule

$$\frac{\mathcal{F}, \mathcal{G}}{(\mathcal{F} \wedge \mathcal{G})} \quad \wedge\text{-intro.}$$

$\left.\begin{array}{l}\\\\\end{array}\right\}$ pf of C_0

$\vdots$

$\left.\begin{array}{l}\\\\\end{array}\right\}$ pf of C_k

$(C_0 \wedge C_1)$

$((C_0 \wedge C_1) \wedge C_2)$

etc.

We need completeness for disjunctions of atomic letters and their negations.

C is $K_0 \vee K_1 \vee \dots \vee K_p$

each K_i is an atomic letter or its negation

C is a tautology

$\therefore$ among the K_i's there must be an atomic letter and its negation.

---

axiom

Create an axiom: $(\mathcal{F} \vee (\neg \mathcal{F}))$
(law of excluded middle)

We need axioms and/or rules to establish the associativity and commutivity of $\vee$ (disjunction)

rule $\dfrac{(\mathcal{F} \vee \mathcal{G})}{(\mathcal{G} \vee \mathcal{F})}$ commutativity

rule $\dfrac{\mathcal{F}}{(\mathcal{F} \vee \mathcal{G})}$ $\vee$-introduction

rule $\dfrac{((\mathcal{F} \vee \mathcal{G}) \vee \mathcal{H})}{(\mathcal{F} \vee (\mathcal{G} \vee \mathcal{H}))}$ associativity

example

$((A_0 \vee \neg A_0) \vee A_1)$
use axiom then
$((\neg A_0 \vee A_1) \vee A_0)$
$A_0 \vee (\neg A_0 \vee A_1)$
$(A_0 \vee \neg A_0) \vee A_1$

to prove: reverse associativity:

$\mathcal{F} \vee (\mathcal{G} \vee \mathcal{H})$	
$(\mathcal{G} \vee \mathcal{H}) \vee \mathcal{F}$	comm.
$\mathcal{G} \vee (\mathcal{H} \vee \mathcal{F})$	assoc.
$(\mathcal{H} \vee \mathcal{F}) \vee \mathcal{G}$	comm.
$\mathcal{H} \vee (\mathcal{F} \vee \mathcal{G})$	assoc.
$(\mathcal{F} \vee \mathcal{G}) \vee \mathcal{H}$	comm.

9/28/89

HW #4: Give a nice account of
$\Gamma \vdash \mathcal{F}$ iff $\Gamma \models \mathcal{F}$

$\Gamma \vdash \mathcal{F}$ iff $\Gamma \models \mathcal{F}$

We've reduced proving this to the following:

Suppose $\mathcal{F}$ is a tautology

Show $\vdash \mathcal{F}$

Did a special case of above last time
$\mathcal{F}$ is in CNF (conjunctive normal form)

conjunction of disjunctions of atomic letters and their negations

Plan for arbitrary $\mathcal{F}$ ($\mathcal{F}$ is a tautology):

$\vdash \mathcal{F} \Leftrightarrow \mathcal{G}$ $\quad \mathcal{G}$ in CNF

$\vdash \mathcal{G}$ $\quad$ OK (i.e., we have proved this when $\mathcal{G}$ is a tautology)

$\vdash \mathcal{F}$ by "modus ponens"

rule $\quad \dfrac{H,\ H \Rightarrow K}{K}$ $\quad$ (should be $\Leftrightarrow$ in this case)

Proof that an arbitrary $\mathcal{F}$ is provably equivalent to a $\mathcal{G}$ in CNF

Proof by induction on the length of $\mathcal{F}$

use # of prop. connectives

it is OK by lemma to assume $\mathcal{F}$ is in NNF

Case 1: $\mathcal{F}$ is $(\mathcal{F}_0 \wedge \mathcal{F}_1)$

$\vdash \mathcal{F}_0 \Leftrightarrow \mathcal{G}_0$ } CNF } assume
$\vdash \mathcal{F}_1 \Leftrightarrow \mathcal{G}_1$

$\vdash (\mathcal{F}_0 \wedge \mathcal{F}_1) \Leftrightarrow (\mathcal{G}_0 \wedge \mathcal{G}_1)$

Define a new rule:

rule $\quad \dfrac{H_0 \Leftrightarrow K_0,\ H_1 \Leftrightarrow K_1}{(H_0 \wedge H_1) \Leftrightarrow (K_0 \wedge K_1)}$

(A) (next page)

Case 2: $\mathcal{F}$ is $(\neg \mathcal{F}_0)$

Define: $\mathcal{F}$ is in negation normal form if every negation symbol in $\mathcal{F}$ has as its scope a single atomic letter.

previous page → (A)

Lemma: $\vdash \mathcal{F} \Leftrightarrow \mathcal{G}$ $\mathcal{G}$ in NNF

Pf by induction on length of $\mathcal{F}$

Lemma case 1: $\mathcal{F}$ is $(\mathcal{F}_0 \wedge \mathcal{F}_1)$

$\vdash \mathcal{F}_0 \Leftrightarrow \mathcal{G}_0$
$\vdash \mathcal{F}_1 \Leftrightarrow \mathcal{G}_1$

$\therefore \vdash (\mathcal{F}_0 \wedge \mathcal{F}_1) \Leftrightarrow (\mathcal{G}_0 \wedge \mathcal{G}_1)$ (use Rule in case 1 above)

Lemma case 2: $\mathcal{F}$ is $\mathcal{F}_0 \vee \mathcal{F}_1$

Similar to lemma case 1 rule

$$\frac{(H_0 \Leftrightarrow K_0), (H_1 \Leftrightarrow K_1)}{(H_0 \vee H_1) \Leftrightarrow (K_0 \vee K_1)}$$ } new rule

Lemma case 3: $\mathcal{F}$ is $\mathcal{F}_0 \rightarrow \mathcal{F}_1$

$\vdash \mathcal{F}_0 \Leftrightarrow \mathcal{G}_0$
$\vdash \mathcal{F}_1 \Leftrightarrow \mathcal{G}_1$
$\therefore \vdash \mathcal{F} \Leftrightarrow (\mathcal{G}_0 \rightarrow \mathcal{G}_1)$ (make a new rule) (not done in class)

Lemma case 4: $\mathcal{F}$ is $\mathcal{F}_0 \Leftrightarrow \mathcal{F}_1$

⋮

Lemma case 5: $\mathcal{F}$ is $(\neg \mathcal{F}_0)$

Subcase 5.1 $\mathcal{F}_0$ is $(\mathcal{F}_{01} \vee \mathcal{F}_{02})$

axiom $\vdash (\neg(\mathcal{F}_{01} \vee \mathcal{F}_{02})) \Leftrightarrow ((\neg \mathcal{F}_{01}) \vee (\neg \mathcal{F}_{02}))$

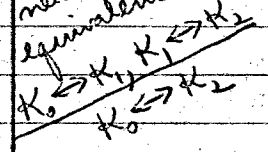
(create new axiom: De Morgan's "axiom")

Subcase 5.2 Exchange $\vee$ and $\wedge$

axiom (create another De Morgan's axiom)

Subcase 5.3 $\rightarrow$

need a transfer equivalence rule



axiom

$\mathcal{F}_0$ is $\mathcal{F}_{01} \rightarrow \mathcal{F}_{02}$

axiom: $\vdash (\neg(\mathcal{F}_{01} \rightarrow \mathcal{F}_{02})) \Leftrightarrow (\mathcal{F}_0 \wedge (\neg \mathcal{F}_1))$

Subcase 5.4: $\Leftrightarrow$

$\vdots$

End of Lemma

Case 2 (cont.): $\mathcal{F}$ is $(\neg \mathcal{Q})$

$\vdash (\neg \mathcal{Q}) \Leftrightarrow \mathcal{H}$ $\mathcal{H}$ is in NNF

$\mathcal{Q}$ is some A_i (because NNF is assumed) in induction hypothesis (i.e., NNF + CNF constructed in parallel)

Case 3: $\mathcal{F}$ is $(\mathcal{F}_0 \vee \mathcal{F}_1)$

Subcase 1. $\mathcal{F}_0$ is $(\mathcal{F}_{01} \wedge \mathcal{F}_{02})$

axiom (distributive law)

$$((\mathcal{F}_{01} \wedge \mathcal{F}_{02}) \vee (\mathcal{F}_1)) \Leftrightarrow (\underbrace{(\mathcal{F}_{01} \vee \mathcal{F}_1)}_{\text{CNF}} \wedge \underbrace{(\mathcal{F}_{02} \vee \mathcal{F}_1)}_{\text{CNF}})$$

this is shorter than $\mathcal{F}_0$, so induction is working.

finish as in Case 1

Subcase 2. $\mathcal{F}_1$ is $(\mathcal{F}_{10} \wedge \mathcal{F}_{11})$

similar to subcase 1

Subcase 3. $\mathcal{F}_0$ is $(\mathcal{F}_{01} \vee \mathcal{F}_{02})$

alternative approach

$\mathcal{F}$ is $(\mathcal{F}_0 \vee \mathcal{F}_1)$

$\mathcal{F} \leftrightarrow (\neg(\neg\mathcal{F}))$ axiom

$(\neg\mathcal{F}) \leftrightarrow ((\neg\mathcal{F}_0) \wedge (\neg\mathcal{F}_1))$ de Morgan

use Lemma? } must use both NNF + CNF assumptions simultaneously

$\mathcal{F}_0$ is $(\mathcal{F}_{01} \vee \mathcal{F}_{02})$

Suppose $\mathcal{F}_{01} \leftrightarrow \mathcal{G}_{01}$

and $\mathcal{G}_{01}$ is in CNF

and is actually a conjunction:

$\mathcal{G}_{01}$ is $(\mathcal{G}_{010} \wedge \mathcal{G}_{011})$

$(\mathcal{G}_{010} \wedge \mathcal{G}_{011}) \vee \mathcal{F}_{02}$

↓ use distributive Rule above

$\underbrace{(\mathcal{G}_{010} \vee \mathcal{F}_{02})}_{\text{CNF}} \wedge \underbrace{(\mathcal{G}_{011} \vee \mathcal{F}_{02})}_{\text{CNF}}$

~~~~~~~~

$(\mathcal{G}_0 \wedge \mathcal{G}_1)$ get to DNF

$\neg\neg(\mathcal{G}_0 \wedge \mathcal{G}_1)$

X $\neg((\underbrace{\neg\mathcal{G}_0}_{\text{CNF}}) \vee (\underbrace{\neg\mathcal{G}_1}_{\text{CNF}}))$ { (will not work because formula is getting longer instead of shorter...?)

$\underbrace{(\neg \text{CNF})}_{\text{DNF}} \wedge \underbrace{\ldots}_{\text{DNF}}$

~~~~~~~~

$\mathcal{F}_0 \vee \mathcal{F}_1$

? $(\mathcal{F}_{00} \wedge \mathcal{F}_{01}) \vee \mathcal{F}_1$

$\underbrace{(\mathcal{F}_{00} \vee \mathcal{F}_1) \wedge (\mathcal{F}_{01} \vee \mathcal{F}_1)}_{\text{CNF}}$

10/3/89

Recap: Assume $\mathcal{F}$ is a tautology

Show $\vdash \mathcal{F}$

> Change definition of WFF (not required on HW problem):
> $\neg, \wedge, \vee$ are the only connectives
> Then introduce $\rightarrow$ and $\leftrightarrow$ in terms of the above
> So $\rightarrow$ and $\leftrightarrow$ can occur in axioms and rules

① $\vdash \mathcal{F} \leftrightarrow \mathcal{G}$, where $\mathcal{G}$ is in negation normal form (by induction on length of $\mathcal{F}$)

② Assume $\mathcal{F}$ is in negation normal form (NNF); show $\vdash \mathcal{F} \leftrightarrow \mathcal{G}$, where $\mathcal{G}$ is in CNF

Case 1: $\mathcal{F}$ is $(\mathcal{F}_1 \wedge \mathcal{F}_2)$ ✓ (done last time)

Case 2: $\mathcal{F}$ is $(\mathcal{F}_1 \vee \mathcal{F}_2)$

Subcase 2.1: $\mathcal{F}_1$ is $\mathcal{F}_{11} \wedge \mathcal{F}_{12}$

$\mathcal{F}$ is $((\mathcal{F}_{11} \wedge \mathcal{F}_{12}) \vee \mathcal{F}_2)$

distr. law $((H \wedge J) \vee K) \leftrightarrow ((H \vee K) \wedge (J \vee K))$

$\underbrace{(\mathcal{F}_{11} \vee \mathcal{F}_2)}_{\text{shorter than } \mathcal{F}} \wedge \underbrace{(\mathcal{F}_{12} \vee \mathcal{F}_2)}_{\text{shorter than } \mathcal{F}}$ OK by induction

Subcase 2.2: $\mathcal{F}_2$ is $\mathcal{F}_{21} \wedge \mathcal{F}_{22}$

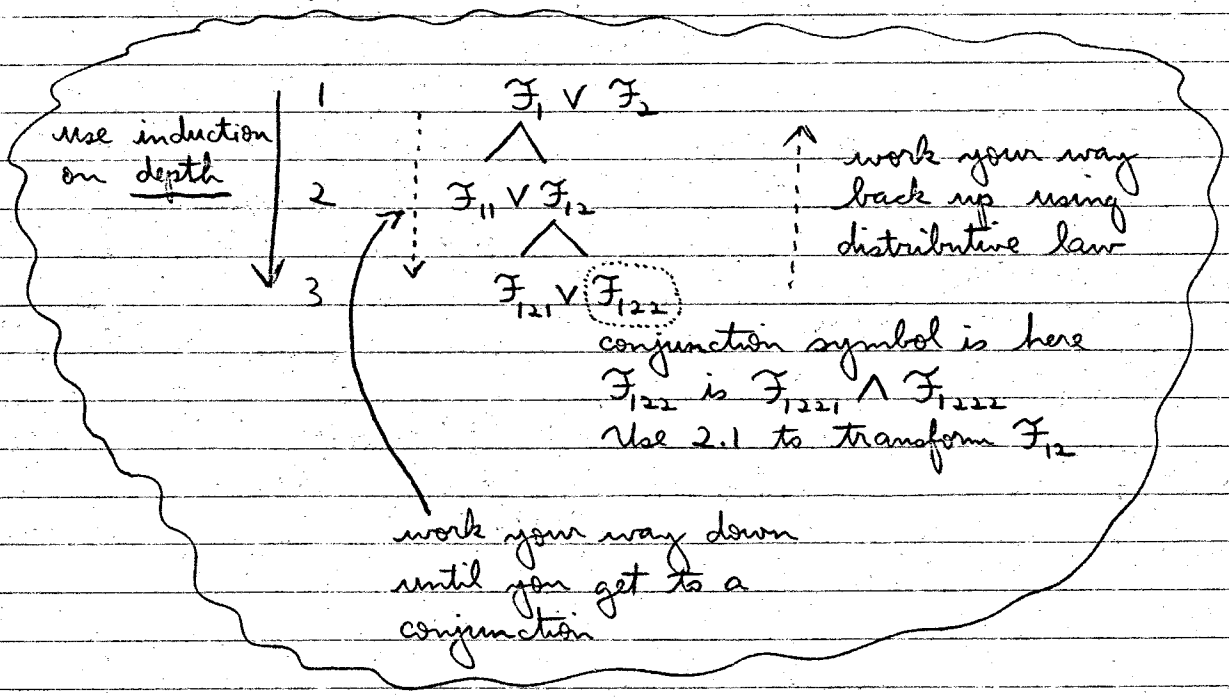
(like 2.1)

Subcase 2.3 (otherwise): $\mathcal{F}_1$ and $\mathcal{F}_2$ are negations of atomic letters or atomic letters or disjunctions

↓ ↑ ↑

✓ OK: already in CNF

Suppose $\mathcal{F}_{21}$ (or $\mathcal{F}_{22}$) is a disjunction



The process of going from a WFF to one of the sub-WFF's increases depth by 1.

We go to the least depth d that reveals a conjunction $\wedge$ symbol. Then we apply the distributive law d times to return a conjunction equivalent to $\mathcal{F}$.

Do we need a lemma? If $\vdash \mathcal{F} \leftrightarrow \mathcal{G}$ infer $\vdash \ldots \mathcal{F} \ldots \leftrightarrow \ldots \mathcal{G} \ldots$

disjunction containing $\mathcal{F}$

build up with

$$\frac{\mathcal{F} \leftrightarrow \mathcal{F}_1,\ \mathcal{G} \leftrightarrow \mathcal{G}_1}{(\mathcal{F} \vee \mathcal{G}) \leftrightarrow (\mathcal{F}_1 \vee \mathcal{G}_1)}$$

Craig's Interpolation Lemma

Suppose $\vdash \mathcal{F} \to \mathcal{G}$

Then there is an $\mathcal{I}$ s.t.

$\vdash \mathcal{F} \to \mathcal{I}$, $\vdash \mathcal{I} \to \mathcal{G}$, and each atomic letter of $\mathcal{I}$ occurs in both $\mathcal{F}$ and $\mathcal{G}$.

Note: If $\vdash \mathcal{F} \to \mathcal{G}$, and $\mathcal{F}$ and $\mathcal{G}$ have no letters in common, then either $\mathcal{F}$ is a contradiction or $\mathcal{G}$ is a tautology.

Pf. Suppose not.

$\exists V \quad V(\mathcal{F}) = T$
$\exists W \quad W(\mathcal{G}) = F$
$\exists U \quad U(\mathcal{F}) = T,\ U(\mathcal{G}) = F,$ so $U(\mathcal{F} \to \mathcal{G}) = F$

↑ because $\mathcal{F}$ and $\mathcal{G}$ have no letters in common

For an $\mathcal{I}$ (interpolant) in this case, we use any tautology if $\mathcal{G}$ is a tautology (T); any contradiction if $\mathcal{F}$ is a contradiction (F).

Introduce T for "standard" tautology
F for "standard" contradiction

"replace T by your favorite tautology..."

$(\mathcal{G} \wedge (T))$ is a WFF

Proof by induction on # of letters in common to both $\mathcal{F}$ and $\mathcal{G}$

$n=0$: ✓ done (see above)

$n>0$: Let A be an atomic letter occurring in both $\mathcal{F}$ and $\mathcal{G}$.

$\mathcal{F}_T$ is the result of replacing each A by T in $\mathcal{F}$.
$\mathcal{F}_F$ is the result of replacing each A by F in $\mathcal{F}$.

$$\mathcal{F} \leftrightarrow ((\mathcal{F}_T \wedge (A)) \vee (\mathcal{F}_F \wedge (\neg(A))))$$

$V(A)=T$ then $V(\mathcal{F}) = V(\mathcal{F}_T \wedge (A))$
$V(A)=F$ then $V(\mathcal{F}) = V(\mathcal{F}_F \wedge (\neg(A)))$

Converse:

$V(\mathcal{F})=T$	$V(\mathcal{F})=T$
$V(A)=T$	$V(A)=F$
↓	↓
$V(\mathcal{F}_T \wedge (A))=T$	$V(\mathcal{F}_F \wedge (\neg(A)))=T$

10/5/89

Craig's Interpolation Lemma (cont.)

Assume $\vdash \mathcal{F} \rightarrow \mathcal{G}$
Find $\mathcal{L}$ s.t. $\vdash \mathcal{F} \rightarrow \mathcal{L}$, $\vdash \mathcal{L} \rightarrow \mathcal{G}$
where each letter of $\mathcal{L}$ occurs in both $\mathcal{F}$ and $\mathcal{G}$

---

n is # of letters common to $\mathcal{F}$ and $\mathcal{G}$

$n=0$: Either $\mathcal{F}$ is a contradiction or $\mathcal{G}$ is a tautology.

We added T and F to list of atomic symbols.
Treat T and F as WFF's s.t.

$V(T) = \text{true} \quad V(F) = \text{false}$ for all V

$(\mathcal{G} \wedge (T))$ is WFF, etc.

Let A be an atomic letter in both $\mathcal{F}$ and $\mathcal{G}$.

$n > 0$

$\mathcal{F}_T$ is $\mathcal{F}$ with A replaced by T
$\mathcal{F}_F$ is $\mathcal{F}$ with A replaced by F

Claim: $\mathcal{F} \Leftrightarrow ((\mathcal{F}_T \wedge A) \vee (\mathcal{F}_F \wedge \neg A))$
$\mathcal{G} \Leftrightarrow ((\mathcal{G}_T \wedge A) \vee (\mathcal{G}_F \wedge \neg A))$

$\mathcal{F}_T \rightarrow \mathcal{G}_T$ (via $\mathcal{I}_1$) $\quad \mathcal{F}_F \rightarrow \mathcal{G}_F$ (via $\mathcal{I}_0$) } induction hypothesis

Try $\mathcal{I}$ as $(\mathcal{I}_0 \wedge A) \vee (\mathcal{I}_0 \wedge \neg A)$ (1?)

? $\mathcal{F} \rightarrow \mathcal{I}$ ✓
? $\mathcal{I} \rightarrow \mathcal{G}$ ✓

$\mathcal{I}$ unfortunately has T's and F's,
which are not real atomic symbols.
Replace T by $A \vee \neg A$, F by $A \wedge \neg A$.

Deduction Theorem

If $\Gamma, \mathcal{F} \vdash \mathcal{G}$, then $\Gamma \vdash \mathcal{F} \rightarrow \mathcal{G}$

In our ~~case~~ version, this follows trivially
from $\Gamma, \mathcal{F} \models \mathcal{G}$ then $\Gamma \models \mathcal{F} \rightarrow \mathcal{G}$

First Order Logic

Specify a first order language $\mathcal{L}$

Logical symbols:

(	$\rightarrow$ } (may also be
)	$\leftrightarrow$ } derived symbols)
$\vee$	
$\wedge$	$\exists$ existential quantifier
$\neg$	$\forall$ universal quantifier
	$x_0, x_1, \ldots$ ∞ supply of letters

"dummy variables are sometimes needed in proofs, so we may run out even though sentences have a given finite # of them"

$=$ equality (in our system)
(sometimes excluded)

Non-logical symbols:

called "signature" of language:

- relation symbols R, n arguments
- function symbols f, n arguments
- individual constants c

e.g. Arithmetic

$<$	relation, 2 arguments
$+, *$	functions, 2 arguments
$0, 1$	constants

Define term

1. Each x_i is a term
2. Each individual constant is a term
3. If $t_1, \ldots, t_n$ are terms and f is an n-place function symbol, then $f(t_1, \ldots, t_n)$ is a term

$f(t_1 \ldots t_n)$ ← strictly speaking, commas are not defined

parentheses are optional

Define WFF

1. $(t_1 = t_2)$ t_1 and t_2 are terms
2. If $t_1, \ldots, t_n$ are terms and R is an n-place relation symbol, then $(R(t_1, \ldots, t_n))$ is a WFF.

   more formally, $(R t_1 \ldots t_n)$

3. If $\mathcal{F}$ and $\mathcal{G}$ are WFF's, so are $(\mathcal{F} \wedge \mathcal{G})$, $(\mathcal{F} \vee \mathcal{G})$, $(\neg \mathcal{F})$, maybe $(\mathcal{F} \to \mathcal{G})$, $(\mathcal{F} \leftrightarrow \mathcal{G})$ (if $\to$ and $\leftrightarrow$ aren't derived)
4. If $\mathcal{F}$ is a WFF, so are $\exists x_i \mathcal{F}$, $\forall x_i \mathcal{F}$

An $\mathcal{L}$-structure $\mathcal{A}$ consists of

1. a nonempty set A, called the universe of $\mathcal{A}$
2. For each n-place relation symbol R of $\mathcal{L}$, $\mathcal{A}$ has an n-place relation $R^{\mathcal{A}}$ on A.

   An n-place relation on X is any subset of X^n.

   $$X^n = \{\langle y_1, \ldots, y_n \rangle \mid y_i \in X\}$$

   e.g. in arithmetic, $<^{\mathcal{A}} \subseteq \{\langle y_1, y_2 \rangle \mid y_i \in A\}$
   $y_1 < y_2$ means $\langle y_1, y_2 \rangle \in <$

3. For each n-place function symbol f of $\mathcal{L}$, $\mathcal{A}$ has an n-place function $f^{\mathcal{A}}: A^n \to A$.
4. For each individual constant c of $\mathcal{L}$, $\mathcal{A}$ has a distinguished element $c^{\mathcal{A}} \in A$.

Define $\mathcal{A} \vDash \mathcal{F}$, where $\mathcal{F}$ is a sentence of $\mathcal{L}$
"$\mathcal{A}$ satisfies $\mathcal{F}$"
(due to Tarski)

An occurrence of x_i in $\mathcal{F}$ is said to be free if it is not within the scope of some $\exists x_i$ or $\forall x_i$.

$\mathcal{F}$ is a sentence if $\mathcal{F}$ has no free occurrence of any variables.

10/12/89

First order language $\mathcal{L}$ (review)

Specified by
- relation symbols $R(\ ,\ ,\ \ldots\ )$ (n-place)
- function symbols $f(\ )$
- individual constants

$\mathcal{L}$-structure $\mathcal{A}$
- universe of $\mathcal{A}$ is A, a non-empty set
- relation $R^{\mathcal{A}} \subseteq A^n$
- function $f^{\mathcal{A}}: A^n \to A$
- distinguished element $c^{\mathcal{A}}$ (constant)

e.g.: arithmetic — $\mathcal{A}$
- $<$ relation — $<^{\mathcal{A}}$
- $+, \cdot$ functions — $+^{\mathcal{A}}, \cdot^{\mathcal{A}}$ } addition and mult. tables
- $0, 1$ individual constants — $0^{\mathcal{A}}, 1^{\mathcal{A}}$
- $=$

Define $\mathcal{A} \models \mathcal{F}$ "$\mathcal{A}$ satisfies $\mathcal{F}$"
or "$\mathcal{A}$ makes $\mathcal{F}$ true" ← (preferred?)

Let $\mathcal{L}_A$ be an extension of $\mathcal{L}$ obtained by adding a new individual constant $\underline{a}$ for each $a \in A$.

↑ a name for each element of A

Let η (Greek letter eta) be a naming map.

iff t is a constant term (a term w/ no variables) of $\mathcal{L}_A$, then $\eta(t) \in A$, and t is a name for $\eta(t)$.

Define $\eta(t)$ by recursion on complexity of t:

$\eta(c) = c^a$ for each individual constant c of $\mathcal{L}$
$\eta(a) = a$ $(a \in A)$
$\eta(f(t_1, \ldots, t_n)) = f^a(\eta(t_1), \ldots, \eta(t_n))$

e.g. in arithmetic example,
$\eta(1+0) = 1^a +^a 0^a$

$a \vDash \mathcal{F}$ (where $\mathcal{F}$ is a sentence of $\mathcal{L}_A$, the extended language) is defined by recursion on the logical complexity of $\mathcal{F}$, i.e., on the number of logical connectives.

1) $\mathcal{F}$ is $t_1 = t_2$

note: remember that $\eta()$ is an element of A

$a \vDash t_1 = t_2$ iff $\eta(t_1) = \eta(t_2)$

($=$: logical symbol; $=$: English equality symbol (i.e., the two elements named by η are identical))

2) $\mathcal{F}$ is $R(t_1, \ldots, t_n)$

$a \vDash R(t_1, \ldots, t_n)$ iff $R^a(\eta(t_1), \ldots, \eta(t_n))$

e.g. $1 < 0$ iff $\underbrace{1^a <^a 0^a}$
this is what we look at (may or may not be true in a)

3) $a \vDash (\mathcal{F}_1 \wedge \mathcal{F}_2)$ iff $a \vDash \mathcal{F}_1$ and $a \vDash \mathcal{F}_2$

4) $a \vDash (\neg \mathcal{G})$ iff it is not the case that $a \vDash \mathcal{G}$

$\exists x \mathcal{G}$ introduces the variable x into a sentence (a sentence may never have free variables)

5) $\mathcal{A} \models \exists x \mathcal{G}$ iff there exists an $a \in A$ s.t. $\mathcal{A} \models \mathcal{G}^x_{\underline{a}}$

Notation (for substitution):
Let $\mathcal{G}$ be a WFF
$\mathcal{G}^x_t$ is the result of substituting t for each free occurrence of x in $\mathcal{G}$:

$\mathcal{G}$ ..... x .....
$\downarrow$
t

Define $\forall x$ as $\neg \exists x \neg$.

$\mathcal{A}$ is a <u>model</u> of $\mathcal{F}$ means $\mathcal{A} \models \mathcal{F}$ ($\mathcal{A}$ makes $\mathcal{F}$ true).

e.g.: Let $\mathcal{M}$ be the standard model for arithmetic.

"$2+2=4$ is true" means the thing <u>named</u> on the left is the same as the thing <u>named</u> on the right.

Let $'$ be <u>successor</u> symbol (function):

$\mathcal{M} \models 0'' + 0'' = 0''''$
iff
$\eta_m(0'') +^m \eta_m(0'') = \eta_m(0'''')$
$\downarrow$ expand
$(0^m)'^m{}'^m +^m \ldots$

Compactness Theorem:

Let S be a set of sentences such that every finite subset of S has a model. Then S has a model.

First we will construct an "algebra" proof before the "real" proof.

Let $\{a_i \mid i \in I\}$ be a family (set) of structures.
(I: index family; they're all $\mathcal{L}$-structures for the same $\mathcal{L}$)

I is an index set. ($\{a_i\}$ could be $\{A_0, A_1, \ldots\}$ but I allows it to be more general.)

Product Structure

Definition of $\prod_{i \in I} a_i$ (product of structures; we want the result to be an $\mathcal{L}$-structure)

1) Universe of $\prod_{i \in I} a_i$ is $\underbrace{\prod_{i \in I} A_i}_{\text{Cartesian product}} =$

$$\{h \mid h \text{ is a function, domain of } h = I, \text{ and } h(i) \in A_i \text{ for all } i \in I\}$$

e.g.: $I = \{0, 1\}$

There are 2 structures a_0, a_1

$h \in \prod_{i \in I} A_i$ means $h: \{0,1\} \to \begin{cases} h(0) \in A_0 \\ h(1) \in A_1 \end{cases}$

h is an ordered pair $(a_0, a_1) \in A_0 \times A_1$

More generally, $(a_0, a_1, a_2, \ldots) \in A_0 \times A_1 \times A_2 \times \ldots$ can be expressed as

$h(i) \in A_i$, where $i \in \{0, 1, 2, \ldots\}$

This is redefined in next lecture (wrong?)

2) For each relation symbol R

$$R^{\prod_{i\in I} a_i} = \{\langle h_1, \ldots, h_m\rangle \mid \langle h_1(i), \ldots, h_m(i)\rangle \in R^{a_i} \text{ for all } i \in I\}$$

i.e., $\langle h_1, \ldots, h_m\rangle \in R^{\prod_{i\in I} a_i}$ iff

$$\langle h_1(i), \ldots, h_m(i)\rangle \in R^{a_i} \text{ for all } i \in I$$

The relationship holds "coordinate-wise"!

e.g. arithmetic

Suppose a_0 and a_1 are structures for arithmetic. Suppose

$(a_0, a_1) \in A_0 \times A_1$

$(b_0, b_1) \in A_0 \times A_1$

Then

$(a_0, a_1) <^{a_0 \times a_1} (b_0, b_1)$

means $a_0 <^{a_0} b_0$ and $a_1 <^{a_1} b_1$.

3) For each function symbol f

$$f^{\prod_{i\in I} a_i}(h_1, \ldots, h_m) = h_{m+1} \text{ iff}$$

$$f^{a_i}(h_1(i), \ldots, h_1(i)) = h_{m+1}(i) \text{ for all } i \in I$$

4) For each constant symbol c

$$c^{\prod_{i\in I} a_i}(i) = c^{a_i}$$

Ultraproducts

First, define <u>Boolean algebra</u> B

$$B = \langle B, \wedge, \vee, ', 0, 1\rangle$$

Axioms for a Boolean algebra:

(can be derived (not axioms)?)

$x \vee x' = 1$
$x \wedge x' = 0$

$(x \vee y)' = x' \wedge y'$
$(x \wedge y)' = x' \vee y'$

$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$
$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$

$x \wedge y = y \wedge x$
$x \vee y = y \vee x$

? also need axioms
$x \vee 0 = x$
$x \wedge 1 = x$

$x \vee (y \vee z) = (x \vee y) \vee z$
$x \wedge (y \wedge z) = (x \wedge y) \wedge z$

Example: Let I be any non-empty set
$2^I \stackrel{\text{def}}{=} \{J \mid J \subseteq I\}$ power set

2^I is a Boolean algebra
- $\wedge$ is $\cap$
- $\vee$ is $\cup$
- J' is $I - J$
- 0 is $\emptyset$ (empty set)
- 1 is I

filter or dual ideal G

Let $\mathcal{B}$ be a Boolean algebra. $F \subseteq B$ is an ideal if

$G \neq B$
$0 \notin G$
$x, y \in G \to x \wedge y \in G$
$x \in G + x \leq y \to y \in G$

0) F is non-empty
1) $1 \notin F$
2) $x, y \in F \to x \wedge y \in F$
3) $x \in F \;\&\; y \leq x \to y \in F$

definition of $\leq$ (for $\mathcal{B}$):
$x \leq y$ means $x \wedge y = x$.
$0 \leq x$ because $0 \wedge x = 0$ ← (must prove)

e.g.: $\{0\}$ is an ideal because $0 \neq 1$, and $\{y \mid y \leq x\} = \{0\}$

Next time: maximal ideal theorem: $\exists$ maximal ideals

"take ultraproduct of models of linear ordering; the result will be a linear ordering"

10/17/89

HW #5 Let F_n be the unique linear ordering of n elements. Let $F_\infty = \frac{\prod_{n\in\omega} F_n}{D}$ where D is non-trivial. Show F_∞ is ∞. Show $\mathbb{Q}$ can be embedded in F_∞. Show $\mathbb{Z}$ can be embedded in F_∞.

Explanations for HW:

Notion of <u>linear ordering</u>: language s.t.

$<$ is binary relation

axioms:

$\forall x \neg(x<x)$

$\forall x \forall y (x<y \vee x=y \vee y<x)$

$\forall x \forall y \forall z ((x<y \wedge y<z) \rightarrow x<z)$

$\mathbb{Q}$ is the linear ordering of the rationals.

$\mathbb{Z}$ is the linear ordering of the integers (positive and negative).

Embedding means there is a subset of F_∞ that looks like $\mathbb{Q}$.

Let L_1 and L_2 be linear orderings. L_1 <u>embeddable</u> in L_2 means

$\exists f: L_1 \xrightarrow{\text{into}} L_2$ (doesn't have to be onto)

such that $\forall x \forall y (x <_1 y \rightarrow f(x) <_2 f(y))$

($x<_1 y$: $x<y$ in the sense of L_1; $f(x)<_2 f(y)$: in the sense of L_2)

Review

$\prod_{i \in I} A_i$ is an ultraproduct

$\mathcal{B}$ is a Boolean algebra: B, $0, 1$, $\vee, \wedge, '$

$x \leq y$ in $\mathcal{B}$ means $x \wedge y = x$

e.g.: $0 \leq x$ means $0 \wedge x = x$

if F is a filter: (dual ideal)

F is an ideal:

$F \subseteq B$

$F \neq B$ $\quad$ (i.e., $1 \notin F$)

$x, y \in F \rightarrow x \vee y \in F$

$x \in F \;\&\; y \leq x \rightarrow y \in F$

$F \subseteq B$

$\phi \notin F$

$\cdots x \wedge y \cdots$

$\cdots x \leq y \cdots$

Maximal Ideal Theorem

↓ (sometimes called prime ideal theorem in ring theory)

Suppose $C \subseteq B$, where B is a Boolean algebra. C is a basis for an ideal if: the join of any finite number of elements from C is not 1.

the meet

not ϕ

Let C be a basis for an ideal. Then $C \subseteq F$, for some F an ideal. To get F:

$F = \{ y \mid y \in B \;\&\; y \leq$ finite join of elements of $C \}$

$F \supseteq C$

$y \geq$ finite meet

less than some finite join $\vee$ less than some finite join

$x \vee y$ } result is less than some finite join

F is a maximal ideal if there is no ideal G s.t. $F \subsetneq G$.

↳ Maximal Ideal Theorem: Each ideal of B is contained in some maximal ideal of B.

(analogous to "either $\mathcal{F}$ or $\neg\mathcal{F}$ is true" in a valuation of propositional calculus)

Dual ideal ↓

Proof

Assume B is countable (for our purposes; not necessarily true in general): $\{b_0, b_1, \ldots\}$

$G_0 = F$

Claim: Either $G_0 \cup \{b_0\}$ is a basis for an ideal
or $G_0 \cup \{b_0'\}$ is a basis for an ideal

Suppose not. Then both of the following are true:

$\underbrace{x_0 \vee \ldots \vee x_m}_{x} \vee b_0 = 1$

$\cdots \wedge \cdots = 0$

$\underbrace{y_0 \vee \ldots \vee y_p}_{y} \vee b_0' = 1$

$\cdots \wedge \cdots = 0$

Then $(x \vee b_0) \wedge (y \vee b_0') = 1$

$((x \vee b_0) \wedge y) \vee ((x \vee b_0) \wedge b_0') = 1$

$(x \wedge y) \vee (b_0 \wedge y) \vee (b_0' \wedge x) \vee \underbrace{(b_0 \wedge b_0')}_{0} = 1$

$(x \wedge y) \vee (b_0 \wedge y) \vee (b_0' \wedge x) = 1$

$(x \wedge y) \vee y \vee x = 1$

$\boxed{y \vee x = 1}$ (contradiction)

$y \wedge x = 0$

Suppose $G_0 \cup \{b_0\}$ is a basis for an ideal.
Let G_1 be the ideal generated by this basis.

(etc. --- analogous to compactness theorem proof)

Note that we assumed that B is countable.
For HW, assume algebra is countable.

Define $\frac{\prod_{i\in I} a_i}{D}$; where D is a maximal dual ideal (also called an ultrafilter) of 2^I

For any set I, 2^I is the Boolean algebra of all subsets of I:

$\wedge = \cap \quad \vee = \cup \quad 0 = \phi \quad 1 = I$

$D \subsetneq 2^I$

If G is a dual ideal, then
1) $G \neq B \quad (0 \notin G)$
2) $x, y \in G \rightarrow x \wedge y \in G$ ($x \wedge y$ is the meet of x and y)
3) $x \in G \;\&\; x \leq y \rightarrow y \in G$

Note: If F is a maximal ideal of B, then $B - F$ is a maximal dual ideal of B

Define $\frac{\prod_{i\in I} a_i}{D}$ } name of a structure; could be loosely called "divided by" or "mod" D; also "reduced product"

Typical member of the universe $\prod_{i\in I} A_i$ of the structure $\prod_{i\in I} a_i$:

$h \in \prod_{i\in I} A_i \qquad \text{dom } h = I \qquad h(i) \in A_i$

h is a function; A_i is universe of structure a_i

Suppose $h, g \in \prod_{i\in I} A_i$. Define "equivalence" $\sim$:

$h \sim g \iff \{i \mid h(i) = g(i)\} \in D$

($h \sim g$: This is a relation (either true or false))

Note: If $h = g$, then $h \sim g$; $\therefore h \sim h$ (because $I \in D$)

$h \sim g$ means h and g are equal "almost everywhere"

Claim: { $h \sim h$
If $h \sim k$, then $k \sim h$ (look at definition)
If $h \sim k$ and $k \sim l$, then $h \sim l$

Proof of third claim:

$\{i \mid h(i) = k(i)\} \in D$

$\{i \mid k(i) = l(i)\} \in D$

Take intersection:

$\{\} \cap \{\cdots\} \in D$ (because D is a dual ideal)

$\underbrace{\{i \mid h(i) = k(i) = l(i)\}}_{\subseteq \{i \mid h(i) = l(i)\}} \in D$

$\therefore h \sim l$

These 3 properties mean that "$\sim$" is an equivalence relation.

Define $[h] = \{k \mid k \in \prod_{i \in I} A_i \;\&\; k \sim h\}$

(equivalence class of h)

$[h]$ is a typical member of the ultraproduct $\frac{\prod_{i \in I} A_i}{D}$.

$[h] \in \frac{\prod_{i \in I} A_i}{D}$

$\frac{\prod_{i \in I} A_i}{D}$ is the universe of the structure $\frac{\prod_{i \in I} a_i}{D}$.

Define $\mathcal{U} = \frac{\prod_{i \in I} a_i}{D}$ (for convenience). Then

$R^{\mathcal{U}}([h_1], \ldots, [h_m])$ means $\{i \mid R^{a_i}(h_1(i), \ldots, h_m(i))\} \in D$

(a relation holds on the ultraproduct if it holds on almost every coordinate)

$f^{\mathcal{U}}([h_1], \ldots, [h_m]) = [h_{m+1}]$ means

$\{i \mid f^{a_i}(h_1(i), \ldots, h_m(i)) = h_{m+1}(i)\} \in D$

$c^{\mathcal{U}} \overset{\text{means}}{=} [c_0]$ (equivalence class of function c_0, i.e., an element of universe $\frac{\prod_{i \in I} A}{D}$)

Explanation:

Let $c_0(i) = c^{a_i}$ for each i; then $c^{\mathcal{U}} = [c_0]$

$c_0 \in \prod_{i \in I} A_i$ i.e., $c_0(i) \in A_i$
i.e., $c_0(i) = c^{a_i}$

(Pick the (one) function c_0 for which all $c_0(i) = c^{a_i}$, where c^{a_i} is a (constant) member of the structure a_i. Then find the equivalence class under D of function c_0.)

$$c^u = [c_0] = \{k \mid k \in \prod_{i \in I} A \;\&\; \underbrace{k \sim c_0}_{\{i \mid k(i) = \underbrace{c_0(i)}_{c^{a_i}}\} \in D}\}$$

Expanded: $c^{\frac{\pi a_i}{D}} = [c^{\pi a_i}]$

Example: In arithmetic, the equivalence class of 0 would be any sequence which is "0 almost everywhere"

Fundamental Theorem of Ultraproducts

$$\underbrace{\frac{\pi a_i}{D} \models \mathcal{F}}_{\mathcal{F} \text{ is true in } \frac{\pi a_i}{D}} \iff \{i \mid a_i \models \mathcal{F}\} \in D$$

"It's true in the ultraproduct if it's true almost everywhere"

This theorem provides a way of building new structures from old ones.

In fact, we prove something stronger:

$$\frac{\Pi a_i}{D} \vDash \mathcal{F}([h_1], \ldots, [h_m])$$

$$\updownarrow$$

$$\{i \mid a_i \vDash \mathcal{F}(h_1, \ldots, h_m)\} \in D$$

Proof: by induction on the complexity of $\mathcal{F}$.

Start with simplest $\mathcal{F}$: $h_1 = h_2$

$$\frac{\Pi a_i}{D} \vDash [h_1] = [h_2]$$

$$\updownarrow$$

$$\{i \mid h_1(i) = h_2(i)\} \in D$$

Def. of relation $(=)$

$\downarrow$: $[h_1] = [h_2]$ means h_1 and h_2 have the same equivalence classes; so they are equal members of $\frac{\Pi A_i}{D}$

$\uparrow$: $[h_1] = \{k \mid k \in \Pi A_i \ \& \ k \sim h_1\}$
$[h_2] = \{k \mid k \in \Pi A_i \ \& \ k \sim h_2\}$
} same because $\{i \mid h_1(i) = h_2(i)\} \in D$

$\therefore [h_1] = [h_2]$

Induction step:

Case 1: $\mathcal{F}_1 \wedge \mathcal{F}_2$

$$\frac{\Pi a_i}{D} \vDash \mathcal{F}_1 \wedge \mathcal{F}_2$$

$$\updownarrow$$

$$\frac{\Pi a_i}{D} \vDash \mathcal{F}_1 \quad \text{and} \quad \frac{\Pi a_i}{D} \vDash \mathcal{F}_2$$

$\updownarrow$ induction hypothesis — $\updownarrow$ induction hypothesis

$$\{i \mid a_i \vDash \mathcal{F}_1\} \in D \qquad \{i \mid a_i \vDash \mathcal{F}_2\} \in D$$

$\therefore \Pi$ is $\in D$ (because it's a maximal dual ideal)

Case 2: $\vdash \neg \mathcal{G}$

$\mathcal{U} \vdash \neg \mathcal{G}$

↓

not $\mathcal{U} \vdash \mathcal{G}$

↓

not $\{i \mid a_i \vdash \mathcal{G}\} \in D$ ⋮ argument is reversible

↓ (maximality of D proves this)

$(I - \{i \mid a_i \vdash \mathcal{G}\}) \in D$

↓

$\{i \mid a_i \vdash \neg \mathcal{G}\} \in D$ (the set of all i's for which $\mathcal{G}$ is not true in a_i, i.e., $\neg \mathcal{G}$ is true in a_i)

See: Chang + Keisler, Model Theory

Next time: quantifiers

10/19/89

Proof of Fundamental Theorem of Ultraproducts (cont.)

$$\frac{\prod_{i \in I} a_i}{D} \vdash \mathcal{F}([h_1], \ldots, [h_n]) \leftrightarrow \{i \mid a_i \vdash \mathcal{F}(h_1(i), \ldots, h_n(i)\} \in D$$

element of ultraproduct $[h] \in \frac{\prod_{i \in I} A_i}{D}$

$[h_i]$: name of element

"ultrapower mod max. dual ideal" $\equiv \mathcal{U}$

$\mathcal{F}$: function of elements of ultraproduct

Case 3: $\mathcal{F}$ is $\exists x \mathcal{G}$

Suppose $\mathcal{U} \vdash \exists x \mathcal{G}$

Then $\mathcal{U} \vdash \mathcal{G}([h])$ ($\mathcal{U}$ makes some instance of $\mathcal{G}$ true)

($\mathcal{G}^x_{[h]}$ would be more precise)

$\{i \mid a_i \vDash \mathcal{B}(h(i))\} \in D$ by induction hypothesis

$\Rightarrow \{i \mid a_i \vDash \exists x \mathcal{B}\} \in D$

Other direction:

Suppose $\underbrace{\{i \mid a_i \vDash \exists x \mathcal{B}\}}_{\equiv Z} \in D$

For each $i \in Z$ choose $a_i \in A$ s.t. $a_i \vDash \mathcal{B}^x_{a_i}$ (uses Axiom of Choice)

Define $h(i) = \begin{cases} a_i \text{ if } i \in Z \\ b_i \text{ if } i \in I - Z, \text{ where } b_i \text{ is any element of } A_i \end{cases}$

then $h \in \prod_{i \in I} A_i$ $\quad [h] \in \frac{\prod_{i \in I} A_i}{D}$

($[h]$: equiv. class of h)

Notice that $\{i \mid a_i \vDash \mathcal{B}^x_{h(i)}\} \supseteq Z$ ($\supseteq$: includes), $Z \in D$

$\therefore \{i \mid a_i \vDash \mathcal{B}^x_{h(i)}\} \in D$ (if something is a dual ideal, then anything bigger is a dual ideal)

So

$\frac{\prod_{i \in I} a_i}{D} \vDash \mathcal{B}^x_{[h]}$

$\Rightarrow \mathcal{U} \vDash \exists x \mathcal{B}$

(if it is true "almost everywhere, it is true in the ultraproduct)

Now we will use the Fundamental Theorem to prove compactness.

Compactness: (Assume S is ∞) Let S be a set of sentences such that each finite $S_0 \subseteq S$ has a model (i.e., there is a structure that makes all sentences of S_0 true). Then S has a model.

Let $P, Q, R, \ldots$ denote finite subsets of S.

(A) (This part is wrong; is re-done below:) ↓

Let I be the set of all finite subsets of S.
↑ this will be our index set

Let F be the set of all co-finite subsets of I
(x is <u>cofinite</u> if $x \in I$ and $I - x$ is finite)

$\mathcal{B}$ = Boolean algebra of subsets of I, namely 2^I

Claim: F is a dual ideal in $\mathcal{B}$

i.e. 1) $F \neq B$ (in particular, $\emptyset \notin F$)
F must be ∞, since it is co-finite
$\emptyset$ is not ∞, $\therefore$ is not co-finite, so this is OK

2) $x, y \in F \rightarrow x \cap y \in F$
$I - x$ is finite
$I - y$ is finite
$I - (x \cap y) = I \cap (x \cap y)' = I \cap (x' \cup y')$ (since $a - b = a \cap (b)'$)
$= (I \cap x') \cup (I \cap y')$
$= (I - x) \cup (I - y)$
which is finite

3) (upward closure) $x \in F \;\&\; x \subseteq y \rightarrow y \in F$
$I - x$ is finite, so $x \subseteq y \rightarrow I - y$ is finite

Extend F to D, a maximal dual ideal. Then $F \subseteq D \subseteq I$

Now use the hypothesis:
For each $P \subseteq S$ (finite subset of S, i.e., $P \in I$), choose a_P, a model of P

Define ultraproduct $\mathcal{U} = \frac{\prod_{P \in I} a_P}{D}$

Claim (B) (referred to below): $\mathcal{F} \in S \Rightarrow \mathcal{U} \vdash \mathcal{F}$ ("$\mathcal{U}$ makes $\mathcal{F}$ true")

We must show $\{i \mid i \in I \& a_i \vDash \mathcal{F}\} \in D$
(if we show this, we're done)

(Corrected definitions)

I = set of all finite subsets of S (correct)
$B = 2^I$ Boolean algebra
For each $\mathcal{F} \in S$, let

$$b_{\mathcal{F}} = \{x \mid \mathcal{F} \in x \text{ and } x \in I\}$$

(all finite subsets of x that have $\mathcal{F}$ as an element)

$b_{\mathcal{F}} \in B$

Let $F = \{b_{\mathcal{F}} \mid \mathcal{F} \in S\}$

↑ see above (A)

Claim: F is a basis for a dual ideal

We must show that no finite intersection of the elements of F is $\emptyset$.

Suppose $b_{\mathcal{F}_1} \cap b_{\mathcal{F}_2} \cap \dots \cap b_{\mathcal{F}_n} = \emptyset$

Notice that $\{\mathcal{F}_1, \mathcal{F}_2, \dots, \mathcal{F}_n\} \subseteq S$ (is a finite subset of S)

$b_{\mathcal{F}_i}$ = all finite subsets of S to which $\mathcal{F}$ belongs
$\therefore \{\mathcal{F}_1, \mathcal{F}_2, \dots, \mathcal{F}_n\} \in b_{\mathcal{F}_i}$ $(1 \le i \le n)$

So $\bigcap_{1 \le i \le n} b_{\mathcal{F}_i} \neq \emptyset$

Now extend F to a maximal ideal.

Note that $b_{\mathcal{F}} \subseteq \{i \mid i \in I \text{ and } a_i \vDash \mathcal{F}\}$

If $j \in b_{\mathcal{F}}$ and $\mathcal{F} \in j$ then $a_j \vDash \mathcal{F}$ (because a_j was chosen to be a model of j)

but $b_{\mathcal{F}} \in D$ (end of proof)

↑ see above (B)

$\therefore$ Claim (B)

Trivial Ultraproducts

If $b \in B$ (a Boolean algebra), $b \neq 0$, define

$$(b) = \{c \mid b \leq c \in B\}$$

(dual ideal generated by b)

Note: (b) is a dual ideal

1) $0 \notin (b)$
2) $x, y \in (b) \rightarrow x \wedge y \in (b)$
3) $x \in (b)$ & $x \leq y \rightarrow y \in (b)$

} to show it's an ideal (use $0, \wedge, \leq$ for general Boolean alg.)

(To show that something is a maximal dual ideal, we must show that it contains everything or its complement)

(b) is the principal dual ideal generated by b.

Suppose $B = 2^I$

If $i \in I$, then $(\{i\})$ is a maximal dual ideal because if $A \subseteq I$, then either $i \in A$ or $i \notin A$

$\Downarrow$ $A \in (\{i\})$ $\quad$ $\Downarrow$ $A' \in (\{i\})$

$$\frac{\prod_{i \in I} a_i}{(\{j\})} \vdash \mathcal{F}$$

$\updownarrow$ $\quad$ $\S\S$ "isomorphic"

$$a_j \vdash \mathcal{F}$$

↑ all that matters is this one factor (the whole ultraproduct reduces to one factor)

If $\mathcal{F}$ is true on a_j, j is fixed. (finite?) Suppose $\mathcal{F}$ is true on a_j. Then the set of coordinates where j is true has $\mathcal{F}$ as an element.

(But there do exist non-trivial maximal dual ideals)

Ultrapower (special case of ultraproduct)

Let $a_i = a$ for all $i \in I$

Then $\frac{\prod_{i \in I} a_i}{D} = \frac{a^I}{D}$

called ultrapower
(in the trivial case of D, this will reduce to a [one of the factors])

Example

$N = \{0, 1, 2, 3, \ldots\}$

$a = \langle N, <, 0 \rangle$ $(= \omega)$ ← (by definition)

$<$: linear ordering of N; 0: least element

$I = N$ $\omega = a_0 = a_1 = a_2 = \ldots$

we're taking the simplest infinite index set

$\frac{\prod \omega^N}{D}$ is a linear ordering, because ω is a linear ordering, then use the fundamental theorem of ultraproducts

Least element:

$[0, 0, 0, 0, \ldots]$ ← equivalence class of numbers which are 0 "almost everywhere"

Every factor has a 2nd element (1), so product does too: anything which is 0 "almost everywhere"

$[1, 1, 1, 1, \ldots]$

∞ $[0, 1, 2, 3, 4, \ldots]$
⋮
2 $[2, 2, 2, 2, 2, \ldots]$
∨
1 $[1, 1, 1, 1, 1, \ldots]$
∨
0 $[0, 0, 0, 0, 0, \ldots]$

} overall structure of linear ordering

If D is non-trivial, then every co-finite set belongs to D.

HW #6 Consider $\frac{\omega^N}{D}$ where D is non-trivial.

a. Show $\frac{\omega^N}{D}$ is a linear ordering.

b. Show $\frac{\omega^N}{D}$ has an infinite element.

c. Show there is no least infinite element (given any ∞ element, show there exists an ∞ element $<$ than it)

d. Show there is no greatest infinite element

e. Show that if x is an infinite element, then there exists an infinite element y such that $x < y$ and there is nothing in between.

f. Show there exists ~~////~~ infinite elements a and b such that there are ∞'ly many elements in between.

If you assume the continuum hypothesis, then the linear ordering doesn't depend on D; it's as big as the continuum (all real numbers)

Rule of first order logic

$\frac{\forall x \mathcal{F}}{\mathcal{F}^x_c}$ } OK if c is a constant

$\frac{\forall x \mathcal{F}}{\mathcal{F}^x_t}$ } not OK if t is a term – must have further restriction

example why it's not OK: (term t is y)

$$\frac{\forall x \exists y (y \neq x)}{\exists y (y \neq y)}$$

$\forall x \exists y (y \neq x)$ ← true

$\exists y (y \neq y)$ ← false

10/24/89

(Final) review of ultraproducts

Elucidation of "almost everywhere"

Let I be any non-empty set.
μ is a finitely additive 0-1 measure on 2^I if:

$\mu: 2^I \to \{0,1\}$ ← 2-member set

$\mu(\phi) = 0$

if $x, y \subseteq I$ & $x \cap y = \phi$ then $\mu(x) + \mu(y) = \mu(x \cup y)$

Does this property apply to 3 sets?

x, y, z

$x \cap y = \phi$
$x \cap z = \phi$
$y \cap z = \phi$ } assume

$\therefore x \cap (y \cup z) = \phi$

$\mu(x \cup y \cup z) = \mu(x) + \mu(y \cup z) = \mu(x) + \mu(y) + \mu(z)$

$\mu(x) = 1 - \mu(I - x)$

Finitely additive 0-1 measures (μ's) $\Leftrightarrow$ maximal max. dual ideal

Suppose μ is such

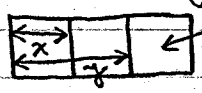
Let $F_\mu = \{x \mid x \subseteq I \;\&\; \mu(x) = 1\}$

Claim: then F_μ is a max. dual ideal

$\phi \notin F_\mu$

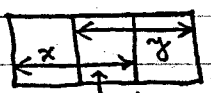
$x \in F_\mu \;\&\; x \subseteq y \to y \in F_\mu$

$\mu(x) = 1 \;\&\; x \subseteq y \to \mu(y) = 1$



complement of y

$x \in F_\mu \;\&\; y \in F_\mu \to x \cap y \in F_\mu$



these are 2 disjoint sets so they can't both have measure 1, which would be true if $\mu(x \cap y) = 0$. Therefore $\mu(x \cap y) = 1$.

Conversely, suppose F is a maximal dual ideal

Define $\mu_F(x) = \begin{cases} 1 & \text{if } x \in F \\ 0 & \text{if } x \notin F \end{cases}$

It is easy to verify that μ_F is a f.a. 0-1 measure.

We can also show:

$$\mu_{(F_\mu)} = \mu$$

$$F_{(\mu_F)} = F$$

μ is said to be <u>trivial</u> (or <u>principal</u>) if $\exists a$, $a \in I$, such that $\mu(\{a\}) = 1$

μ is "concentrated" on a if $\mu(x) = 1 \leftrightarrow a \in x$

μ_a is the trivial measure determined by a

trivial measures

$\updownarrow$

trivial maximal dual ideals

$F_a = \{x \mid a \in x \subseteq I\}$ notation means: $a \in x$ & $x \subseteq I$

Back to <u>First Order Logic</u> (F.O.L.)

(imagine a finite system of axiom schemes and rules for FOL)

$T \vdash \mathcal{F}$ "$\mathcal{F}$ is <u>deducible</u> from T"

means:

there is a finite sequence $\mathcal{F}_0, \ldots, \mathcal{F}_n$ of sentences such that

1) $\mathcal{F}$ is $\mathcal{F}_n$
2) $(i \leq n)$ $\mathcal{F}_i \in T$
   or $\mathcal{F}_i$ is an axiom
   or $\mathcal{F}_i$ is the result of a rule applied to some $\mathcal{F}_j$'s $(j < i)$

$T = \phi$: $\phi \vdash \mathcal{F}$, abbreviated $\vdash \mathcal{F}$, means "$\mathcal{F}$ is provable"

T consistent means $T \not\vdash$ contradiction

↑ syntactic notion, "the weakest notion of truth"

↑ "does not yield"

ϕ is consistent (because we've chosen our axioms and rules this way)

Fundamental Theorem: If S is a consistent set of sentences, then S has a model

↑ formula w/ no free variables

↑ an $\mathcal{L}$-structure which makes all of S true

HW #7 a) Derive ~~completeness~~ compactness from the Fundamental Theorem

b) Derive completeness (Gödel) from the Fundamental Theorem

"if it's true in every $\mathcal{L}$-structure, then it's provable"

Henkinization

$\mathcal{L}$ ← the set of symbols in the language

(Assume $\mathcal{L}$, hence S, is countable for our purposes. In general, it may be uncountable, but then Zorn's lemma or the Axiom of Choice would have to be invoked.)

We define (recursively) $\mathcal{L}_i$ $(i = 0, 1, 2, \ldots)$, a sequence of first order languages.

$\mathcal{L}_0 = \mathcal{L}$

$\mathcal{L}_{i+1} = h(\mathcal{L}_i)$, the Henkinization of $\mathcal{L}_i$

Digression:

Let K be a countable first order

language, i.e., the set of all atomic symbols in K' is countable.
Let $\{\mathcal{F}_i(x) \mid i = 0, 1, 2, \ldots\}$ be a list of all formulas of K whose only free variable is x.

x doesn't stand for a specific free variable; this would be better expressed as "a list of all formulas of K with one free variable" exactly

For each i, create a new individual constant $\underline{c}_i$.
("New" means that $\underline{c}_i \notin K$, and $i \neq j \rightarrow \underline{c}_i \neq \underline{c}_j$)
($\underline{c}_i$ and $\underline{c}_j$ are different symbols; they do not necessarily map to different values in the universe of a model)
Then
$$h(K) = K \cup \{\underline{c}_i \mid i = 0, 1, 2, \ldots\}$$
(end of digression)

Let $\mathcal{L}_\infty = \bigcup_i \mathcal{L}_i$

Define recursively:
$S_0 = S$ (S = set of sentences of $\mathcal{L}$)
$S_{i+1} = h(S_i)$ (Henkinization at step i adds new constants & thus new formulas with one free variable; thus S_{i+1} is needed to Henkinize these new ones as well)

Digression:
$h(S_i)$ is the following set of sentences:
S_i
plus:
Let $\{\mathcal{F}_j(x) \mid j = 0, 1, 2, \ldots\}$ be all formulas of $\mathcal{L}_i$ with one free var.
Add to S_i:
$$\exists x \mathcal{F}_j(x) \rightarrow \mathcal{F}_j(\underline{c}_j) \quad \text{(Henkin axiom)}$$
for each j
(end of digression)

To summarize:

$S_0 = S \qquad \mathcal{L}_0 = \mathcal{L}$

S_0 is from the language $\mathcal{L}_0$

Add new constants to $\mathcal{L}_0$ to get $\mathcal{L}_1$

Add new Henkin axioms to S_0 to get S_1

$\vdots$

Let $\mathcal{L}_\infty = \bigcup_i \mathcal{L}_i$, $\quad S_\infty = \bigcup_i S_i$

Note: if $\mathcal{F}(x) \in \mathcal{L}_\infty$, then

$\exists x\, \mathcal{F}(x) \to \mathcal{F}(c) \qquad \in S_\infty$

↑ for some Henkin constant c not occurring in $\mathcal{F}(x)$

S_∞ is the <u>complete Henkinization</u> of S

Show S_∞ is consistent.

Suffices to show S_i is consistent by induction on i. (because of compactness theorem?)

$S_0 = S$ is consistent (by the initial hypothesis).

Assume S_i is consistent. Show S_{i+1} is consistent.

Suppose $S_{i+1} \vdash$ contradiction, i.e.,

S_i, finitely many Henkin axioms $\vdash$ contradiction

Let's look at the case of 1 Henkin axiom to start with:

$S_i, \exists x\, \mathcal{F}(x) \to \mathcal{F}(c) \vdash$ contra.

(c "$\in$" S_i, c "$\notin$" $\mathcal{F}(x)$)

↑ $\notin$?

Using tautologies,

$S_i \vdash (\exists x\, \mathcal{F}(x) \to \mathcal{F}(c)) \to$ contra

Since it yields a contradiction,

$S_i \vdash \neg(\exists x\, \mathcal{F}(x) \to \mathcal{F}(c))$

<u>Rule of constants</u>: Suppose $T \vdash \mathcal{G}(c)$ $(c \notin T)$ then $T \vdash \forall x\, \mathcal{G}(x)$ (because c is not mentioned in T, so is arbitrary)

$\therefore S_i \vdash \forall x \neg(\exists x \mathcal{F}(x) \to \mathcal{F}(x))$

$S_i \vdash \forall x(\exists x \mathcal{F}(x) \wedge \neg \mathcal{F}(x))$

$S_i \vdash \exists x \mathcal{F}(x) \wedge \forall x \neg \mathcal{F}(x)$ (contradiction)

(we assumed S_i is consistent)

(new derivation?)

$S_i, \exists x \mathcal{F}(x) \vdash \mathcal{F}(c) \to$ contra.

$S_i, \exists x \mathcal{F}(x) \vdash \neg \mathcal{F}(c)$

$S_i, \exists x \mathcal{F}(x) \vdash \forall x \neg \mathcal{F}(x)$

need an axiom: $\exists x \mathcal{F}(x) \to \neg \forall x \neg \mathcal{F}(x)$

$S_i \vdash$ contradiction

10/26/89

Henkinization (cont.)

Review:

Start with S – a consistent set of sentences

Add many new (Henkin) constants $c_{\mathcal{F}(x)}$ ($\mathcal{F}(x)$ ↑ subscript is a formula)

Add (to S) the axiom

$\exists x \mathcal{F}(x) \to \mathcal{F}(c)$ for 2 diff. formulas, use 2 different c's

c is "new"

c does not occur in $\mathcal{F}(x)$

Define a recursion:

$S_0 = S$

$S_{n+1} = h(S_n)$ ← (growth step) this represents ∞ many steps - one for each $\mathcal{F}(x)$

$S_\infty = \bigcup_n S_n$

Suppose $\exists x \mathcal{F}(x) \to \mathcal{F}(c)$ (Henkin axiom) was added to S_n as part of the process of obtaining S_{n+1}. Suppose c does not occur in S_n.

Show consistency (syntactic) of S_∞ (appeal to rule of constants + various tautologies)

Show consistency of S_n by induction on n

Special case:

$S_{n+1} \vdash$ contra

$S_n, H_1 \vdash$ contra

Suppose $S_n, H_1, H_2 \vdash$ contra

Show $S_n, H_1 \vdash$ contra

(Use subinduction on the # of Henkin axioms used in the deduction)

HW #8 Let S be a consistent set of sentences. Let $T \supseteq S$ be an extension of S, with additional sentences and symbols (i.e., extend language). T is said to be a conservative extension of S if for each sentence $\mathcal{F}$ in the language of S, $T \vdash \mathcal{F}$ only if $S \vdash \mathcal{F}$. (In other words, T does not prove anything new.) Show S_∞ is a conservative extension of S.

The next step is to extend S_∞ to a maximum consistent set of sentences (to be called $S_{\infty\infty}$).

$S_{\infty 0} = S_\infty$

$$S_{\infty\, n+1} = \begin{cases} S_{\infty n} \cup \{\mathcal{F}_n\} & \text{if this combination is consistent} \\ S_{\infty n} \cup \{\neg\mathcal{F}_n\} & \text{otherwise} \end{cases}$$

(assumes $\mathcal{F}_1, \mathcal{F}_2, \ldots$ is a countable list of all sentences)

Definition of $\mathcal{A}$, the proposed model for S

Started with: $\mathcal{L}$ was language of S
$\mathcal{L}_\infty$ was language {of S_∞ / of $S_{\infty\infty}$}

Let c and d be Henkin constants.
$c \sim d$ means $S_{\infty\infty} \vdash \underline{c} = \underline{d}$, i.e., $(\underline{c} = \underline{d}) \in S_{\infty\infty}$

(every derivation has length 1, since all sentences are in $S_{\infty\infty}$)

$$S_{\infty\infty} \vdash \mathcal{G}$$
$$\Updownarrow$$
$$\mathcal{G} \in S_{\infty\infty}$$

Show $c \sim d$ is an equivalence relation

$\underline{c} \sim \underline{c}$ $\quad (\underline{c} = \underline{c}) \in S_{\infty\infty}$ } (make this an axiom, or derive it from one)

Digression:
We know "from common sense" that
$\forall x \mathcal{F} \rightarrow \mathcal{F}_t^x$ where t is a term
($\mathcal{F}_t^x$: result of substituting t for all free x's in $\mathcal{F}$)

But this has a problem:
Suppose $\mathcal{F}$ is $\exists y\, (y \neq x)$
$\forall x \mathcal{F}$ is OK: $\forall x \exists y\, (y \neq x)$

Suppose t is y

Then $\mathcal{F}_t^x$ is $\exists_y (y \neq y)$ ← wrong

We need a "proviso":

$\mathcal{F}_t^x$ is OK if no free occurrence of x sits inside the scope of a quantifier of a variable that occurs in t.

A way to remember this is:

"free must stay free"

↑ variable of t ↑ remain free in $\mathcal{F}_t^x$

(End of digression)

Create an axiom: $\forall x\,(x=x)$

" " axiom: $\forall x\,\mathcal{F} \to \mathcal{F}_t^x$ (subject to proviso)

$\therefore \forall x\,(x=x) \to \underline{c}=\underline{c}$

By modus ponens, $\underline{c}=\underline{c}$

If $c \sim d$, then $d \sim c$

Axiom: $\forall x \forall y\,(x=y \to y=x)$

Apply $\forall x\,\mathcal{F} \to \mathcal{F}_t^x$ twice

If $c \sim d$ and $d \sim e$, then $c \sim e$

Axiom: $\forall x \forall y \forall z\,(x=y \wedge y=z \to x=z)$

(Now we've shown that $c \sim d$ is an equivalence relation)

Let $[\underline{c}] = \{\underline{d} \mid \underline{d} \sim \underline{c}\}$ set of all Henkin constants that are equivalent to c

↑ an equivalence class

Let $A = \{[\underline{c}] \mid c \text{ is a Henkin constant}\}$

↑ universe of our model

We need to add relations, functions, and distinguished elements (constants) to complete the definition of model a

$$R^a([\underline{c}_1],\ldots,[\underline{c}_m]) \Leftrightarrow R(\underline{c}_1,\ldots,\underline{c}_m) \in S_{\infty\infty}$$

$$f^a([\underline{c}_1],\ldots,[\underline{c}_m]) = [\underline{c}_{m+1}]$$

$$\Leftrightarrow f(\underline{c}_1,\ldots,\underline{c}_m) = \underline{c}_{m+1} \in S_{\infty\infty}$$

Let $\underline{d}$ be an individual constant of $\mathcal{L}$ in $\mathcal{L}_1$ and S_1:

$\exists x(x=\underline{d}) \rightarrow (\underline{c}=\underline{d})$ (Henkin axiom in S_1)

claim: $\exists x(x=\underline{d}) \in S_{\infty\infty}$

then $(\underline{c}=\underline{d}) \in S_{\infty\infty}$ ∴ the individual constant $\underline{d}$ in $\mathcal{L}$ is equivalent to something in some equiv. class

$d^a = [\underline{c}]$

→ Suppose $S_n, \exists x\mathcal{F}(x) \rightarrow \mathcal{F}(c) \vdash$ contradiction

$S_n \vdash \exists x\mathcal{F}(x) \wedge \neg\mathcal{F}(c)$ tautological reasoning

$\therefore S_n \vdash \exists x\mathcal{F}(x)$, $S_n \vdash \neg\mathcal{F}(c)$

$\leftrightarrow S_n \vdash \forall x\neg\mathcal{F}(x)$ rule of constants

↑ want these to be contradictory

Let $\exists$ be an abbreviation for $\neg\forall\neg$; assume $\forall$ is primitive

$?\mathcal{F}(\star) \rightarrow \exists x\mathcal{F}(x)$

$\mathcal{F}(\star) \rightarrow \neg\forall x\neg\mathcal{F}(x)$

$\forall x\neg\mathcal{F}(x) \rightarrow \neg\mathcal{F}(\star)$ ← special case of previous axiom; OK if proviso holds

$x = \underline{d}$ is $\mathcal{F}(x)$, d is t

$\underline{d} = \underline{d} \to \exists x (x = \underline{d})$

Last step: Show $\mathcal{A}$ is a model of S

Prove: $\mathcal{A} \vDash \mathcal{F} \iff \mathcal{F} \in S_\infty$
($\mathcal{A}$ "makes $\mathcal{F}$ true")

for all sentences $\mathcal{F} \in \mathcal{L}_\infty$

By induction:

Case 0: $\mathcal{F}$ could be $R(t_1, \ldots, t_n)$ where t_i is a constant term

$t_i \sim c_i$ "every constant term t_i is equivalent to some Henkin constant c_i"

$(t_i = c_i) \in S_\infty$

We know $t = c$, know $R(t)$

$t = c, R(t) \vdash R(c)$

need: $t = c \to (R(t) \to R(c))$

new axiom: $\forall x \forall y (x = y \to (R(x) \to R(y)))$

$(R(t) \to R(c)) \in S_\infty$

Assume $R(t) \in S_\infty$

then $R(c) \in S_\infty$

then $R^{\mathcal{A}}([c]) \in S_\infty$

which is the same as saying $\mathcal{A} \vDash R(c)$

reverse argument also holds

We also need an axiom for functions:

$\forall x \forall y (x = y \to f(x) = f(y))$

$\mathcal{F}$ could be $t_1 = t_2$

$\downarrow$

$c_1 = c_2$ OK

Case 1: $\mathcal{F}_1 \wedge \mathcal{F}_2 \in S_{\infty\infty}$

$\mathcal{F}_1, \mathcal{F}_2 \in S_{\infty\infty}$ $\quad \downarrow \uparrow$ reversible

$a \vdash \mathcal{F}_1 \quad a \vdash \mathcal{F}_2$

$a \vdash \mathcal{F}_1 \wedge \mathcal{F}_2$

Case 2: $\neg\mathcal{G} \in S_{\infty\infty}$

$\mathcal{G} \notin S_{\infty\infty}$ $\quad \uparrow$ use maximality of $S_{\infty\infty}$ to get reverse

$a \nvdash \mathcal{G}$

$a \vdash \neg\mathcal{G}$

Case 3: Quantifier

$a \vdash \exists x \mathcal{F}(x)$ $\leftarrow$ assumption ~~what we want~~

$a \vdash \mathcal{F}(c)$ $\quad [c] \in A$

$\downarrow$ by induction hypothesis

$\mathcal{F}(c) \in S_{\infty\infty}$

? $\downarrow$ need an axiom?

$\exists x \mathcal{F}(x) \in S_{\infty\infty}$

Reversing:

$\exists x \mathcal{F}(x) \in S_{\infty\infty}$

$\exists x \mathcal{F}(x) \to \mathcal{F}(c) \in S_{\infty\infty}$ Henkin axiom

$\mathcal{F}(c) \in S_{\infty\infty}$

$a \vdash \mathcal{F}(c)$ by induction hypothesis

$a \vdash \exists x \mathcal{F}(x)$ rule of constants

Open question here: Why didn't we need the axiom

$\forall x (\mathcal{F} \to \mathcal{G}) \to (\forall x \mathcal{F} \to \forall x \mathcal{G})$

from Bell + Machover?

HW #9 Give a nice proof of the fundamental theorem

10/31/89

Generalization Rule

Gen Rule: if $T \vdash \mathcal{F}(x)$
then $T \vdash \forall x \mathcal{F}(x)$
where T doesn't contain x freely (or T is a set of sentences)

Axiom: $\forall x H(x) \to H(t)$, proviso on t
$\neg H(t) \to \neg \forall x H(x)$
$H(t) \to \exists x H(x)$
$H(x) \to \exists x H(x)$

Proof by induction on # of steps in deduction (on length of derivation)

$\mathcal{F}(x)$ $\quad$ $\forall x \mathcal{F}(x)$

$l=1$: $\mathcal{F}(x)$ is an axiom
(universal closure of an axiom is a theorem, by the rule of constants)

A is an axiom – show $\forall x A$
$\forall x$ (tautology)
$\forall x (\mathcal{F} \vee \neg \mathcal{F})$

$A(x)$ is an axiom – show $\vdash \forall x A(x)$
If $A(x)$ is an axiom, then A^c_x (i.e., $A(c)$) is an axiom.
By rule of constants, $\forall x A(x)$ is provable.

$l > 1$:

$\mathcal{F}(x)$ ⋮ $\mathcal{G}(x,c)$ ← change y to c in all axioms during deduction

⋮

$\forall x\, \mathcal{G}(x,c)$ ↑

$\mathcal{G}(d,c)$ (?)

$\forall y\, \mathcal{G}(y,c)$ ↓

$\forall x \forall y\, \mathcal{G}(y,x)$

$\forall y\, \mathcal{G}(x,y)$ rule of constants

Importance of no free variable in Γ

Suppose $\mathcal{F}(x) \vdash \forall x \mathcal{F}(x)$ ← this is a false rule

$\vdash \mathcal{F}(x) \to \forall x \mathcal{F}(x)$

$\vdash \forall x (\mathcal{F}(x) \to \forall x \mathcal{F}(x))$

$\vdash \mathcal{F}(d) \to \forall x \mathcal{F}(x)$ not valid

---

Theorem If $\Gamma \vdash \mathcal{F}$, then $\mathcal{A} \models \mathcal{F}$ for every $\mathcal{A}$ which is a model of Γ (Γ is a set of sentences, $\mathcal{F}$ is a sentence)

Pf by induction on length of derivation

✓ every axiom is true in every structure

induction hypothesis: ⋮ $\mathcal{G}(c)$ c is not mentioned in Γ

⋮ $\forall x\, \mathcal{G}(x)$ ← this is $\mathcal{F}$

⋮

$\mathcal{A} \models \mathcal{G}(\underline{a})$ for every $\underline{a} \in A$

$\mathcal{A} \models \forall x\, \mathcal{G}(x)$

} quantifier case

(other cases straightforward...)

Deduction Theorem If $\mathcal{F} \vdash \mathcal{G}$, then $\vdash \mathcal{F} \to \mathcal{G}$

($\mathcal{F}$ and $\mathcal{G}$ are formulas; no free variable of $\mathcal{F}$ is in $\mathcal{G}$)

Proof: Add $\mathcal{F}$ as antecedent in each step of deduction of $\mathcal{G}$

K	$\vdash \mathcal{F} \to K$ tautology if K is an axiom
⋮	⋮
$H(c)$	$\vdash \mathcal{F} \to H(c)$ assume x not free in $\mathcal{F}$
$\forall x H(x)$	$\vdash \forall x (\mathcal{F} \to H(x))$ rule of constants
	$\vdash \mathcal{F} \to \forall x H(x)$ since $\mathcal{F}$ doesn't mention x
⋮	⋮
$\mathcal{G}$	$\vdash \mathcal{F} \to \mathcal{G}$

(Stronger) Gen Rule: if $T \vdash \mathcal{F}(x)$ then $T \vdash \forall x \mathcal{F}(x)$ (x not free in T)

(Stronger) Deduction Rule: if $T, \mathcal{F} \vdash \mathcal{G}$ then $T \vdash \mathcal{F} \to \mathcal{G}$

Some standard quantifier manipulation rules

Suppose x is not free in $\mathcal{F}$ (for ①, ②, ⑤, ⑥)

① $\forall x (\mathcal{F} \to \mathcal{G}) \leftrightarrow \mathcal{F} \to \forall x \mathcal{G}$

② $\forall x (\mathcal{G} \to \mathcal{F}) \leftrightarrow (\exists x \mathcal{G}) \to \mathcal{F}$

③ $\exists x (\mathcal{F} \vee \mathcal{G}) \leftrightarrow (\exists x \mathcal{F}) \vee (\exists x \mathcal{G})$

④ $\forall x (\mathcal{F} \wedge \mathcal{G}) \leftrightarrow (\forall x \mathcal{F}) \wedge (\forall x \mathcal{G})$

⑤ $\exists x (\mathcal{F} \to \mathcal{G}) \leftrightarrow \mathcal{F} \to \exists x \mathcal{G}$

⑥ $\exists x (\mathcal{G} \to \mathcal{F}) \leftrightarrow \forall x \mathcal{G} \to \mathcal{F}$

Proof of $\forall x (\mathcal{F} \to \mathcal{G}) \to (\mathcal{F} \to \forall x \mathcal{G})$ (x not free in $\mathcal{F}$)

Given $\forall x (\mathcal{F} \to \mathcal{G})$, show $\mathcal{F} \to \forall x \mathcal{G}$

$\forall x (\mathcal{F} \to \mathcal{Q})$
$\mathcal{F} \to \mathcal{Q}(c)$ (c does not occur in $\mathcal{F}$)
$\mathcal{F} \vdash \mathcal{Q}(c)$
$\mathcal{F} \vdash \forall x\, \mathcal{Q}(x)$ rule of constants
$\vdash \mathcal{F} \to \forall x\, \mathcal{Q}(x)$

Prenex normal form

(string of quantifiers) (formula without quantifiers)

Claim: For each $\mathcal{F}$, there is a prenex normal $\mathcal{Q}$ such that $\vdash \mathcal{F} \leftrightarrow \mathcal{Q}$

e.g.: $\forall u\, \exists v\, P \to \forall u\, \exists v\, Q$

u is not free

$\updownarrow$

$\forall u\, [\forall u\, \exists v\, P \to \exists v\, Q]$ rule ①

$\forall u\, \exists v\, [\forall u\, \exists v\, P \to Q]$ rule ⑤

$\forall x\, \exists y\, P' \to Q$ rename variables

P is $R(u,v)$

P' is $R(x,y)$

$\forall u\, \exists v\, \exists x\, \forall y\, (P' \to Q)$ ← prenex normal form (answer)

The renaming scheme we used was:

$\mathcal{F}(x)$, y does not occur in $\mathcal{F}(x)$
$\vdash \mathcal{F}(x) \leftrightarrow \mathcal{F}(y)$

$\mathcal{F}(x)$ ⋯ ← ? How do we get from $\mathcal{F}(x)$ to $\mathcal{F}(c)$ (unresolved in classroom)

$\vdots$ $\mathcal{F}(c)$

$\mathcal{F}(y)$ ⋯

11/2/89

First order logic (continued)

Interpolation Theorem: (Assume $\mathcal{F}$, $\mathcal{G}$, and $\mathcal{L}$ are sentences.) Suppose $\vdash \mathcal{F} \to \mathcal{G}$. Then there is an $\mathcal{L}$ such that $\vdash \mathcal{F} \to \mathcal{L}$, $\vdash \mathcal{L} \to \mathcal{G}$, and every non-logical symbol of $\mathcal{L}$ occurs in both $\mathcal{F}$ and $\mathcal{G}$. (and equality?)

Note: If $\mathcal{F}$ and $\mathcal{G}$ have no non-logical symbols in common and $\vdash \mathcal{F} \to \mathcal{G}$, then either $\vdash \neg \mathcal{F}$ ($\mathcal{F}$ is a contradiction) or $\vdash \mathcal{G}$ ($\mathcal{G}$ is provable).

Proof: Assume $\vdash \mathcal{F} \to \mathcal{G}$ and $\mathcal{F}$ and $\mathcal{G}$ have nothing in common.

Suppose $\not\vdash \neg \mathcal{F}$ and suppose $\not\vdash \mathcal{G}$
↖ "I can't prove"

Show there is a structure $\mathcal{A}$ such that $\mathcal{A} \models (\mathcal{F} \wedge \neg \mathcal{G})$ ("in $\mathcal{A}$, $\mathcal{F}$ is true and $\mathcal{G}$ is false).

The Fundamental Theorem says:

$\Gamma \vdash \mathcal{F}$ { Γ is a set of sentences; $\mathcal{F}$ is a sentence

$\Updownarrow$

For all $\mathcal{A}$, if $\mathcal{A}$ is a model of Γ, then $\mathcal{A} \models \mathcal{F}$

So by the Fundamental Theorem, if $\not\vdash \mathcal{H}$, there is a structure in which $\mathcal{H}$ is false, i.e., $\neg \mathcal{H}$ is true. (If $\mathcal{H}$ were true in every structure, then by the Fundamental Theorem $\mathcal{H}$ would be provable)

Therefore there (must be) are structures $\mathcal{A}_0$ and $\mathcal{A}_1$ such that

$\mathcal{A}_0 \models \mathcal{F}$ $\quad$ $\mathcal{A}_1 \models \neg \mathcal{G}$

The idea is to try to combine $\mathcal{A}_0$ and $\mathcal{A}_1$ in such a way that the conjunction of $\mathcal{F}$ and $\neg \mathcal{G}$ is true. A t...

Try to build $\mathcal{A}$ by a Henkin argument
Try to build a model of $\mathcal{F} \wedge \neg \mathcal{G}$

$\not\vdash \neg \mathcal{F}$ $\quad$ $\not\vdash \mathcal{G}$ $\quad$ ($\mathcal{F}, \neg \mathcal{G}$ are consistent (means))

$\mathcal{F}$ and $\mathcal{G}$ have no non-logical symbols in common (not even equality?)

build a model $\mathcal{A}$ of $\mathcal{F}$ $\quad$ build a model $\mathcal{B}$ of $\neg \mathcal{G}$

$\mathcal{L}_\mathcal{A}$ $\quad$ $\mathcal{L}_\mathcal{B}$

these two languages have nothing in common but the universe

Try to build structures $\mathcal{A}$ and $\mathcal{B}$ simultaneously with the same universe

Henkinizing $\mathcal{L}_\mathcal{A}$ $\quad$ Henkinizing $\mathcal{L}_\mathcal{B}$

?

(there is a problem with equality, if $\mathcal{F}$'s universe has one element but $\neg \mathcal{G}$'s has two)

(proof postponed)

Applications of Fundamental Theorem

① Let T be a countable set of sentences. If T has a model, then T has a countable model.

Proof: T is consistent (because it has a model). Look at the Henkin construction of model $\mathcal{A}$ for T. $\mathcal{A}$ is automatically countable. (There were countably many Henkin constants, one for each formula.)

Skolem's paradox: Set theory ZFC has countably many axioms. By ①, ZFC has a countable model M. A theorem in ZFC is:

ZFC $\vdash$ "the set of real numbers is uncountable"

i.e., $M \models$ "there exists an uncountable set"

but M is countable. (Solution: looking from inside M, the set is "uncountable" from M's point of view — but the set which describes M is countable) (?)

② Let $\mathcal{A}$ and $\mathcal{B}$ be "similar" structures. (Similar means they are both $\mathcal{L}$-structures for the same $\mathcal{L}$.)

$\mathcal{A} \subseteq \mathcal{B}$ "$\mathcal{A}$ is a substructure of $\mathcal{B}$"

means $A \subseteq B$

$R^{\mathcal{A}} \subseteq R^{\mathcal{B}}$

if $f^{\mathcal{A}}(a_0, \ldots, a_m) = a_{m+1}$, then $f^{\mathcal{B}}(a_0, \ldots, a_m) = a_{m+1}$

$c^{\mathcal{A}} = c^{\mathcal{B}}$

e.g.: groups and subgroups

$\mathcal{A} \prec \mathcal{B}$ "$\mathcal{A}$ is an elementary substructure of $\mathcal{B}$"

means $\mathcal{A} \subseteq \mathcal{B}$

$\mathcal{A} \models \mathcal{F}(a_0, \ldots, a_m) \Leftrightarrow \mathcal{B} \models \mathcal{F}(a_0, \ldots, a_m)$

($\Leftarrow$ is the important direction)

e.g.: if $\mathcal{A}$ and $\mathcal{B}$ are algebraicly closed fields, and $\mathcal{A} \subseteq \mathcal{B}$, then $\mathcal{A} \prec \mathcal{B}$

(Assume $\mathcal{L}$ is countable.) For any $\mathcal{B}$, there exists a countable $\mathcal{A} < \mathcal{B}$

11/7/89

Return to Craig's Interpolation Theorem:

If $\vdash (\mathcal{F} \to \mathcal{G})$, then there is an $\mathcal{L}$ such that $\vdash (\mathcal{F} \to \mathcal{L})$ and $\vdash (\mathcal{L} \to \mathcal{G})$ and every non-logical symbol of $\mathcal{L}$ occurs in both $\mathcal{F}$ and $\mathcal{G}$

(Assume $\mathcal{F}$ is not true in any finite model and $\mathcal{G}$ is not false in any finite model)

Note: If $\mathcal{F}$ and $\mathcal{G}$ have no non-logical symbols in common, then either $\mathcal{F}$ is a contradiction or $\mathcal{G}$ is provable.

Suppose not. Then there is a model of $\mathcal{F}$: $\mathcal{A} \models \mathcal{F}$ and of $\neg\mathcal{G}$: $\mathcal{B} \models \neg\mathcal{G}$.
$\mathcal{A}$ and $\mathcal{B}$ are infinite. It is safe to assume $\mathcal{A}$ and $\mathcal{B}$ are countably infinite. (Because if $\mathcal{F}$ and $\neg\mathcal{G}$ have infinite models, then they have countably infinite models by theorem from last lecture.)
We can assume $A = B = \omega = \{0, 1, 2, \ldots\}$ (universes of $\mathcal{A}$ and $\mathcal{B}$)
Define the structure $\mathcal{C}$:

$C = \omega$
relations of $\mathcal{A}$ and $\mathcal{B}$
functions of $\mathcal{A}$ and $\mathcal{B}$
distinguished elements of $\mathcal{A}$ and $\mathcal{B}$
} it is OK to combine them because they have nothing in common

$\mathcal{C} \models \mathcal{F}$ because $\mathcal{A} \models \mathcal{F}$
$\mathcal{C} \models \mathcal{G}$ because $\mathcal{B} \models \neg\mathcal{G}$

$\therefore \mathcal{C} \models \mathcal{F} \wedge \neg \mathcal{G}$. But we assumed $\vdash \mathcal{F} \rightarrow \mathcal{G}$, i.e., $\vdash \neg(\mathcal{F} \wedge \neg \mathcal{G})$ (contradiction)

Proof of Interpolation Theorem:

Suppose not. Our goal is to build a model $\mathcal{M}$ such that $\mathcal{M} \models (\mathcal{F} \wedge \neg \mathcal{G})$; if we can do this, we've established a contradiction, since $\vdash \mathcal{F} \rightarrow \mathcal{G}$ was assumed.

Set up Henkin constructions for $\mathcal{F}$ and for $\neg \mathcal{G}$. (It is OK to assume $\mathcal{F}$ is not a contradiction and $\mathcal{G}$ is not a tautology — otherwise the proof is trivial.) (Therefore it is OK to set up Henkin constructions for $\mathcal{F}$ and $\neg \mathcal{G}$.)

Henkin construction for $\mathcal{F}$	Henkin construction for $\neg \mathcal{G}$
$\mathcal{F}$	$\neg \mathcal{G}$
Henkenize — add constants and axioms w/ respect to symbols of $\mathcal{F}$	Henkenize — add constants and axioms w/ respect to symbols of $\neg \mathcal{G}$

Extend to maximally consistent sets of sentences
Consider K, the very first sentence

Add either K or $\neg K$ to $\mathcal{F}$ such that the result is consistent	Add either K or $\neg K$ to $\neg \mathcal{G}$ such that the result is consistent

Suppose it's not possible. Then
either $\mathcal{F}, K \vdash$ contra. (A) or $\neg \mathcal{G}, K \vdash$ contra. (C)
and
either $\mathcal{F}, \neg K \vdash$ contra. (B) or $\neg \mathcal{G}, \neg K \vdash$ contra. (D)

There are 4 cases to consider.

Ⓐ & Ⓑ $\Rightarrow \mathcal{F}$ is a contradiction; but we assumed not, so we can eliminate this case.

Ⓒ & Ⓓ $\Rightarrow \neg\mathcal{G}$ is a contradiction; but we assumed not, so we can eliminate this case.

So the only two possibilities are Ⓐ & Ⓓ or Ⓑ & Ⓒ.

Look at Ⓐ & Ⓓ. Suppose $\mathcal{F}, K \vdash$ contra and $\neg\mathcal{G}, \neg K \vdash$ contra. Then

$$\vdash \mathcal{F} \to \neg K, \quad \vdash \neg K \to \mathcal{G}$$

$\neg K$ looks like an interpolant.

(Similarly for Ⓑ & Ⓒ; in this case K looks like an interpolant.)

After the Henkinization, make a list $K_0, K_1, \ldots$ of all sentences all of whose sentences are common to both.

Then either K_0, or $\neg K_0$, can be added consistently to both Henkin constructions. Otherwise there is an interpolant (contrary to initial assumption that an interpolant doesn't exist; so proof is done -- otherwise continue construction)

$\mathcal{F}$	$\neg\mathcal{G}$
Henkin axioms (only symbols in $\mathcal{F}$)	Henkin axioms (only symbols in $\neg\mathcal{G}$)

settle the same way all sentences with symbols common to $\mathcal{F}$ and $\neg\mathcal{G}$

? not clear

Digression (technicality) - Suppose
$\mathcal{F} \to \neg K_0(c)$ $\quad \neg K_0(c) \to \mathcal{G}$
where c is a Henkin constant of $\mathcal{F}$, but not of $\mathcal{G}$
$\mathcal{F} \to \exists x \neg K_0(x)$ $\quad \exists x \neg K_0(c) \to \mathcal{G}$

remaining sentences are settled consistently (because they have at least one symbol not in $\neg\mathcal{Q}$)	remaining sentences are settled consistently (because they have at least one symbol not in $\mathcal{F}$)
$\therefore \mathcal{A} \vdash \mathcal{F}$	$\therefore \mathcal{B} \vdash \neg\mathcal{Q}$

Try to make $\mathcal{C}$

$\mathcal{C} = A = B = \omega = \{0, 1, 2, 3, \ldots\}$

Relations of $\mathcal{C}$ are those of $\mathcal{A}$ and $\mathcal{B}$

"If a relation occurred on both sides, those relations were built up simultaneously - $\mathcal{A}$ and $\mathcal{B}$ agree where it "matters"

$\left.\begin{array}{l} \therefore \mathcal{C} \vdash \mathcal{F} \\ \mathcal{C} \vdash \neg\mathcal{Q} \end{array}\right\} \therefore \mathcal{C} \vdash \mathcal{F} \wedge \neg\mathcal{Q}$, contrary to assumption that $\vdash \mathcal{F} \rightarrow \mathcal{Q}$

Look back at our assumptions:

Assumed $\mathcal{F}$ has no finite model
Assumed $\neg\mathcal{Q}$ has no finite model

Assumption could be changed to:
$\mathcal{F}$ and $\neg\mathcal{Q}$ have ∞ models
From last class, we know if something has an infinite model, it has a countably infinite model.

Robinson's Joint Consistency

T_1 is a theory in language $\mathcal{L}_1$
T_2 is a theory in language $\mathcal{L}_2$
} countable theories

T_1 is consistent
T_2 is consistent

$T_1 \cup T_2$ is consistent when: $\underbrace{T_1 \cap T_2 \text{ is consistent}}$

?

must look it up –
may not be quite right

A theory is a set S of sentences such that if $S \vdash \mathcal{F}$, then $\mathcal{F} \in S$

Proof of joint consistency is similar to interpolation proof

HW#10	State and sketch a proof of Robinson's joint consistency

---

11/9/89

Last farewell to First Order Logic and (in particular) interpolation

Review: $\vdash \mathcal{F} \to \mathcal{G}$

Assume no $\mathcal{L}$ such that ($\vdash \mathcal{F} \to \mathcal{L} \to \mathcal{G}$ and $\mathcal{L}(\mathcal{L}) \subseteq \mathcal{L}(\mathcal{F}) \cap \mathcal{L}(\mathcal{G})$)

Assumption so far: $\mathcal{F}$ and $\neg\mathcal{G}$ have ∞ (i.e., countably ∞) models

$\mathcal{F}$	$\neg\mathcal{G}$
universe is ∞	universe is ∞
Henkinization for $\mathcal{L}(\mathcal{F})$	Henkinization for $\mathcal{L}(\mathcal{G})$

(11/21/89) "We need an additional condition – add K or $\neg K$ in such a way that neither is an interpolant"

settle all sentences from $\mathcal{L}(\mathcal{F}) \cap \mathcal{L}(\mathcal{G})$	settle all sentences from $\mathcal{L}(\mathcal{F}) \cap \mathcal{L}(\mathcal{G})$
settle all remaining sentences (which have a symbol in common with $\mathcal{L}(\mathcal{G})$)	settle all remaining sentences (which have a symbol in common with $\mathcal{L}(\mathcal{F})$)

Example:

$a_{\mathcal{F}}$ $\quad \langle \omega, <^{a_{\mathcal{F}}} \rangle$

$a_{\neg\mathcal{G}}$ $\quad \langle \omega, <^{a_{\neg\mathcal{G}}} \rangle$

$c_1 < c_2$ is settled here

↑ symbol in both languages

settled here

$a_{\mathcal{F}}$ $\quad \langle \omega, <^{a_{\mathcal{F}}}, R^{a_{\mathcal{F}}} \rangle$

$a_{\neg\mathcal{G}}$ $\quad \langle \omega, <^{a_{\neg\mathcal{G}}}, S^{a_{\neg\mathcal{G}}} \rangle$

$R \in \mathcal{L}(\mathcal{F}) - \mathcal{L}(\mathcal{G}) \overset{?}{<} \mathcal{L}(\mathcal{F}) \cap \mathcal{L}(\mathcal{G})$

$S \in \mathcal{L}(\mathcal{G}) - \mathcal{L}(\mathcal{F})$

a $\quad \langle \omega, <^{a_{\mathcal{F}}}, R^{a_{\mathcal{F}}}, S^{a_{\neg\mathcal{G}}} \rangle$

Henkin constants have to be quantified out

$K \in \mathcal{L}(\mathcal{F}) \cap \mathcal{L}(\mathcal{G})$

Add K to both or add $\neg K$ to both

Suppose it's not possible:

$\mathcal{F}+ \vdash \neg K$ or $\neg\mathcal{G}+ \vdash \neg K$

and

$\mathcal{F}+ \vdash K$ or $\neg\mathcal{G}+ \vdash K \leftarrow (\neg\mathcal{G})\cap+ \vdash K$

Diagonals are the only possible cases ($\mathcal{F}$ not contradiction; $\mathcal{G}$ not tautology)

examination of size of universe; unclear; postponed

$\mathcal{F} + \vdash \neg K$ · $\neg K \vdash \mathcal{G} \vee \neg +$

$\mathcal{F} \wedge |v| \geq 7$ $\mathcal{G} \vee \neg(|v| \geq 7)$

↑ size of universe

universe must have at least 6 elements?

I is $(|v| \geq 7) \rightarrow \neg K$

$\vdash (\mathcal{F} \wedge (|v| \geq \overset{2?}{7})) \rightarrow I$ $\vdash I \rightarrow (\mathcal{G} \vee \neg(|v| \geq \overset{2?}{7}))$

one element model specification up to symbols in both $\mathcal{F}$ and $\mathcal{G}$

Recursion Theory

Outline

① Definition of partial recursive functions

② Develop pure recursion theory
- recursively enumerable sets
- recursion (notion of)
- fixed point theorem
- non-recursive sets
- simple sets

③ Applications of recursion theory
- Gödel's incompleteness
- Church's undecidability of first-order logic (FOL)

Make-up class will be held Tues. Dec. 19th

11/16/89

Recursive Functions

History: It took a long time to arrive at a definition of computable function.

Diagonal argument: used to refute many supposed definitions

Gödel: cannot effectively define the class of effectively computable functions
- Imagine some such definition; list all such functions:

$f_0(x)$
$f_1(x)$
$f_2(x)$
⋮
$f_k(x)$
⋮

Regard $f_k(x)$ as a computable function of k and x. Let $g(x) = f_x(x)+1$.
Then $g(x) = f_{k_0}(x)$ for some k_0.
But $g(k_0) = f_{k_0}^{k_0}(k_0)+1 = f_{k_0}(k_0)$ (contradiction)

Gödel: One can give an effective definition of the class of all effectively computable partial functions (a function whose domain $\subsetneq \mathbb{N}$)

i.e., There is an effective procedure for $f(x)$, but for some values of x it may not terminate or it may terminate in nonsense

---

History

Church's Thesis:
Intuitively computable functions are the same as the λ-computable functions
↑ (we will not cover the definition of this)

Gödel viewed Turing machines as a (philosophical) "proof" of Church's thesis

---

Definition of partial recursive function

0) Pairing functions $N^2 \leftrightarrow N$

$p(x,y)$ codes the pair
$q_0(p(x,y)) = x$
$q_1(p(x,y)) = y$
} decodes the pair
} allows us to treat pairs of numbers as numbers

e.g.: $p(x,y) = 2^{x+1} \cdot 3^{y+1}$

$q_0(z) =$ "find the highest power of 2 that divides z"
$= q_0(2^{n_2} \cdot 3^{n_3} \cdot \dots)$
$= n_2 - 1$

$q_1(z) = n_3 - 1$

Coding (Gödel numbering) – can represent any finite sequence of numbers with numbers (we could also use polynomials instead of exponentials to "reduce complexity")

1) Constant functions
$f(x_1, \dots, x_n) = c$ c is a constant

2) Projection function
$f(x_1, \dots, x_m) = x_j$

3) Successor function
$f(x_1, \dots, x_m) = x_1'$ $(= x_1 + 1)$ ← this is where the actual computation is done (increment by 1)

4) Scheme of composition
$f(x_1, \dots, x_m) = g(h_1(x_1, \dots, x_m), \dots, h_m(x_1, \dots, x_m))$

5) Closure condition or Enumeration Scheme

$f(e, \underbrace{x_1, \ldots, x_n}_{\text{auxiliary arguments}}) =$ result of applying e'th computable function to $x_1, \ldots, x_n$

We want to interpret e as a computable function. So, we must assign indices to all computable functions.

The index of a partial recursive function: an n-tuple that identifies the scheme (0-5) that gave rise to the function, and the number of arguments.

scheme

1) The index for a constant function is $\langle 1, n, c \rangle$
2) $\langle 2, n, j \rangle$ ← projecting j'th coordinate
3) $\langle 3, n \rangle$ ← number of arguments in successor function
4) $\langle 4, m, \langle\rangle, \underbrace{\langle\rangle, \ldots, \langle\rangle}_{m \text{ indices for functions with } n \text{ arguments}} \rangle$

↑ composition

↑ index for function with m arguments

5) $\langle 5, m, ? \rangle$?

$\langle a_1, \ldots, a_n \rangle$ = code number for finite sequence of integers $a_1, \ldots, a_n$

$\langle a_1, \ldots, a_n \rangle$ is $2^{a_1+1} \cdot 3^{a_2+1} \cdot \ldots \cdot p_n^{a_n+1}$ $\quad p_1=2, p_2=3, p_3=5, \ldots,$ p_n = nth prime

0) index needs some elaboration
↳ pairing (maybe coding and decoding finite sequences) } ?

Suppose e is an index. Then $\{e\}$ is the partial recursive function whose index is e.

$\{e\}(x_1, \ldots, x_n)$

(e may not be the index of anything)

5) $f(e, x_1, \ldots, x_n) \simeq \{e\}(x_1, \ldots, x_n)$

$f \simeq g$ means the graph of f = graph of g

$\forall x$ if $f(x)$ is defined, then $g(x)$ is defined and $f(x) = g(x)$; similarly, if $g(x)$ is defined, then ...

Example: $g(x) \simeq \{x\}(x) + 1$

$g(x) \simeq \{e_0\}(x)$

$\{e_0\}(e_0) + 1 \simeq \underbrace{\{e_0\}(e_0)}_{\text{not defined}}$

11/21/89

Review
0) coding ("pairing")
1) constant
2) projection
3) successor
4) composition
5) enumeration (function parameters)

index is $\langle 5, m \rangle$ (m = # args.)

$\{e\}(x_1, \ldots, x_m)$ — partial recursive function with index e

assume that we have the right number of arguments for e

$e = \langle i, m, \ldots \rangle$

i: scheme # 0–5; m: # arguments; $\ldots$: Gödel #'s of functions used in composition

$f(x, x_1, \ldots, x_m) \simeq \{x\}(x_1, \ldots, x_m)$

$f(x_1,\dots,x_m)$ is partial recursive iff $\exists\, e$ s.t.
$f(x_1,\dots,x_m) \simeq \{e\}(x_1,\dots,x_m)$

↑ "agrees completely"
Kleene equality: they have the same domain

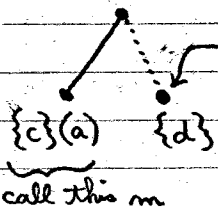
A computation tree is generated by the attempt to evaluate $\{e\}(x_1,\dots,x_m)$

HW #11: Show consistency of the schemes:
$\{e\}(a_0,\dots,a_m)$ has at most one value

↑ assume these are actual numbers (not variables)

Each node of the tree is a computation instruction, i.e., an expression of the form $\{e\}(a_0,\dots,a_m)$

$\{e\}(\overbrace{a_0,\dots,a_m}^{\text{call this } a})$ $\quad (= \{d\}(\{c\}(a))$ (e.g.) (composition)



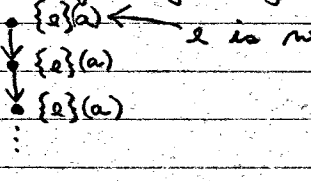
The set of immediate predecessors? successors of a node cannot be effectively determined from that node (but can be effectively enumerated) ?

finitely branching tree (composition, enumeration)
x is a terminal node
(constant, projection, or successor)
(and coding?)

The tree always exists. A computation (or, i.e., computation instruction) is said to converge if every path on its computation tree is finite (hence by Konigé lemma, the entire tree is a finite object)

A tree diverges if it is not convergent.
"Converge" means "is defined."
$\{e\}(a)$ converges means $\{e\}(a)$ is defined
$\{e\}(a)\downarrow$ means "converges"
$\{e\}(a)\uparrow$ means "diverges"

We need to add a "phony clause" to the definition of computation: if $\{e\}(a)$ is a node on the tree and e is not an index, then $\{e\}(a)$ is an immediate successor of $\{e\}(a)$. This forces an infinite path (divergent) for garbage.



Kleene Schemes (↙ pronounced "Klay-nee") for recursive functions

1), 2), 3), 4) as before

5) primitive recursion

$$f(0,x_1,\ldots,x_n) = g(x_1,\ldots,x_n)$$
$$f(y',x_1,\ldots,x_n) = i(y, f(y,x_1,\ldots,x_n), x_1,\ldots,x_n)$$

↖ successor

Example: addition

$$\text{plus}(0,x) = x \quad \leftarrow \text{identity function (one of the projection functions)}$$
$$\text{plus}(y',x) = (\text{plus}(y,x))'$$

6) least number operator

$$f(x) \simeq \mu z\,(g(x,z)=0) \qquad \text{"least } z \text{ such that } g(x,z)=0\text{"}$$

g is some already known partial recursive function. This defines a search: you

must work your way up to the least z, and as you work your way up g must be defined.

Diagonalizing over the primitive recursive functions:

Each primitive recursive function f is the result of a "derivation" that describes how f was put together using Kleene Schemes 1) - 5).

Note that any derivation of f makes it clear how to compute f.

Make a list of all derivations for primitive recursive functions of one argument:

d_0
d_1
d_2
$\vdots$

Let $d_n(x)$ be the value at argument x of the function specified by d_n. $d_n(x)$ is a computable function of n and x.

Suppose $d_n(x)$ is primitive recursive. Then $d_n(n)$ is primitive recursive, and so is $d_n(n)+1$. Therefore for some number, say 99, $d_n(n)+1$ is in the list.

$$d_n(n)+1 = d_{99}(n)$$
$$d_{99}(99)+1 = d_{99}(99) \quad \text{contradiction}$$

Concrete example of function which is not primitive recursive: Ackermann's function (see tutorial)

Kleene's Fixed Point Theorem:

Let f be a total recursive function (total means defined everywhere); then there exists an e such that

$$\{e\} \simeq \{f(e)\}$$

Implicit: we fix n

$$\{e\}(x_1,\ldots,x_n) \mapsto \{f(e)\}(x_1,\ldots,x_n)$$

("maps")

(one theorem for each n)

Proof

Sublemma: There exists a total recursive function t such that for all e:

$$\{t(e)\} \simeq \begin{cases} \{\{e\}e\} & \text{if } \{e\}e\downarrow \\ \text{NULL} & \text{if } \{e\}e\uparrow \end{cases}$$

Note: $\{z\}$, z a random number
If z is not an index, then
$\{z\}(x)\uparrow$ and $\{z\}$ is NULL
(NULL can be any function
not defined for any argument)

(t is called a "doubler")

Proof of F.P.T.:

$(f\circ t)(x) = f(t(x))$ (definition)

f & t are total, so $f(t(x))\downarrow$, so $\{c\}(c)\downarrow$

$\exists c$ such that $\{c\}(x) = f(t(x))$ for all x

$\{t(c)\} \simeq \{\{c\}(c)\}$ by sublemma

$\{c\}(c) = f(t(c))$ by definition

$\therefore \{t(c)\} \simeq \{f(t(c))\}$ $\therefore t(c)$ is the fixed point

Sublemma description:

$\{t(e)\}(x)$

1. $\{e\}(e) = m$ ← scheme 5) enables us to look at functions like $f(e,x) \simeq \{e\}(x)$
2. $\{m\}(x)$

Done

11/28/89

Fixed Point Theorem (cont.)

The proof of the fixed point theorem used a sublemma:
$\exists$ a total recursive function t such that
$\{t(e)\} \simeq \{\{e\}(e)\}$ for all e

- $\{t(e)\}$: the partial recursive function whose index is $t(e)$
- $\simeq$: "has the same graph as"
- $\{\{e\}(e)\}$: either the partial recursive function whose index is $\{e\}(e)$ if $\{e\}(e)$ is defined, or the null function (idea of the index itself being variable)

(the proof of the sublemma will be deferred for a while)

The fixed point theorem is proved, except for this lemma.

Fixed point theorem: Let f be a total recursive function. Then $\exists$ e such that $\{f(e)\} \simeq \{e\}$

Effective Transfinite Recursion

← we will not discuss transfinite

Idea behind recursion: define a new value from an old value

Recursion: define a function g by recursion via some iterator I.

Notation: $g \restriction x = \{\langle u, v\rangle \mid u < x \wedge v = g(u)\}$

- $g \restriction x$: "g restricted to x"
- $\{\langle u, v\rangle \mid u < x \wedge v = g(u)\}$: the graph of the function g for arguments less than x
- $\langle u, v\rangle$: ordered pair

$g(x) = I(g \upharpoonright x)$

new value — we know all previous values

I is a function which acts on numbers which are codes of $g \upharpoonright x$

Note: for each I there exists a unique g that satisfies the above recursion scheme for all x. (Really a proof by induction...)

$g(0) = I(g \upharpoonright 0)$ ← code number for the empty set

$g(1) = I(g \upharpoonright 1)$ ← includes only codes up to and including $g(0)$

$\vdots$

This is called "course-of-values" recursion

A suitable code for $g \upharpoonright x$ is $\prod_{i<x} p_i^{1+g(i)}$ (p_i = ith prime) (by definition, $\prod_{i<0} m = 1$)

notation: $\bar{g}(x)$ (due to Kleene) — sometimes called the sequence number. The length of sequence number $\bar{g}(x)$ is x.

$\bar{g}(0) = 1$

$g(x) = I(\bar{g}(x))$

Claim: Fixed point theorem yields course-of-values recursion

Claim: Course-of-values recursion yields primitive recursion

We want to claim that $g(x)$ is a fixed point of a certain process, maybe a fixed point of I

How can I act on (some arbitrary) $\{e\}(x)$?

Answer: Think of I as extending some method of computation from arguments less than x to x.
Suppose e is the method in use below x.
Let $I_0(e)$ be the method to be used at x.

$$\{I_0(e)\}(x) \simeq I(\overline{\{e\}}(x))$$

$\{I_0(e)\}$: new method to work for x
$\overline{\{e\}}(x)$: (think of e as a variable) (do your best to compute this) (I is given)

(Another deferred lemma: For each total recursive I there is a total recursive I_0 satisfying the above for all e)

$\{I_0(e)\}$ is a set of instructions which is applied to argument x. What does it do? It first applies $\{e\}(x)$ to all arguments less than x. If it succeeds it computes $\overline{\{e\}}(x)$ then applies I to it. (description in words)

I_0 has a fixed point c (by Fixed Point Theorem)

$$\{c\}(x) \simeq \{I_0(c)\}(x) \simeq I(\overline{\{c\}}(x))$$

$\{c\}(x)$: "c applied to x"
"has the same graph as"
$\overline{\{c\}}(x)$: "c bar of x"
F.P.T. lemma

Look at $\{c\}(x) \simeq I(\overline{\{c\}}(x))$
Let $g(x)$ be $\{c\}(x)$
Then $g(x) \simeq I(\overline{g}(x))$ ✓ (desired result)

How do we know g is total?

Course-of-values recursion scheme: For each total recursive iterator I, there exists a unique g such that $g(x) = I(\overline{g}(x))$ and g is total recursive.

We know g is total by induction (look at $g(0), \ldots$) and fact that I is total. (I doesn't have to be completely total, just defined where it is needed for g)

S-M-N Theorem (won't be proved here):

There exists a recursive function s such that

$$\{e\}(x,y) \simeq \{s(e,x)\}(y)$$

for all e, x, and y.

"take e, interpret it as a set of instructions, apply it to x and whatever is y"

To show the **primitive recursion scheme**: if g and h are recursive, then $\exists_1 f$ etc...

("exists a unique")

$$f(0,y) = g(y) \quad \text{(treat } y \text{ as a parameter)}$$
$$f(x',y) = h(f(x,y), x, y)$$

(x': successor)

needed because h may want to know x and y; we can't deduce them from f extract

Get rid of y (to simplify things)

$f(0) = 99$ (for example)
$f(x') = h(f(x), x)$

} can we get this from course-of-values recursion?

$\overline{f}(x+1) \mapsto f(x)$

$\exists$ recursive t such that $t(\overline{f}(x+1)) = f(x)$

$\exists$ recursive l such that $l(\overline{f}(x+1)) = x$

$\exists$ recursive I such that $I(\overline{f}(x+1)) = h(f(x), x)$

so I exists by "composition" of h, t, l

$$f(0) = 99$$
$$f(x+1) = I(\overline{f}(x+1))$$

looks like a course-of-values recursion except it starts with 1 instead of 0 (small adjustment needed)

essentially a course-of-values recursion

Least Number Operator ← our goal is to derive this

$$f(x) \simeq \underbrace{\mu y}_{\text{"the least } y \text{ such that"}} (g(x,y)=0)$$

Selection: There exists a partial recursive function W such that for all e:

(i) $\exists n \left(\{e\}(n)\downarrow\right) \Leftrightarrow W(e)\downarrow$
"converges for all e"

(ii) $\exists n \left(\{e\}(n)\downarrow\right) \rightarrow \{e\}(W(e))\downarrow$
"then $W(e)$ gives you one of those n's" (?)

$A_e = \{n \mid \{e\}(n)\downarrow\}$
if $A_e \neq 0$, then some element of A_e can actually be computed from e uniformly (with respect to e)
↑ an obscure notion; mentioned in a starred section in Kleene's book; this adverb means $\exists W$

How would we do this? Someone gives you $\{e\}$ — how would you find n? $\{e\}n$

Informal version of W:
Try for a while (e.g., "1 day") to compute $\{e\}(0)$
Then try $\{e\}(1)$
Then try $\{e\}(0)$ for a 2nd day
Then try $\{e\}(1)$ again
Then try $\{e\}(2)$ for a while ...
In this manner, try $\{e\}(n)$ for each n for longer and longer periods...
Eventually some convergence(?) will be found, i.e., $\{e\}(n)$ will be seen to converge for some n, and the first such n observed to converge is $W(e)$, or the above will go on forever, and $W(e)$ will not converge.

First we will look at the case whose only possible values for n are 0 or 1, then we will look at the general case.

For selection, then, we first consider the special case where at least one of the following two converges:

$$\{e\}0 \quad \text{or} \quad \{e\}1$$

Statement of this special case: There exists a partial recursive function W_0 such that for all e:

(i) $[\{e\}(0)\downarrow$ or $\{e\}(1)\downarrow] \leftrightarrow W_0(e)\downarrow$

↑ mathematical or; 3 cases

(ii) $[\{e\}(0)\downarrow$ or $\{e\}(1)\downarrow] \rightarrow$
$W_0(e) \in \{0,1\} \wedge \{e\}(W_0(e))\downarrow$

11/30/89

Preparation to selection

Pre-selection: There exists a partial recursive function f such that for all c and d:

(i) $\{(c)_0\}((c)_1)\downarrow \vee \{(d)_0\}((d)_1)\downarrow \leftrightarrow f(c,d)\downarrow$

(ii) $\{(c)_0\}((c)_1)\downarrow \vee \{(d)_0\}((d)_1)\downarrow \rightarrow$
$f(c,d) \in \{c,d\} \;\&\; \{(f(c,d))_0\}((f(c,d))_1)$

fine point: this could be a finite sequence of arguments

i.e., f is either c or d, and whichever one it is, it converges

"actually" c doesn't even have to be the code for a pair; for any number in fact this makes sense; in other words I can interpret any number c as a code for a pair; a lot of numbers will code the same pair"

Notation: $x = \prod_i p_i^{e_i}$ $\quad p_0=2,\ p_1=3,\ p_2=5,\ \ldots$ (primes)

then $(x)_i = e_i$ (definition)

Coding of a, b:

$$\langle a,b\rangle = 2^{1+a}\cdot 3^{1+b} = c$$

Change to (for convenience?):

$$\langle a,b\rangle = 2^a \cdot 3^b \quad \text{(new definition)}$$

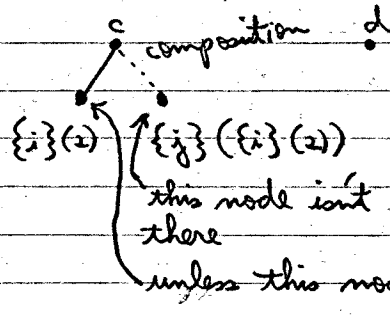
Then: $(c)_0 = a$
$(c)_1 = b$

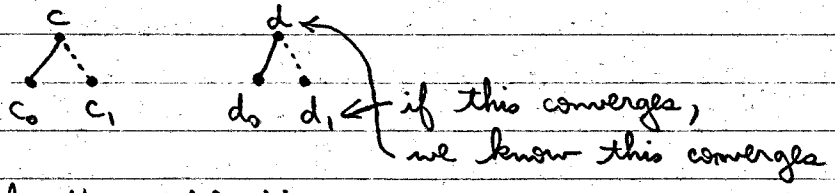
Proof: by recursion on the min $(|c|, |d|)$ (length of computation of c)
f is defined

Abbreviation: $c\downarrow$ means $\{(c)_0\}((c)_1)\downarrow$
If $c\downarrow$, then $|c|$ is the height of the computation tree for c

$|c| = 4$ = height

If $c\uparrow$, $|c| = \infty$
at least one of $|c|, |d|$ is finite, so it's a number.
We do a recursion on this number.





Look at the 4 combinations
$f(c_0, d_0)$
$f(c_0, d_1)$
$f(c_1, d_0)$
$f(c_1, d_1)$

every one of these yields an answer; if we know the 4 answers we can get $f(c,d)$ (the converse is true also)

"the key to the recursion, mathematically, is just a product of the trees"
There is a well-defined concept of product of trees which is not elaborated here.

The product of these trees would have as a typical node a pair of nodes, one from each tree.

Hypothesis: $c\downarrow \vee d\downarrow$

$c_0\downarrow \vee d_0\downarrow$ ← one of these two must converge

$\min(|c_0|, |d_0|) < \min(|c|, |d|)$

This recursion is justified by the fixed point theorem (as was course-of-values recursion.)

Imagine $\{a\}$ computes f correctly when $\min(|n|, |v|) < z$. Then we indicate how $\{\underset{\uparrow}{I}(a)\}$ computes f when $\min(|n|, |v|) = z$.

iterator

Then we take a fixed point e:

$\{I(e)\} \simeq \{e\}$

So if $\{e\}$ computes it correctly below z, it computes it at z; but that's true for every z, so $\{e\}$ computes it correctly at every level.

$\therefore f$ is $\{e\}$

What remains is to show the recursion step: if we know how to compute it below a certain level, then we know how to compute it at that level.

$\{a\}(|c_0|, |d_0|)$ computes $f(c_0, d_0)$

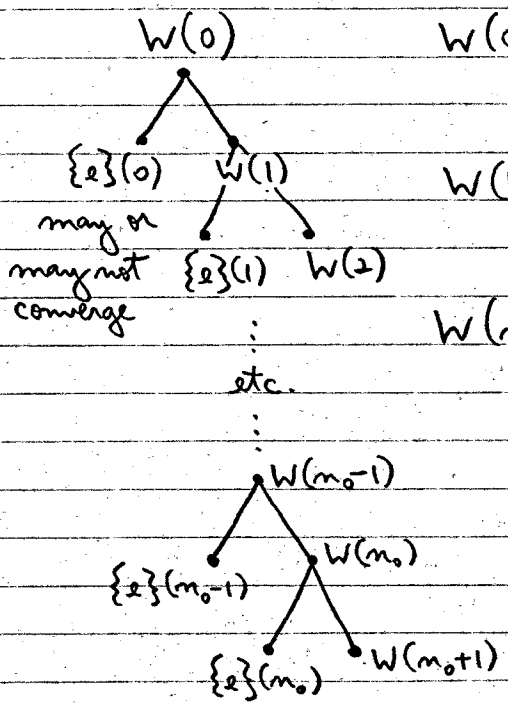
Full selection:

Selection: $\exists$ partial recursive t such that for all e:

(i) $\exists n\,(\{e\}(n)\downarrow) \leftrightarrow t(e)\downarrow$ ← "this guy picks such an n"

(ii) $\exists n\,(\{e\}(n)\downarrow) \rightarrow \{e\}(t(e))\downarrow$

$t(e)$ is really a procedure $W(e,n)$:



$W(0) = f(\{e\}(0), W(1))$

↑ from pre-selection

$W(1) = f(\{e\}(1), W(2))$

$\vdots$

$W(n_0) = f(\{e\}(n_0), W(n_0+1))$

Suppose $\exists n\,(\{e\}(n)\downarrow)$

Suppose $\{e\}(n_0)\downarrow$

Then $f(\{e\}(n_0), W(n_0+1))\downarrow$

Then $W(n_0)\downarrow$

$W(n_0-1)\downarrow$

$\vdots$

$W(0)\downarrow$

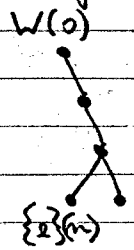
Similarly, if $W(0)\downarrow$

$\dashrightarrow W(n_0)\downarrow$ for some n_0, because otherwise $W(0)$ would diverge

$\therefore \exists n\,(\{e\}(n)\downarrow) \leftrightarrow W(0)\downarrow$

Suppose $W(0)\downarrow$

?How to compute an n such that $\{e\}(n)\downarrow$

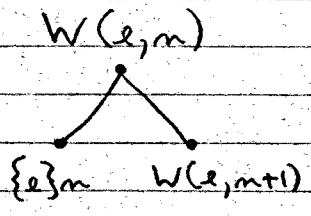


We know $W(0)\downarrow$ so compute $W(0)$
Before you're done, you will compute $\{e\}(n)$ for some n

Existence of $W(e,n)$ as a partial recursive function is justified by the fixed point theorem.

We seek a c such that $\{c\}(e,n) \simeq W(e,n)$

$$\{\underset{\text{iterator}}{I}(d)\} \simeq f(\{e\}(n), \{d\}(e,n+1))$$



$W(e,n) =$
$f(\{e\}(n), W(e,n+1))$

There exists a total recursive I such that the above holds for all e, d, and n.

($\{I(d)\}$ is little more than the composition of f, $\{e\}$, and $\{d\}$)

Pick a fixed point $\{I(c)\} = \{c\}$

$$\{c\}(e,n) \simeq f(\{e\}(n), \{e\}(e,n+1))$$
$$\{c\}(e,n) = W(e,n)$$
$$W(e,n) \simeq f(\{e\}n, W(e,n+1))$$

← this looks like a backwards recursion, but $\exists n \mid \{e\}(n)\downarrow$ prevents an ∞ loop

---

Recursion Theory

Definition of partial recursive function: done ✓

Let $A \subseteq \omega$ be a set of natural numbers. A is said to be recursive if c_A (characteristic function) is recursive.

$$c_A(n) = \begin{cases} 1 \text{ if } n \in A \\ 0 \text{ if } n \notin A \end{cases}$$

i.e., it's decidable whether a number belongs to A.

A is <u>recursively enumerable</u> if there exists a partial recursive function φ such that
$\forall n \; (n \in A \leftrightarrow \varphi(n)\downarrow)$

Proposition 1: Let $A \neq \emptyset$. A is recursively enumerable $\leftrightarrow$ A is the range of some total recursive function

(Note: If $A = \emptyset$, just take φ = null function, so φ is recursively enumerable)

Suppose $A \neq \emptyset$ is recursively enumerable.
If A is finite, proof is trivial (e.g., if $A = \{6\}$, then φ is the constant function, etc.)
Assume A is infinite.
Let $A = \{n \mid \varphi(n)\downarrow\}$. Then define

$f(0) = \mu n \; (\varphi(n)\downarrow)$ (least number operator comes from Selection)

$f(1) = \mu n \; (n \neq f(0) \wedge \varphi(n)\downarrow)$

$\vdots$

$f(x+1) = \mu n \; (n \neq \underbrace{f(0), f(1), \ldots, f(x)}_{f\restriction(x+1)} \wedge \varphi(n)\downarrow)$

Converse: Suppose $A = \{f(n) \mid n = 0, 1, 2, \ldots\}$ where f is a total recursive function.
Define $\varphi(x) = \mu n \; (f(n) = x)$ (there may not be such an n)
Then $\varphi(x)$ is partial recursive

$\varphi(x)\downarrow \leftrightarrow \exists n \; (f(n) = x) \leftrightarrow x \in A$

$P(x,y)$ is a <u>recursive predicate</u> if there exists a total recursive $t(x,y)$ such that

$$\forall x \forall y\, P(x,y) \leftrightarrow t(x,y)=1$$

$\mu y\, P(x,y)$ is a recursive predicate of x ? if $P(x,y)$ is recursive

HW #12: Find a set A such that A is recursively enumerable but A is not recursive.

12/5/89

Make up class:
Friday 2:30-4:30 Rm 2-142

<u>Facts:</u>

1. If A is recursive, then $\overline{A}$ is recursive. ($\overline{A}$: complement of A)

2. If A is recursive, then A is r.e. (recursively enumerable).

3. If A and $\overline{A}$ are both r.e., then A is recursive.

To answer "$n \in A$?" enumerate A and $\overline{A}$ simultaneously, until n appears in A or $\overline{A}$.

Simultaneous enumeration of all re. sets
(comes ultimately from our scheme 5:)
Enumeration Theorem

$\exists$ a partial recursive $f(e,n)$ such that for any partial recursive g, $\exists e$ such that

$$\forall n\, (f(e,n) \simeq g(n))$$

$$(f(e,n) \simeq \{e\}(n))$$

"omega"?

W_e = e th r.e. set = domain of $\{e\}(n)$
i.e., $W_e = \{n \mid \{e\}(n)\downarrow\}$

$\{W_e \mid e \geq 0\}$ is class of all r.e. sets

Enumerate all of them simultaneously:

W_0 .....
W_1 .....
W_2 .....
⋮

Intuitively, evaluate (work on) W_0, then W_1, then W_0 some more... As the enumeration proceeds, you will return to each one of them ∞ many times, and each time you return, you spend more time there.

$W_e^s = \{n \mid \{e\}(n)$ is seen to converge in less than s "steps"$\}$
↖ could be unit of time, height of computation, etc.

$\{e\}(0), \ldots, \{e\}(s-1)$
Look at computation if height $< s$

$W_e^s \subseteq W_e^{s+1}$

$W_e = \bigcup_{s>0} W_e^s$

W_e^s is a recursive function of e and n
(follows mainly from enumeration theorem)

More generally, suppose K^s is a finite set.
K^s is a recursive function of s.
Then $\bigcup_{s>0} K^s$ is r.e.

This style of recursion theory is due mainly to Emil Post. A great logician, he didn't realize his full potential due to mental problems.

Post, 1944 – paper that presented recursion theory in this informal way

Friedberg, 1954 – paper that established Post's informal theory – solution to "Post's problem"

Post: notion of <u>Simple Set</u>

A set A is <u>simple</u> if

1) A is r.e.
2) $\overline{A}$ is ∞
3) for all e, if W_e is ∞, then $W_e \cap A \neq \emptyset$ ("W_e touches A")

Informally: clause 2 says "put a lot of stuff in $\overline{A}$", and clause 3 says "keep a lot of stuff out of $\overline{A}$" – this makes the construction of A challenging

Note: If A is simple, then A is not recursive.

Proof: Suppose A is recursive.
Then $\overline{A}$ is recursive.
Then $\overline{A}$ is r.e. (and infinite, by construction)
Then $\overline{A} \cap A \neq \emptyset$ (contradiction) ←?

A is going to be simple
A is constructed in stages.
$A^{<s}$ is the set of elements put in A prior to stage s
A^s is the set of elements put in A prior to or at stage s
Our intention: $A = \bigcup_s A^s$

$A^0 = \emptyset$.
Stage $s > 0$: (product of primes...) ← exponent of power of 2 factor of s
Let $e = (s)_0$ ← "they don't touch"
if $W_e^s \cap A^{<s} = \emptyset$ and $\exists x\,(x \in W_e^s \;\&\; x \geq 2e)$
then put the least such x in A, i.e.,
$A^s = A^{<s} \cup \{\text{least such } x\}$
Otherwise, do nothing.
End of construction.

Is A simple?

① A is r.e. because $A = \bigcup_s A^s$ and A^s is a recursive function of s.

② Suppose $W_e = \infty$.
Suppose $W_e \cap A = \emptyset$.
This is the same as saying $W_e^s \cap A^{<s} = \emptyset$ for all s.
Since $W_e = \infty$, $\exists x$, call it x_0, such that $x_0 \geq 2e$ and $x_0 \in W_e$.
Since $x_0 \in W_e$, then $x_0 \in W_e^t$ for all sufficiently large t, i.e.,
$$\exists t_0 \, \forall t \, (t \geq t_0 \rightarrow x_0 \in W_e^t)$$
There are ∞ many s such that $e = (s)_0$
(just look at all $2^e \cdot q$, where q is odd)
There exists an s such that
$$\exists s \; W_e^s \cap A^{<s} = \emptyset$$
$$x_0 \in W_e^s \quad x_0 \geq 2e$$
$$(s)_0 = e$$
but then at stage s, some $x \leq x_0$ is put in A.

$\therefore$ condition ③ has been met
In words: If W_e is ∞, it will contain all #'s $> 2e$.

③ Check our construction against condition 2: $\overline{A}$ is ∞
If x is put in A at stage s, then we say x was put in A for the sake of W_e, where $e = (s)_0$.

Note: In the course of the construction, at most one x is put in A for the sake of W_e.

Suppose x_1 was put in A for the sake of W_e at stage t_1
Ⓐ Suppose x_2 was put in A for the sake of W_e at stage t_2

Assume $t_1 < t_2$.
This means that $x_1 \in A^{t_1} \cap W_e^{t_1} \neq \emptyset$
(x_1 was put in A^{t_1} and when it was put in it was a member of $W_e^{t_1}$)

$A^{t_1} \subseteq A^{<t_2}$ $\quad W_e^{t_1} \subseteq W_e^{t_2}$

$A^{<t_2} \cap W_e^{t_2} \neq 0$

(A) ↳ But $W_e^{t_2} \cap A^{<t_2} = 0$ (contradiction)

Look at numbers in the closed interval $[0, 2e]$

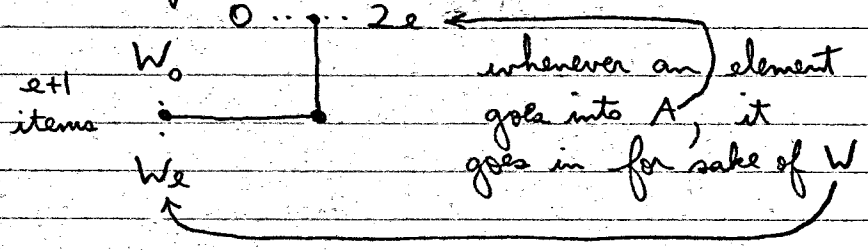
Suppose $x \in [0, 2e]$

x can be put in A only if $x \geq 2i$ for some i, and x is put in for the sake of W_i (where $i \leq x/2$)

The biggest x in $[0, 2e]$ is $2e$, so $i \leq e$.

If $x \in [0, 2e]$, and x is put in A, then x is put in A for the sake of W_i for some $i \leq e$. Each such i gives rise to at most one element put in A. Hence at most $e+1$ members of $[0, 2e]$ are put in A.

make a picture:



so at least e elements of $[0, 2e]$ are not put in A. ($\therefore$ cA is ∞)

A Post simple set is an example of a dynamic construction of an r.e. set ("a sense of time passing" – at stage s we had to know exactly what W_e^s was for every e and every s).

Contrast this to a static construction ("syntactical"), e.g., Gödel's construction of non-recursive r.e. sets via diagonal argument.

Post's Problem

A, B are sets of natural numbers

$A \leq_m B$ (A is <u>many-one reducible</u> to B) if there exists a (total) recursive function f such that

$\forall x\ (x \in A \leftrightarrow f(x) \in B)$

Some facts:

$A \leq_m A$

$A \leq_m B \ \& \ B \leq_m C \rightarrow A \leq_m C$

$\therefore A \leq_m B \ \& \ B \leq_m A$ is an equivalence relation:

$A \equiv_m B \leftrightarrow A \leq_m B \ \& \ B \leq_m A$ (definition)

$\underline{A}$ is the <u>many-one degree</u> of A.

$\underline{A} = \{B \mid B \equiv_m A\}$ (note: this is a countable set because there are countably many recursive functions)

There exists a partial ordering:

$\underline{A} \leq \underline{B}$ means $A \leq_m B$

$$\begin{cases} \underline{A} \leq \underline{A} \\ \underline{A} \leq \underline{B} \text{ and } \underline{B} \leq \underline{C} \rightarrow \underline{A} \leq \underline{C} \\ \underline{A} \leq \underline{B} \text{ and } \underline{B} \leq \underline{A} \rightarrow \underline{A} = \underline{B} \end{cases}$$

(requirements of definition of partial ordering)

Note: If A is recursive and $B \neq \phi$ and $cB \neq \phi$, then $A \leq_m B$

Proof: want to show: $x \in A \Leftrightarrow f(x) \in B$

Choose $b_0 \in B$, $b_1 \notin B$

Define $f(x) = \begin{cases} b_0 & \text{if } x \in A \\ b_1 & \text{if } x \notin A \end{cases}$

$X \leq_m \phi \rightarrow X = \phi$

$\phi \leq_m X \rightarrow \quad n \in \phi \Leftrightarrow f(n) \in X \quad \therefore f(n) \notin X \ \therefore cX \neq \phi$

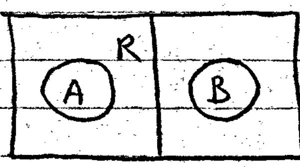
$\underline{\phi} = \{\phi\}$ (degree of empty set)

12/7/89

Definitions:

Let A and B be r.e. sets. A and B are said to be <u>recursively inseparable</u> if:

1) $A \cap B = \emptyset$
2) $\neg\exists$ recursive set R such that $A \subseteq R$ and $R \cap B = \emptyset$



← we're saying that there is no such R

HW #13: Find a pair of recursively inseparable r.e. sets.

You might want to approach this dynamically (easier?) or statically; could be either way. (Goes back to Rosser, who "used it" to strengthen Gödel's incompleteness theorem, i.e., throw out the requirement for ω-consistency.)

[Margin note, with arrow: Thesis = "Foundation of mathematics without variables"]

co-r.e. = complement of an r.e. set

HW #14: Proposition: Any two disjoint co-r.e. sets can be separated by a recursive set.

Suggestion: give a dynamic argument; build r.e. and co-r.e. sets simultaneously

[Margin note: Last time talked abt [illegible] arg's for building r.e. sets. How would we use a dyn. arg to build a rec set? Use fact that rec set consists of a set [illegible] & complement both of which are r.e. Build the r.e. set & its complement as r.e. sets & make sure they're [illegible]; when you're all done, you know the set is recursive]

Let A and B be sets of natural numbers. Define A is recursive in B (or A is Turing reducible to B)

$A \leq_T B$

Return to definition of partial recursive functions. This definition can be relativized to an arbitrary total (not necessarily recursive) function g as follows:

Add "scheme (6)": $f(x_0,\ldots,x_n) = g(x_0,\ldots,x_n)$

Schemes (0) - (6) yield partial functions computable from g (we now have g at our disposal)

e.g. $\underbrace{\{e\}}^{g}(6,11) = 14$
notation

Computations are still finite

e.g. $f(x) = (g(x))'$
f is computable from g

$A \leq_T B$ means $c_A = \{e\}^{c_B}$ for some e.
(c_A, c_B: characteristic functions)

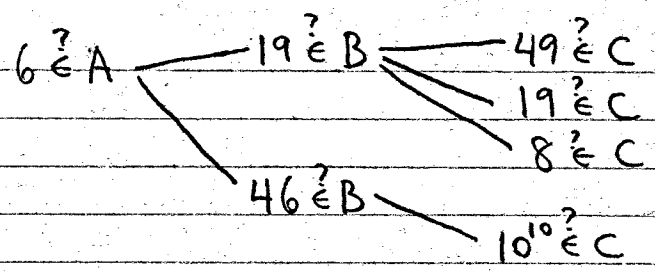
Before, we had finite programs; now we're allowed to use g.
Idea of "oracle": The oracle gives the value of g to the program whenever the program asks for it

Properties:

$A \leq_T A$

$A \leq_T B \wedge B \leq_T C \rightarrow A \leq_T C$

Proof: Ask a question about A; we know how to compute it from B; ask oracle finitely many questions; but each fact about B can be computed from C.



This is essentially the composition of the two programs.

Notation: Let $A = \{e\}^B$ mean $c_A = \{e\}^{c_B}$ for convenience

$A = \{e_1\}^B$

$B = \{e_2\}^C$

$A = \{e_1\}^{\{e_2\}^C}$

$A \equiv_T B$ (A and B have the same Turing degree or are Turing equivalent)
if $A \leq_T B \wedge B \leq_T A$

$\underline{A}$ = Turing degree of A
$= \{B \mid B \equiv_T A\}$

empty set → $\underline{\phi}$ = set of all recursive sets (we have ϕ as our oracle, but we can still compute all recursive sets

Note: If A is a recursive set, then $A \leq_T B$ (i.e., A is Turing reducible to any set)

$\underline{A} \leq \underline{B}$ means $A \leq_T B$

$\underline{\phi} \leq \underline{B}$ ← any degree

↖ degree of empty set

There is an upper semi-lattice of Turing degrees (?)
(Kleene–Post degrees)
(they called them degrees of recursive unsolvability)

Now we can state Post's problem

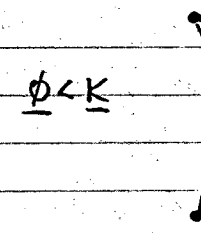
First, we need some trivial propositions:
An r.e. set A is said to be <u>complete</u> if for every r.e. set B, $B \leq_T A$
(at the moment, we do not know if any complete r.e. sets exist.)
Candidate:
(exponent of power of 2 factor; exponent of power of 3 factor)
Let $K = \{e \mid \{(e)_0\}((e)_1)\downarrow\}$
(tells you how to enumerate K: enumerate all r.e. sets)

K contains everything we know about all r.e. sets

Note: Let B be r.e. Then $B \leq_T K$ (i.e., K is complete).
$B = W_c$ for some c if B is r.e.
$B = \{n \mid \{c\}(n)\downarrow\}$
$n \in B \Leftrightarrow 2^c \cdot 3^n \in K$

<u>Post's problem:</u> Is there an r.e. set which is neither recursive nor complete?

i.e., Among r.e. sets is there a third degree of recursive unsolvability?



$\underline{\emptyset} < \underline{K}$

$\exists A$ such that $\underline{\emptyset} < \underline{A} < \underline{K}$?
(where A is r.e.)

Answer: YES – Solved by Richard Friedberg, as

answer to homework problem given by Rogers (MIT)
Proof is in Shoenfield's book (one page),
maybe in Machover's book?

Myhill's partial results - make clear why
"natural" examples don't provide an answer to
Post's problem

A is said to be <u>creative</u> if

1) A is r.e.
2) There exists a recursive function c (<u>productive function</u>) such that for all e

$$W_e \subseteq cA \rightarrow c(e) \in (cA - W_e)$$

This means there is a uniform effective method of doing the following: If you give me some r.e. subset of the complement, and you give me its Gödel number or a program for enumerating it, then I can effectively find the number which is outside the r.e. set and (not)? in the complement. So it follows that the complement can't be r.e. because you can always get one more number in the complement that's not in the r.e. set.

Hence a creative set is not recursive.

Gödel essentially showed that the set of theorems for any reasonable mathematical system is creative.
In other words, by definition of reasonable mathematical systems, the theorem set is r.e.; then if you give Gödel a method for enumerating sentences which are not provable in the system, then he can give you one more sentence which is still not provable; so in other words

he is telling you there's no way to enumerate all the non-theorems; in other words if you give him an r.e. set of non-theorems he will give you one more non-theorem; hence the set of non-theorems is not r.e.; hence the set of theorems is non-recursive.

Myhill: Every creative set is complete.

(That explains why the "natural" examples, the theorem sets, are complete -- from Gödel the theorem sets are creative, and from Myhill they are complete.)

(In fact, every r.e. set is many-one reducible to every creative set:)

$$A \leq_m B \rightarrow A \leq_T B$$

$A \leq_m B$: $n \in A \leftrightarrow f(n) \in B$

$A \leq_T B$: you have a routine for answering questions about A by asking questions about B

(but the converse is not true — Turing degrees are much larger than many-one degrees)

Let A be any r.e. set (show $A \leq_m B$)
Let B be creative with productive function c
Find a total recursive f such that
$n \in A \leftrightarrow f(n) \in B$

There exists a total recursive function t such that for all e and n

$$W_{t(e,n)} = \begin{cases} \{c(\{e\}(n))\} & \text{if } n \in A \\ \emptyset & \text{if } n \notin A \end{cases}$$

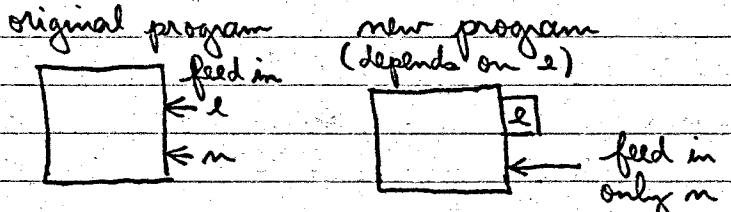
↑ instructions for enumerating r.e. set $W_{t(e,n)}$, i.e., the Gödel number of a program that enumerates $W_{t(e,n)}$

($W_{t(e,n)}$ is empty or contains at most one element)

$t(e,n) \simeq \{\mu(e)\}(n)$ for some recursive μ (by S-M-N theorem)

↑ total recursive function of 2 variables

↑ move the value of e into the program



Pick a fixed point of μ (by Fixed Point Theorem):

$$\{\mu(d)\} \simeq \{d\}$$

$$W_{t(d,n)} = W_{\{\mu(d)\}(n)}$$

$$= W_{\{d\}(n)} \quad \text{by fixed point}$$

$$= \begin{cases} \{c(\{d\}(n)\} & \text{if } n \in A \\ \emptyset & \text{if } n \notin A \end{cases}$$

$$n \in A \rightarrow W_{\{d\}(n)} = \{c(\{d\}(n))\}$$

n.e. set with one member

$$\rightarrow c(\{d\}(n)) \in W_{\{d\}(n)}$$

$$\rightarrow W_{\{d\}(n)} \not\subseteq cB$$

(if $W_{\{d\}(n)}$ were $\subseteq cB$, then the productive function applied to it would yield a brand new member of cB. But it doesn't; it "lands you right back in.")

$$\rightarrow c(\{d\}(n)) \notin cB$$

(because $W_{\{d\}(n)}$ has only one element)

$\rightarrow c(\{d\}(n)) \in B$

On the other hand,

$n \notin A \rightarrow W_{\{d\}(n)} = \emptyset \subseteq cB$

$\rightarrow c(\{d\}(n)) \in cB$

($W_{\{d\}(n)}$ is empty, so if we apply the productive function to it, we still get something in cB)

Putting this together,

$n \in A \Leftrightarrow c(\{d\}(n)) \in B$

↑ this is our $f(n)$

$\therefore$ we've proved that A is many-one reducible to B.

12/8/89

"Return match" with
Craig's Interpolation Theorem

A theory T is simply a (countable) consistent set of sentences. ← for our purposes

Robinson's joint consistency theorem:

Let T_1 be a theory in the language $\mathcal{L}_1$.
Let T_2 be a theory in the language $\mathcal{L}_2$.
Then (a) and (b) are equivalent:

(a) $T_1 \cup T_2$ is consistent

(b) T_1 and T_2 agree on $\mathcal{L}_1 \cap \mathcal{L}_2$ (i.e., it's not the case that there exists an $\mathcal{F} \in \mathcal{L}_1 \cap \mathcal{L}_2$ such that $T_1 \vdash \mathcal{F}$ and $T_2 \vdash \neg\mathcal{F}$)

Proof:

Suppose $T_1 \cup T_2$ is consistent.
Suppose $T_1 \vdash \mathcal{F}$ and $T_2 \vdash \neg\mathcal{F}$, where $\mathcal{F} \in \mathcal{L}_1 \cap \mathcal{L}_2$.
This is a contradiction. (End of (a) → (b))

Conversely, assume (b) and show (a):

Let $\mathcal{Z}_n$ be the sentence "the universe has at least n elements"
$\mathcal{Z}_n \in \mathcal{L}_1 \cap \mathcal{L}_2$ ($\mathcal{Z}_n$ is in the common language)

Suppose $T_1 \vdash \neg\mathcal{Z}_n$, then $T_2 \not\vdash \mathcal{Z}_n$.

Scheme: make $\mathfrak{M}_1 \models T_1$, $\mathfrak{M}_2 \models T_2$ ("a model of")
such that: (1) card $\mathfrak{M}_1$ = card $\mathfrak{M}_2 \leq \omega$ ("cardinality")
(2) $\mathfrak{M}_1$ and $\mathfrak{M}_2$ agree on $\mathcal{L}_1 \cap \mathcal{L}_2$

Note that (2) → (1), so we don't have to worry about (1). Since cardinalities are the same, the universes are the same, so they can be the same object.

$\mathfrak{M}_1 = \langle U$ (universe), common stuff, stuff peculiar to $\mathcal{L}_1 \rangle$
$\mathfrak{M}_2 = \langle U$, common stuff, stuff peculiar to $\mathcal{L}_2 \rangle$

$\mathfrak{M} = \langle U$, common stuff, $\mathcal{L}_1$ stuff, $\mathcal{L}_2$ stuff$\rangle$

(2) → (1): $\mathfrak{M}_1$ and $\mathfrak{M}_2$ agree on all cardinality statements

T_1 and T_2 agree on $\mathcal{L}_1 \cap \mathcal{L}_2$ (assumption)
Do a countable version of Henkinization
Construct $\mathfrak{M}_1$ and $\mathfrak{M}_2$ simultaneously
$\mathfrak{M}_1 \models T_1$ $\mathfrak{M}_2 \models T_2$

$\mathfrak{M}_1$ and $\mathfrak{M}_2$ agree on relations, functions, and individual constants of $\mathcal{L}_1 \cap \mathcal{L}_2$.

$\mathfrak{M}_1$	$\mathfrak{M}_2$
1. Henkinize d $\exists x \mathcal{B}(x) \to \mathcal{B}(d)$ $(\mathcal{B} \in \mathcal{L}_1)$	2. Henkinize c $\exists x \mathcal{B}(x) \to \mathcal{B}(c)$ $(\mathcal{B} \in \mathcal{L}_2)$ (use disjoint sets of Henkin constants for $\mathfrak{M}_1$ and $\mathfrak{M}_2$)
At the end of step 1, we have a conservative extension of $T_1 = T_{1,\omega} \subseteq \mathcal{L}_{1,\omega}$	At the end of step 2, we have a conservative extension of $T_2 = T_{2,\omega} \subseteq \mathcal{L}_{1,\omega}$

Claim: $T_{1,\omega}$ and $T_{2,\omega}$ still agree on $\mathcal{L}_{1,\omega} \cap \mathcal{L}_{2,\omega}$

Assume $T_{1,\omega} \vdash \mathcal{F}$ $\quad T_{2,\omega} \vdash \neg\mathcal{F}$, $\mathcal{F} \in \mathcal{L}_1 \cap \mathcal{L}_2$

then $\quad$ then

$T_1 \vdash \mathcal{F}$ $\quad T_2 \vdash \neg\mathcal{F}$ (because extension is conservative)

$\longleftrightarrow$ contradicts assumption

2. Let $J_0, J_1, J_2, \ldots$ be a list of all sentences $\in \mathcal{L}_1 \cap \mathcal{L}_2$.
We wish to add J_0 to both $T_{1,\omega}$ and $T_{2,\omega}$ or add $\neg J_0$ to both $T_{1,\omega}$ and $T_{2,\omega}$, so that
$T_{1,\omega} \cup \{J_0\}$ and $T_{2,\omega} \cup \{J_0\}$ agree on $\mathcal{L}_1 \cap \mathcal{L}_2$
or $T_{1,\omega} \cup \{\neg J_0\}$ and $T_{2,\omega} \cup \{\neg J_0\}$ agree on $\mathcal{L}_1 \cap \mathcal{L}_2$.

Suppose they both fail: then we have an $\mathcal{F}$, $\mathcal{G}$ in the common language such that
$\mathcal{F} \in \mathcal{L}_1 \cap \mathcal{L}_2$ $\quad \mathcal{G} \in \mathcal{L}_1 \cap \mathcal{L}_2$

$T_{1,\omega}, J_0 \vdash \mathcal{F}$ $\quad T_{2,\omega}, J_0 \vdash \neg\mathcal{F}$

$T_{1,\omega}, \neg J_0 \vdash \mathcal{G}$ $\quad T_{2,\omega}, \neg J_0 \vdash \neg\mathcal{G}$

$T_{1,\infty} \vdash (J_0 \to \mathcal{F}) \wedge (\neg J_0 \to \mathcal{G})$

$T_{2,\infty} \vdash (J_0 \to \neg\mathcal{F}) \wedge (\neg J_0 \to \neg\mathcal{G})$

Then $T_{1,\infty}$ and $T_{2,\infty}$ disagree, contrary to assumption.

Similarly, add $J_1, J_2, \ldots$

Basic lemma just proved:

If Σ_1 and Σ_2 agree on the common language, and J' is in the common language, then either $\Sigma_1 \cup \{J\}$ and $\Sigma_2 \cup \{J\}$ agree, or $\Sigma_1 \cup \{\neg J\}$ and $\Sigma_2 \cup \{\neg J\}$ agree.

3. $T_{1,\infty,\infty}$ and $T_{2,\infty,\infty}$ agree on $\mathcal{L}_1 \cap \mathcal{L}_2$.

$T_{1,\infty,\infty}$	$T_{2,\infty,\infty}$
Now add sentences in $\mathcal{L}_1$ but not in $\mathcal{L}_1 \cap \mathcal{L}_2$	Now add sentences in $\mathcal{L}_2$ but not in $\mathcal{L}_1 \cap \mathcal{L}_2$
Obtain $T_{1,\infty,\infty,\infty}$	Obtain $T_{2,\infty,\infty,\infty}$

Henkinization
common language
not in common language

Then by Henkin argument, these theories "read off" models:

$\mathfrak{M}_1$ $\langle M, \text{common stuff}, \text{rest}\rangle$ $\quad$ $\mathfrak{M}_2$ $\langle M, \text{common stuff}, \text{rest}\rangle$

e.g. $R \in \mathcal{L}_1 \cap \mathcal{L}_2$

$R^{\mathfrak{M}}(c,d)$ iff $T_{1,\infty,\infty,\infty} \vdash R(c,d)$

$T_{1,\infty,\infty,\infty} \vdash R^{-}(c,d) \leftrightarrow T_{2,\infty,\infty,\infty} \vdash R(c,d)$

↑ actually $[c]$, equivalence class of Henkin constants

← (common relations are exactly the same)

Final detail:

Should we use same Henkin constants in $T_{1,\infty}$ and $T_{2,\infty}$? Common language would be $(\mathcal{L}_1 \cap \mathcal{L}_2) \cup \{\text{Henkin constants}\}$.

If they disagree:

$T_{1,\infty} \vdash \mathcal{F}(c)$ $\quad$ $T_{2,\infty} \vdash \neg\mathcal{F}(c)$

Is this a problem, and how do we avoid it? (Needs to be clarified)

HW #15 (a) Show that joint consistency → interpolation.
(b) Prove the joint consistency theorem.

12/12/89

Posts' Problem

Theorem (Friedberg, Muchnik): There exists an r.e. set A such that A is neither recursive nor complete.

What do we want from A? First, we want A to be non-recursive. Our strategy there will be roughly the same as the simple set strategy.

1) $\forall e$ if $W_e = \infty$, then $A \cap W_e \neq \emptyset$
2) $cA = \infty$
3) $\forall e\ \exists m \left[\{e\}^A(3^{e+1}\cdot 5^m)\uparrow \quad \text{or} \quad B(3^{e+1}\cdot 5^m) \neq \{e\}^A(3^{e+1}\cdot 5^m) \right]$

Note: $B = \{e\}^A$ means $c_B = \{e\}^{c_A}$, (char. functions)

where $\{e\}^g$ means "computable from g" using "scheme 6" (see 12/7/89 notes)

A and B are r.e. sets constructed simultaneously by stages.

1) and 2) imply A is not recursive.

3) implies A is not complete (because if A were complete, we could compute every r.e. set from it; but we can't compute B from it, because in particular if we take Gödel number e and we apply it to A, there's an argument which either it just gives us nothing at all, or, if it really gave us a set, that set is not B). I.e., because $B \not\leq_T A$

"Requirements":

P_e: $W_e = \infty \rightarrow A \cap W_e \neq \phi$

P_e is the eth positive requirement

(it is called positive because it may require putting some number into A to meet the condition)

N_e: $\exists_n \left[\{e\}^A(3^{e+1} \cdot 5^n)\uparrow \ \vee \ B(3^{e+1} \cdot 5^n) \neq \{e\}^A(3^{e+1} \cdot 5^n) \right]$

More succint notation:

$\exists_n \ \underbrace{B(3^{e+1} \cdot 5^n)}_{\text{always defined (either 0 or 1)}} \neq \underbrace{\{e\}^A(3^{e+1} \cdot 5^n)}_{\text{either this is undefined, or it has a different value than B}}$

(Note: when we refer to A or B, we really mean its characteristic function)

N_e is the eth <u>negative requirement</u>

Reason it's called negative: we never know what A and B look like along the way; we only know what they look like at stage s. At the end of stage s, we have

$$B^s(3^{e+1}\cdot 5^m) \neq \{e\}_s^{A^s}(3^{e+1}\cdot 5^m)$$

A^s is a finite set

$\{e\}_s$ means compute, via e, but only look at the first s computations (this is a finite bound on the computation)

Note: $\{e\}_s^{A_s}(m)$ is a computable function of s and m ("we might as well put a bound on m" (?why?); assume $m<s$)

we're only looking at computations that involve x units of say time and space; a big m there's no room for. So that implies a bound on m.

Compute $\{e\}_s^{A^s}(m)$; possible results:

$\{e\}_s^{A_s}(m)$ <u>appears</u> to diverge <u>or</u> it converges.

To preserve an $\neq$ (inequality), a <u>promise</u> is made to keep some number out of A at all future stages (so it is called a <u>negative requirement</u>)

There is a potential conflict between P_e (it wants to put numbers in) and N_d (it wants to keep numbers out). How do we resolve these conflicts?

Resolve by the priority method: if $c < d$, then P_c wins over N_d; otherwise not.

This means that for N_0, any promise made is eternal; it can't be broken. For P_0: the only thing that can prevent P_0 from putting a number in is N_0.

This creates a strange situation: you might suddenly see an inequality that you like; you make the promises; some time passes; and you break them; so the inequalities go away. That's OK. What we'll do in that case is increase the value of n and try again.

The hope is that this will only happen finitely often; in other words for a fixed e we'll only have finitely many stages where we break a promise made earlier to preserve inequality. So then hopefully there will be a later stage where somehow an inequality "appears again" and after that we'll get through.

This is sometimes called the finite injury method. In other words you make finitely many attempts to satisfy each requirement; each one is undone except for the last one. ("Finite injury" and "priority" mean same thing.)

This is different from the simple dynamic set argument. There we made at most one attempt to satisfy a requirement, and we were done.

(End of preliminaries)

Now we try to write down the actual construction method:

Stage 0: - Initialization

$B^0 = A^0 = \emptyset$

$w(0,e) = 0$ "witness", i.e., a way of keeping track of n

(initially, when we're seeking the inequality all the n's are zero; but of course the witnesses are eventually different for different e)

$r(0,e) = 0$ r is a way of keeping track of promises

(r means "keep all numbers less than this out of A from now on")

Stage $s > 0$:

Case I: $(s)_0 = 0 \wedge (s)_1 = e$

($(s)_0 = 0$: refers to simple set business; $(s)_1 = e$: refers to W_e)

<u>If</u> $W_e^{s-1} \cap A^{s-1} = \emptyset$ (then there's a reason to do something) and

$$\exists n \left[\underbrace{n \geq 2e}_{\text{this clause makes the complement infinite}} \wedge \underbrace{\forall d \left(d \leq e \rightarrow n \geq r(s-1, d) \right)}_{\text{we mustn't break any promises made for the sake of the negative requirements}} \right]$$

then put the least such n into A

$A^s = A^{s-1} \cup \{\text{least such } n\}$

We also have to update w, r, B

There might be some $d > e$ such that at an earlier stage $t < s$,

$B^t(\ ) \neq \{e\}^{A^t}(\ )$

(You made some promises, and now you've broken them. Our reaction is to introduce a new witness here)

For each $d > e$:

$w(s,d) = s$ ← fresh witness

$r(s,d) = 0$

(we're updating even if not necessary, to cover the worst possible case)

Also, $B^s = B^{s-1}$ (trivial update)

For each $d \leq e$:

$w(s,d) = w(s-1,d)$

$r(s,d) = r(s-1,d)$

(we respected all these promises, so we just carry them along)

Else do nothing (i.e., all updates are trivial):

$w(s,d) = w(s-1,d)$

$r(s,d) = r(s-1,d)$

$B^s = B^{s-1}$

Case II $(s)_0 > 0 \wedge (s)_1 = e$

If $r(s-1,e) = 0$ (either no promise was ever made, or if it was made it was broken and got updated down to 0 at an earlier stage)

and $\{e\}_s^{A^{s-1}}(3^{e+1} \cdot 5^{w(s,e-1)})\downarrow$ and $= v$

then

$r(s,e) = \mu n [n >$ any negative fact about A mentioned in above convergence$]$

and

$$B^s(3^{e+1} \cdot 5^{w(s,e-1)}) = \begin{cases} 1 \text{ if } v = 0 \\ 0 \text{ if } v > 0 \end{cases}$$

(Note: $B^{s-1}(3^{e+1} \cdot 5^{w(s,e-1)}) = 0$)

↑ because B starts out empty

↓

There's a worry here: we're building an r.e. set B, so at stage s we're not really free to assign any values we want to B^s. If the value at stage s-1 was 0, we can change it to 1, but not vice-versa. (Hence the note.)

w is a non-decreasing function and takes a jump up each time a promise is broken. If all previous promises have been broken, the current value of w is absolutely fresh.

To summarize: we first try to compute the right-hand side of the inequality. If we succeed, we know that on the left-hand side the number has not yet been put into B; we put it in or don't put it in depending on value of the right-hand side.

Putting the number into B doesn't hurt anybody; there are no promises to keep numbers out of B. (In Friedberg's approach, there are.)

Trivial updating of w

Else do nothing (i.e., trivial updating)

(End of construction)

Now we have to show that it works.

Lemma: $\lim_{s\to\infty} r(s,e) < \infty$ (fix e and let s increase)

i.e., $r(s,e)$, as a function of s, changes only finitely often.

This lemma establishes the main combinatoric fact, which is that everything settles down.

Proof:

Fix e. Suppose $r(s,e)$ changes ∞'ly often.

Consider a case I change in $r(s,e)$.
It's caused by some W_d, where $d<e$.
This happens at most once for each $d<e$
(because of clause $W_e^{s-1} \cap A^{s-1} = \emptyset$; once you put a number into A for the sake of this clause, you will never be asked to again; each positive simple set requirement is implemented only once)

So $r(s,e)$ must change ∞'ly often according to case II. But case II can only change r from 0 to some positive value.
Hence r must change from positive value to 0 ∞'ly often, but only case I can do this. □

A is simple, as before, hence recursive.
Look at case I "if" clause: $\ldots\ldots \wedge \forall d\,(d \le e \to m \ge r(s-1,d))]$

For a fixed e, this clause only has to worry about finitely many d's, and r only changes finitely often for each d, so there's a maximum value that will ever appear here. So if W_e is infinite, there will be lots of numbers that will satisfy the inequalities.

Suppose $B = \{e\}^A$.
Since r settles down, the lemma implies w settles down too:

$$w(e) = \lim_{s\to\infty} w(s,e) < \infty$$

(The only time w changes is when r drops back to 0 suddenly, which only happens finitely often.)

For all sufficiently large s,

$$\{e\}^{A^{s-1}}(w(s,e)) = w$$
$$\| \quad w(e)$$

If $w=0$, then for some large s, we've set

$$B(s, w(s,e)) = 1 \qquad \text{(so inequality is not)}$$

If $w=1$, then for some large s,

$$B(s, w(s,e)) = 0$$

We know then that for a fixed e, if we go out far enough, r and w will settle down, and no promises will be broken.

Summary: We have a system here for setting up inequalities and preserving them. The only time you violate one is for the sake of a simple set requirement. But you break things so that will happen only finitely often. So the next time you set up an inequality it's going to stay. Now if you never get a next time to set up an inequality, it means that $\{e\}^A$ is undefined in which case you don't have to worry.

In our construction, the eth negative requirement gets injured at most e times. It can only be injured by a positive requirement P_d where $d<e$. The way Friedberg has it, N_e can be injured at most $2e$ (2^e?) times.

(Sacks) Commentary: A lot of people have interpreted the work on recursion theory, and in particular the incompleteness theorem, as a proof that "man are just machines." Gödel himself held just the opposite opinion; he felt his work showed man are not machines (a minority holds his view).

12/14/89

Gödel's Incompleteness Theorem

Let $\mathcal{Z}$ be a formal system for mathematics.
1) $\mathcal{Z}$ is an r.e. set of sentences in some first order language $\mathcal{L}$.
2) $\mathcal{L}$ has terms that resemble $\underline{0}, \underline{1}, \underline{2}, \underline{3}, \ldots$ (numerals)
Note: It really has $\underline{0}, \underline{1}, +$, so $\underline{5}$ is $\underline{1}+\underline{1}+\underline{1}+\underline{1}+\underline{1}$
(Actually, any infinite sequence of distinct terms that we can generate effectively, will do.)

A set A (of numbers) is <u>definable</u> in $\mathcal{Z}$ if there exists a formula $\mathcal{F}(x)$ of $\mathcal{L}$ such that for all n

$$n \in A \iff \mathcal{Z} \vdash \mathcal{F}(\underline{n})$$

↖ "you can prove"

<u>Gödel</u>: Let $\mathcal{Z}$ be a formal system for mathematics. Suppose $\mathcal{Z}$ defines every r.e. set.* Then there exists a sentence $\mathcal{G}$ such that $\mathcal{Z} \not\vdash \mathcal{G}$ and $\mathcal{Z} \not\vdash \neg\mathcal{G}$.

*This hypothesis is fairly meaty (?), because the axioms of $\mathcal{Z}$ are r.e. But in fact normally in mathematics they're better than that; very often they're finite, & hence r.e.; or at worse you have infinitely many but it's always a recursive set of axioms. It's possible in real-life situations to give very simple examples of such sets. You can make them concrete enough so you can understand what they say, i.e., they can be about numbers and equations involving numbers, and the existence of solutions to those equations.

Proof:

Let A be a non-recursive, r.e. set defined by $\mathcal{F}$.

$\forall n$,

$n \in A$ iff $\mathcal{Z} \vdash \mathcal{F}(\underline{n})$

Suppose no such $\mathcal{G}$ exists. Then for all n, either $\mathcal{Z} \vdash \mathcal{F}(\underline{n})$ or $\mathcal{Z} \vdash \neg\mathcal{F}(\underline{n})$.

Note ①: The set of all theorems of $\mathcal{Z}$ is r.e.

Proof: The set of axioms of $\mathcal{Z}$ is r.e. (by assumption). ∴ The set of all sequences of axioms is r.e., i.e., the set of all proofs are r.e., since a proof is just a finite sequence of axioms. (The only rules we have are those of first-order logic itself, and there are only finitely many of those.)

Note ②: $\mathcal{Z}$ is consistent

Proof: $\mathcal{Z}$ defines every r.e. set. Take the empty set $\phi = \{\}$.

$n \in \{\}$ iff $\mathcal{Z} \vdash E(\underline{n})$

↑ $\mathcal{Z}$ defines the empty set with some formula $E(n)$

If $\mathcal{Z}$ were inconsistent, $E(n)$ would be provable for every n (because everything would be provable), but then every n would belong to the empty set.

But then A is recursive. The way we see A is recursive is the following: we ask the question "is n a member of A"?

? $n \in A$ — we decide this by enumerating all proofs; since $\mathcal{Z}$ is consistent, we will eventually get a proof of either $\mathcal{F}(n)$ or $\neg\mathcal{F}(\underline{n})$.

If $(\mathcal{Z} \vdash \mathcal{F}(n))$, then $n \in A$. On the other hand, if $(\mathcal{Z} \vdash \neg\mathcal{F}(n))$, then by consistency $\not\vdash \mathcal{F}(n)$, so $n \notin A$. $\therefore A$ is recursive.

But we assumed A is non-recursive (contradiction).

Recapping essential points:
- existence of r.e. sets
- definability of r.e. sets
- set of all theorems is r.e. (although this restriction is such a weird assumption that we can forget about it, because in real life we always have something better than this, as mentioned earlier)

When you take this extremely stark approach to the incompleteness theorem, you can see there's no way to get around it. Suppose you didn't like it and you decided to re-do the foundations of mathematics to get rid of it, you're faced with an impossible task, because if it's called "math", then it certainly has the power to calculate r.e. sets. And of course it's an absolute fact that in the world of nature, that is, the world of mathematics, there exists a non-recursive r.e. set; there's no getting rid of that. The only thing left to fool with (Sacks guesses) is the idea that the axioms are r.e., and some people have taken that approach. Some people have proposed a formal system(s) of mathematics where it's very tough to see some of the axioms. But this strikes Sacks as insanity; if you can't see clearly what the axioms are, this is contrary to the whole idea of the axiomatic method, which is to derive as much as we can from first principles, and the first principles are supposed to be somewhat

evident — easy to understand. Maybe we can argue about them to bits, but they're still easy to get a hold on.

Let's try to weaken one of the hypotheses. Instead of Z defining every r.e. set, let Z have the power to compute every recursive function.

Ⓐ ↓ (continued below)

Corollary (a la Church): Z has no decision procedure. (It is a fact that F is either provable or not provable, but we can't compute that fact because otherwise A would be recursive in proof above) Church's Theorem goes one notch better:

Church's Theorem: There is no decision procedure for first-order logic itself

Means: no non-logical axioms
language L has an ample
supply of relation symbols

Wittgenstein showed propositional logic has a decision procedure; he seemed to be saying that you could do this for all of logic; he tried and failed; and other people tried and failed. Church put an end to this.

There is no way you can look at a formula of first-order logic and decide whether it's valid or not, because that would constitute a decision procedure. It's true that its validity is a consequence of its syntax, the way it's put together, but

there's no way to look at it and ascertain its validity. You have to say something weaker: it's valid because of the way it's built up of the logical particles. In that sense we can rescue Wittgenstein to some degree by taking that view. But there's nothing like a truth table, which is what Wittgenstein wanted.

Church's proof was extremely obscure.

We haven't done that here, but we've come pretty close. You can see what's involved; if you had a Σ like the one mentioned earlier, but only a finite number of axioms, (and you can think of that Σ as only having one axiom by conjunction), then something is provable in Σ iff that one axiom $\rightarrow \mathcal{F}$ (?) is valid in first order logic. But we just showed that there's no decision procedure for Σ; hence there can't be a decision procedure for first order logic. The only obstacle is to show that there exists a finite Σ. That is a bit of a pain; but it can be done, because after all, all Σ has to do is express these r.e. predicates, and we gave a "sort of" (?) finite set of schemes for putting together all recursive functions. So there should be a finitary system that does that.

(A) →

We want to weaken the assumption about Σ.

Σ defines a function f $(y = f(x))$ if there exists a formula $\mathcal{F}(x,y)$ such that $\forall m \forall n$,

$$f(m) = n \text{ iff } \Sigma \vdash \mathcal{F}(\underline{m}, \underline{n})$$

Proposition: If Z defines every r.e. set, then Z defines every recursive function.

Let f be recursive.

$A_f = \{2^x \cdot 3^y \mid y = f(x)\}$ is a recursive set, hence r.e.

$n \in A_f$ iff $\vdash_{Z?} \mathcal{F}_{A_f}(\underline{n})$

$f(m) = n$ iff $2^m \cdot 3^n \in A_f$ iff $Z \vdash \mathcal{F}_{A_f}(2^{\underline{m}} \cdot 3^{\underline{n}})$

(assumes we have elements of arithmetic in Z)

(multiplication, exponentiation, order pairs of nos, ...)

Converse of proposition (Rosser)

(At first glance, the converse looks almost trivially true, but it isn't. If I can define every recursive function, why can't I define every r.e. set?)

Assume Z defines every recursive function.
Let A be r.e. in hope of defining A.
A is the range of some recursive f.
$f(m) = n$ iff $Z \vdash \mathcal{F}(\underline{m}, \underline{n})$

Proposal: To define A,

$n \in A$ iff $\exists m\,(f(m) = n) \overset{?}{\Leftrightarrow} Z \vdash \exists x\,(\mathcal{F}(x, \underline{n}))$

"maybe iff"

this is true

this is what we want to test

Test proposal:

$n \in A \Rightarrow \exists m\,(f(m) = n)$
$\Rightarrow Z \vdash \mathcal{F}(\underline{m}, \underline{n})$
$\Rightarrow Z \vdash \exists x\,\mathcal{F}(x, \underline{n})$

this step may not be reversible (no logic says we can do this)

We cannot reverse the last step on purely logical grounds.

One assumption we can make (in the spirit of Gödel; this is one of his assumptions) is ω-consistency.

Z is <u>ω-consistent</u> means there is no $F(x)$ such that all of the following are provable in Z:

$$\exists x F(x)$$
$$\neg F(0)$$
$$\neg F(1)$$
$$\neg F(2)$$
$$\vdots$$

(if Z is not ω-consistent, you can prove there exists a number with property F, and then you can prove that any particular number fails for that property F. How could that be? We know what the answer to that is because we once talked about a non-standard model for arithmetic — we know we can have infinite numbers. But still, this is hard to believe, because we also have the standard model of arithmetic, and anything I prove in Z must be true in the standard model. So if I prove that there exists a number such that $F(x)$, that means that in the standard model there's a particular number like 97. So then I can also prove $\neg F(97)$. So if you believe that the standard model for arithmetic is in fact the model for the Peano axioms, then of course you have ω-consistency. So if you believe that arithmetic has a standard model, then our usual formal systems of arithmetic are ω-consistent. So Gödel didn't worry about this. But if you're very "proof-oriented" then this looks like an (unpleasant) possibility, and it looks like demanding that Z be ω-consistent is a lot stronger

than demanding that Z be consistent (from a purely proof-theoretic point of view).)

Claim: If we have ω-consistency we can reverse the last step.

Assume Z is ω-consistent in order to reverse the last step (and so show that definability of all r.e. sets $\equiv$ definability of all recursive functions) $\uparrow$ is equiv. to

$$Z \vdash \exists x \mathcal{F}(x, \underline{n})$$

We need an m such that

$$Z \vdash \mathcal{F}(\underline{m}, \underline{n})$$

Suppose there is no such m. We intend to show

$$Z \vdash \neg \mathcal{F}(\underline{m}, \underline{n}) \text{ for all } m.$$

There is a recursive function such that $\forall m \forall n$

$f(m) = n$ iff $Z \vdash \mathcal{F}(\underline{m}, \underline{n})$

(this will work if Z is complete)

If Z is not complete: we must correct the definition of Z slightly.:

The correct definition of "Z defines a function" is:

r.e. set $\quad f(m) = n$ iff $Z \vdash \mathcal{F}(\underline{m}, \underline{n})$

r.e. set $\quad f(m) \neq n$ iff $Z \vdash \neg \mathcal{F}(\underline{m}, \underline{n})$

Then we have to check the "trivial" part of the proposition: if I can define every r.e. set, can I define every recursive function? It's the same proof: when I just have the first line of the definition

I collect the set of ordered pairs such that $2^m \cdot 3^n$ is in the set. Some logical trickery has to be used to make sure we're talking about one formula. (?)

Rosser: didn't want to assume ω-consistency.

If Z is a formal system for mathematics and Z defines every recursive function, then Z is incomplete (weaker assumption than ω-consistency).

Rosser's proof: Let A and B be recursively inseparable r.e. sets. Suppose Z is complete. We recursively separate A and B.

$$n \in A \Leftrightarrow \exists m\,(f(m)=n)$$ because A is the range of a recursive function

$$n \in B \Leftrightarrow \exists m\,(g(m)=n)$$

We want to make some connection with the formal system:

$$f(m)=n \Leftrightarrow Z \vdash \mathcal{F}(\underline{m},\underline{n})$$
$$f(m)\neq n \Leftrightarrow Z \vdash \neg\mathcal{F}(\underline{m},\underline{n})$$

(in other words, we can compute f inside of Z)

$$g(m)=n \Leftrightarrow Z \vdash \mathcal{G}(\underline{m},\underline{n})$$
$$g(m)\neq n \Leftrightarrow Z \vdash \neg\mathcal{G}(\underline{m},\underline{n})$$

Look at the formula

$$H(x) \text{ is } \exists y\left[\mathcal{F}(y,x) \wedge \forall w\left(w<y \rightarrow \neg\mathcal{G}(w,x)\right)\right]$$

Suppose Z were complete, i.e., suppose $Z \vdash H(\underline{n})$ or $Z \vdash \neg H(\underline{n})$ for all n.

The axioms of Z are still r.e., so if Z decides

every one of the $H(\underline{n})$ or $\neg H(\underline{n})$, then Z is defining some recursive set, so

$\{n \mid Z \vdash H(\underline{n})\}$ is recursive

So we're hoping that this set, call it H, separates A and B.

$$n \in A \Rightarrow \exists m \left(f(m) = n \Rightarrow Z \vdash \mathcal{F}(\underline{m}, \underline{n}) \right)$$

$A \cap B = \phi$ (are disjoint) because they're recursively inseparable

We have an m that "puts n into A". Now n is certainly not a member of B; in particular ?

$$\Rightarrow Z \vdash \neg \mathcal{G}(\underline{w}, \underline{n}) \quad (\forall w < n)$$

$$n \in A \Rightarrow Z \vdash \mathcal{F}(\underline{m}, \underline{n}) \wedge \forall w (w < \underline{m} \rightarrow \neg \mathcal{G}(w, \underline{n}))$$
$$\Rightarrow Z \vdash \exists y [\mathcal{F}(y, \underline{n}) \wedge \forall w (w < y \rightarrow \neg \mathcal{G}(w, \underline{n}))$$
$$\Rightarrow Z \vdash H(\underline{n})$$

$\therefore A \subseteq H$ ← a recursive set

We still need $H \cap B = \phi$. "H doesn't touch B"

Suppose it does. Let $n \in H \cap B$. Then

① $Z \vdash \mathcal{G}(\underline{m}, \underline{n})$ for some m ← because $n \in B$

② $Z \vdash \exists y [\mathcal{F}(y, \underline{n}) \wedge \forall w (w < y \rightarrow \neg \mathcal{G}(w, \underline{n}))]$ ← because $n \in H$

Imagine that the y was actually finite; then it would be putting n into A. For example if y was 6 we would have a proof of $\mathcal{F}(6, \underline{n})$. That would mean, in fact, that n is a member of A and hence can't possibly be a member of B. So there's no hope of replacing y by anything finite. But I claim that means (speaking intuitively) that y is infinite. So when you say $\forall w (w < y)$, w does not put n into B. So the contradiction is here: I have a definite $\underline{m}$ (in ①?). Now if

there is a y less than or equal to that m, that works over here (②?). Then we actually got some n in A, hence it can't possibly be in B. So I can assume that y is in fact bigger than m. But that implies $\neg \beta(m, n)$ is actually provable, which contradicts ①. So $\mathbb{Z}$ is inconsistent (contradiction). ~~[illegible]~~ ($\mathbb{Z}$ is consistent since it computes every recursive function properly.)

Norman D. Megill
18.511 HW
Assigned: 9/14/89
Due: 9/21/89

Claim: There exists an effective method for deciding whether or not an expression is a WFF.

Let $\mathcal{F}$, $\mathcal{G}$, $\mathcal{H}$ be finite sequences of atomic symbols. (Actual atomic symbols will be underlined for clarity.)

Let c be one of $\rightarrow \leftrightarrow \vee \wedge$. Let A_m be a propositional letter.

Let $S_i(\mathcal{F})$ be the shortest subsequence of $\mathcal{F}$ which starts at position i and has an equal number of (and). (If there is no such subsequence, let $S_i(\mathcal{F})$ be an (the?) empty sequence.)

By the way: (,) aren't propositional connectives; the latter are truth functional.

Lemma. If $\mathcal{F}$ is a WFF, then $S_1(\mathcal{F}) = \mathcal{F}$.

Proof: Construct $S_1(\mathcal{F})$ in parallel with $\mathcal{F}$, and use induction on the number of propositional connectives other than (and) in $\mathcal{F}$. During the construction, note that the count of) never exceeds the count of (when the atomic symbols in $\mathcal{F}$ are scanned from left to right; this remains true when new (and) are added.

$S_1(\mathcal{F}) = \mathcal{F}$ is obvious

Define a function TEST($\mathcal{F}$) whose range is {T, F}:

TEST($\mathcal{F}$) = T if $\mathcal{F} = (A_m)$

= TEST($S_3(\mathcal{F})$) if $\mathcal{F} = (\neg S_3(\mathcal{F}))$

= TEST($S_2(\mathcal{F})$) $\wedge$ TEST($S_i(\mathcal{F})$) if $\mathcal{F} = (S_2(\mathcal{F}) \; c \; S_i(\mathcal{F}))$ where $i-3$ is the length of $S_2(\mathcal{F})$.

= F otherwise.

This should be written differently

"$\wedge$" means T if both TEST's are T, F otherwise.

replace

= T if Test($S_2(\mathcal{F})$) = T and Test($S_i(\mathcal{F})$) = T

This is already a prop. connective

Test($S_i(\mathcal{F})$) = otherwise

TEST($\mathcal{F}$) = T if Test($S_2(\mathcal{F})$) = T and Test($S_i(\mathcal{F})$) = T

Need to be specified about i — even in my replacement.

Theorem TEST($\mathcal{F}$) = T iff $\mathcal{F}$ is a WFF.

Proof by induction on the number n of propositional connectives in $\mathcal{F}$ other than (and)! We compute one F.TEST in parallel with the construction of $\mathcal{F}$.

a syntactic element, part of

it is ambiguous. No

n=0: If $\mathcal{F} = (A_m)$, TEST($\mathcal{F}$) = T, otherwise TEST($\mathcal{F}$) = F.

$\wedge$, 8, °

$n>0$: The possible ways of constructing $\mathcal{F}$ correspond exactly to the cases defining TEST($\mathcal{F}$). For brevity we will provide details for $\mathcal{F} = (\mathcal{G} \Rightarrow \mathcal{H})$ only:

$$\begin{aligned}
\text{TEST}(\mathcal{F}) &= \text{TEST}((\mathcal{G} \Rightarrow \mathcal{H})) && \text{WFF construction rule}\\
&= \text{TEST}((S_1(\mathcal{G}) \Rightarrow S_1(\mathcal{H}))) && \text{by Lemma}\\
&= \text{TEST}((S_3(\mathcal{F}) \Rightarrow S_2(\mathcal{F}))) && \text{by def. of } S_i()\\
&= \text{TEST}(S_3(\mathcal{F})) \wedge \text{TEST}(S_2(\mathcal{F})) && \text{by def. of TEST}\\
&= \text{TEST}(S_1(\mathcal{G})) \wedge \text{TEST}(S_1(\mathcal{H})) && \text{by def. of } S_i()\\
&= \text{TEST}(\mathcal{G}) \wedge \text{TEST}(\mathcal{H}) && \text{by Lemma}\\
&= T \wedge T && \text{by induction hypotheses}\\
&= T && \text{by def. of "}\wedge\text{"}
\end{aligned}$$

(Note: these are the first occurrences of the words "valid rules" on this page)

What are "valid rules" in this proof?

If $\mathcal{F}$ is not a WFF, there must be step in its construction where one of the ~~valid rules~~ is not followed. Because of the correspondence between these rules and the cases of the TEST definition, TEST will be F in this step. By the definition of TEST, any F computed during the construction of $\mathcal{F}$ will propagate to the final value of TEST.

Despite ambiguity of "$\wedge$" and improper restrict to one case (textbooks, not problem sets, are allowed to appeal to brevity to omit details) I will concede that you have shown that if $\mathcal{F}$ is a WFF, TEST($\mathcal{F}$)=T.

But I don't see how you intend to get the converse of your theorem.

The lemma allows the moves numbered ① above only ~~is this case~~ when $\mathcal{G}$ and $\mathcal{H}$ are WFF. If they are not, how do we know what TEST($\mathcal{F}$) is? More detail needed here.

valid
true
} Sem.

9/12

Mr. Picard - This is a more detailed version of the converse part of HW #1's proof. I would appreciate your comments.
-N. Megill

(See old HW attached for reference)

Assume $\mathcal{F}$ is not a WFF. (Show this implies $TEST(\mathcal{F})=F$.)

Use induction on the number of atomic symbols n in $\mathcal{F}$ (i.e., the length n of $\mathcal{F}$).

$n=0,1,2$: $TEST(\mathcal{F})$ will be F (only case 4 of TEST can be matched; the other cases need at least 3 symbols).

$n=3$: Case 1 of TEST cannot be matched since (A_m) is a WFF and $\mathcal{F}$ is not by hypothesis.

Case 2: The only $\mathcal{F}$ that can match $(\neg S_3(\mathcal{F}))$ is $\mathcal{F}=(\neg)$, where $S_3(\mathcal{F})$ is the empty sequence. $TEST(S_3(\mathcal{F}))=F$, so $TEST(\mathcal{F})=F$.

Case 3: The only $\mathcal{F}$ that can match $(S_2(\mathcal{F}) \; c \; S_i(\mathcal{F}))$ [where $c\in\{\vee,\wedge,\rightarrow,\leftrightarrow\}$ and $i-3=$ length of $S_2(\mathcal{F})$ and $i\leq n$] is $\mathcal{F}=(c)$. In this case both $S_2(\mathcal{F})$ and $S_i(\mathcal{F})[=S_3(\mathcal{F})]$ are the empty sequence, so $TEST(\mathcal{F})=F\&F=F$.

Anything else will make $TEST(\mathcal{F})=F$ (case 4).

$n>3$: (Induction hypothesis) Assume $TEST(\mathcal{G})=F$ for all non-WFF sequences $\mathcal{G}$ with length $<n$.

Case 1 of TEST cannot be matched since $n\neq 3$.

If case 2 is matched, $S_3(\mathcal{F})$ cannot be a WFF because otherwise $\mathcal{F}$ would be a WFF, contrary to hypothesis. Since $S_3(\mathcal{F})$ is shorter than $\mathcal{F}$, $TEST(S_3(\mathcal{F}))=F$ by the induction hypothesis, so $TEST(\mathcal{F})=F$.

If case 3 is matched, $S_2(\mathcal{F})$ and $S_i(\mathcal{F})$ cannot both be WFF's because otherwise $\mathcal{F}$ would be a WFF, contrary to hypothesis. Since $S_2(\mathcal{F})$ and $S_i(\mathcal{F})$ are shorter than $\mathcal{F}$, either $TEST(S_2(\mathcal{F}))=F$ or

TEST($S_i(\mathcal{F})$) = F (or both) by the induction hypothesis. Therefore TEST($\mathcal{F}$) = F.

Anything else will make TEST($\mathcal{F}$) = F (case 4).

By induction, then, any finite-length non-WFF sequence $\mathcal{F}$ will cause TEST($\mathcal{F}$) to have a value of F.

No comments.
It seems right.

Norman D. Megill
18.511 HW
assigned: 9/21/89
Due: 9/28/89

HW #2 If each finite submap of M has a coloring, then M has a coloring

Definitions:

a map M is a set of countries $\{C_0, C_1, \ldots\}$

a color is an element of the set $\{K_1, K_2, K_3, K_4\}$

a map with preassignments M_P is a map M together with a set of preassignments $\{P_{i_1}, P_{i_2}, \ldots\}$ that associate fixed colors with countries $\{C_{i_1}, C_{i_2}, \ldots\}$. Thus $M_P = \{C_0, C_1, \ldots\} \cup \{P_{i_1}, P_{i_2}, \ldots\}$.

(Specifically, P_i is an ordered pair $\langle C_i, K_m \rangle$)

Note that some, none, or all of $\{C_0, C_1, \ldots\}$ may have an associated preassignment. In addition, there may be a P_i with no corresponding C_i, in which case P_i has (i.e., is ignored) no meaning; this is done to allow taking arbitrary subsets of M_P.

From this point on, the term map may refer to a map with or without preassignments.

12

a coloring K of a map is a function that assigns to each country C_i (that does not have a preassignment) a color K_m such that: if country C_i borders C_j, C_i and C_j have different colors, for all C_i and C_j (including those with preassignments). If C_i has a preassignment P_i, then K assigns to C_i the color associated with the preassignment.

Note that K may not exist. Also, if the preassignments violate the border condition, K is said not to exist. If a country has more than one preassignment, K is said not to exist.

a map is colorable if it has a coloring.

a map is finitely colorable if each finite subset has a coloring.

Extension Lemma: If a map M is finitely colorable, then a preassignment P_i exists for each country $C_i \in M$ such that $M \cup \{P_i\}$ is finitely colorable.

Proof:

If country C_i already has a preassignment, then $P_i \in M$, so $M \cup \{P_i\} = M$.

If country C_i has no preassignment, we construct a proof by contradiction. Suppose the lemma is false. Then all of the following 4 statements are true:

$M \cup \{P_i\}$ is not finitely colorable if P_i associates K_1 w/ C_i
" " " " " " " " K_2 " "
" " " " " " " " K_3 " "
" " " " " " " " K_4 " "

These imply (by definition of "finitely colorable"):

$\exists$ finite $M_1 \subseteq M$ s.t. $M_1 \cup \{P_i\}$ is not colorable if P_i associates K_1 with C_i
" " M_2 " " " " " " " K_2 " "
" " M_3 " " " " " " " K_3 " "
" " M_4 " " " " " " " K_4 " "

Note: C_i must be in all of $P_1, \ldots, P_n$ because otherwise P_i would be ignored (irrelevant) and $M \cup \{P_i\}, \ldots$ would be colorable

However, $M_1 \cup M_2 \cup M_3 \cup M_4 \cup \{C_i\}$ is a finite subset of M, so by hypothesis there exists a coloring K for $M_1 \cup M_2 \cup M_3 \cup M_4 \cup \{C_i\}$. Pick one such K. Assign to P_i the color that this K assigns to C_i. Then $M \cup \{P_i\}$ is finitely colorable. (Proof by contradiction.)

Proof of main theorem:

Suppose M (a map without preassignments) is finitely colorable.

Define by recursion $M_0, M_1, \ldots$

Let $M_0 = M$

Assume $M_0, \ldots, M_n$ have been defined.
Assume $M_0 \subseteq M_1 \subseteq \ldots \subseteq M_n$
Assume M_n is finitely colorable.

By extension lemma, a preassignment P_n exists for country C_n such that $M_n \cup \{P_n\}$ is finitely colorable. Let $M_{n+1} = M_n \cup \{P_n\}$, where P_n is any such preassignment.

Then:

$M_0, \ldots, M_{n+1}$ will be defined
$M_0 \subseteq M_1 \subseteq \ldots \subseteq M_{n+1}$
M_{n+1} is finitely colorable.

Let $M_\infty = \bigcup_n M_n$. M_∞ is finitely colorable because each finite subset of M_∞ is contained in some M_n.

Let a function K assign to each country C_i in M the color associated with C_i by P_i in M_∞.

Final claim: K is a coloration of M, i.e., for any country C_i in M, the border condition is met.

Proof: Let M_N be the map of C_i and all of its k neighbors: $M_N = \{C_i, C_{N_1}, \ldots, C_{N_k}\}$. M_N is a finite subset of M_∞. Therefore M_N is colorable. Therefore the border condition of C_i is met. Since C_i is arbitrary, the border condition for all countries is met by the function K. Therefore K is a coloration of M.

HW #3 (a) Show $\{\neg, \wedge\}$ is complete.

We assume $\{\neg, \wedge, \vee\}$ is complete (shown in classroom).

Consider the truth tables for $(\mathcal{F} \vee \mathcal{G})$ and $(\neg((\neg\mathcal{F}) \wedge (\neg\mathcal{G})))$.

$\mathcal{F}$	$\mathcal{G}$	$(\mathcal{F} \vee \mathcal{G})$	$(\neg((\neg\mathcal{F}) \wedge (\neg\mathcal{G})))$
T	T	T	T
F	T	T	T
T	F	T	T
F	F	F	F

The truth tables are the same, so $(\mathcal{F} \vee \mathcal{G})$ can be replaced by $(\neg((\neg\mathcal{F}) \wedge (\neg\mathcal{G})))$ in a WFF. When this is done, all truth values of the new WFF will have the same result as those of the old (by induction, starting at the point where the replacement was made). Therefore, $\{\neg, \wedge\}$ is complete.

(on the # of propositional connectives in the WFF)

(b) Show $\{\vee, \wedge\}$ is not complete.

Consider the truth tables of $\vee$ and $\wedge$:

$\mathcal{F}$	$\mathcal{G}$	$\mathcal{F} \vee \mathcal{G}$	$\mathcal{F} \vee \mathcal{G}$
T	T	T	T
F	T	T	F
T	F	T	F
F	F	F	F

(Look at first line of truth table.)

By induction on the number of propositional connectives, any WFF constructed from $\vee$ and $\wedge$ will have a truth value of T if all of its propositional letters are assigned a value of T.

On the other hand, the WFF $(\neg(A_0))$ has a truth value of F if A_0 is assigned a value of T.

Therefore $\{\vee, \wedge\}$ is not complete because it cannot construct a WFF with this property.

(c) Find a single binary connective that is complete.

Define a propositional connective $(\mathcal{F} \mid \mathcal{G})$ ("NAND"):

$\mathcal{F}$	$\mathcal{G}$	$(\mathcal{F} \mid \mathcal{G})$
T	T	F
F	T	T
T	F	T
F	F	T

Consider the following two truth tables.

$\mathcal{F}$	$\mathcal{G}$	$(\mathcal{F} \mid \mathcal{F})$	$((\mathcal{F} \mid \mathcal{G}) \mid (\mathcal{F} \mid \mathcal{G}))$
T	T	F	T
F	T	T	F
T	F	F	F
F	F	T	F

These match the truth tables of $(\neg \mathcal{F})$ and $(\mathcal{F} \wedge \mathcal{G})$: $\{\neg, \wedge\}$ was shown above to be complete. Therefore $\{\mid\}$ is complete.

(Note: Of the 16 possible binary connectives, it appears that only NAND and NOR are individually complete.)

Norman D. Megill
18.511
HW assigned 9/28/89
HW due 10/5/89

HW#4: $\Gamma \vdash \mathcal{F}$ iff $\Gamma \models \mathcal{F}$

We will break the proof down into Lemmas whose outline follows:

Index

Note: If $\Gamma = \phi$, only Lemmas 2.3 through 2.5 should be used, and $\mathcal{H}$ should be replaced by $\mathcal{F}$ in 2.2 and 2.5. "Lemma 2.2" becomes the hypothesis $\models \mathcal{F}$.

Conventions:

① a WFF is assumed to have the propositional connectives $\{\vee, \wedge, \neg\}$ only. We will define $\{\rightarrow, \Leftrightarrow\}$:

$(a \rightarrow B)$ is an abbreviation for $(\neg a \vee B)$
$(a \Leftrightarrow B)$ " " " " $((a \rightarrow B) \wedge (B \rightarrow a))$.

② $(\mathcal{F}_1 \wedge \mathcal{F}_2 \wedge \mathcal{F}_3 \wedge \ldots \wedge \mathcal{F}_n)$ is an abbreviation for

$((\ldots((\mathcal{F}_1 \wedge \mathcal{F}_2) \wedge \mathcal{F}_3) \wedge \ldots) \wedge \mathcal{F}_n)$

(i.e., association of parentheses from the left.

Similarly for $(\mathcal{F}_1 \vee \ldots \vee \mathcal{F}_n)$. — If $n=1$, this abbreviation means $\mathcal{F}_1$.

③ The axioms and rules will be presented explicitly where needed and enclosed in boxes. This is done to eliminate the need to cross-reference a list, to make reading the proof easier! E.g.:

Axiom $a \rightarrow a$

Rule $\dfrac{a \rightarrow B,\ a}{B}$

No claim is made that the axioms and rules are independent or in simplest form. In many cases a more complex form is chosen to reduce the number of steps in the proof (& make reading it easier, hopefully).

Lemma 1. If $\Gamma \vdash \mathcal{F}$, then $\Gamma \models \mathcal{F}$

By definition of $\Gamma \vdash \mathcal{F}$ there is a deduction (sequence of formulas) $\mathcal{F}_0, \ldots, \mathcal{F}_{n-1}, \mathcal{F}$ (for convenience, let $\mathcal{F}$ be called $\mathcal{F}_n$) such that:

① $\mathcal{F}_i \in \Gamma$
or ② $\mathcal{F}_i$ is an axiom
or ③ $\mathcal{F}_i$ is the result of a rule applied to some formula(s) from the sequence $\mathcal{F}_0, \ldots, \mathcal{F}_{i-1}$.

We prove that $\Gamma \models \mathcal{F}_n$ by induction on the number n of formulas in the deduction.

Induction hypothesis: Assume that $\Gamma \models \mathcal{F}_i$, i.e., $V(\Gamma) = T \Rightarrow V(\mathcal{F}_i) = T$, for each $i < n$.

Induction step (which becomes the basis step when $n = 0$):

If $\mathcal{F}_n \in \Gamma$, then $V(\mathcal{F}_n) = T$ when $V(\Gamma) = T$.
If $\mathcal{F}_n$ is an axiom, then $V(\mathcal{F}_n) = T$ for all V (by soundness requirement, an axiom must be a tautology).
If $\mathcal{F}_n$ is the result of a rule, then since any V such that $V(\Gamma) = T$ will make $V(\mathcal{F}_i) = T$ $(i < n)$ (by induction hypothesis), so that $V(\mathcal{F}_n) = T$ (by soundness requirement of a rule: truth is preserved).

Therefore, $V(\Gamma) = T \Rightarrow V(\mathcal{F}_n) = T$, i.e., $\boxed{\Gamma \models \mathcal{F}_n}$.

Lemma 2.1. If $\Gamma \models \mathcal{F}$, then there exists a finite $\Gamma_0 \subseteq \Gamma$ such that $\Gamma_0 \models \mathcal{F}$.

Proof: Suppose not. Then for each finite $\Gamma_0 \subseteq \Gamma$, there is a valuation V that makes $V(\Gamma_0) = T$ but $V(\mathcal{F}) = F$, i.e., $V((\neg\mathcal{F})) = T$. By compactness theorem, there is a V such that $V(\Gamma) = T$ and $V((\neg\mathcal{F})) = T$, i.e., $V(\mathcal{F}) = F$. This contradicts the hypothesis: $\Gamma \models \mathcal{F}$ means (by definition) $V(\Gamma) = T \Rightarrow V(\mathcal{F}) = T$.

Lemma 2.2. Suppose $T_0 \vdash \mathcal{F}$ where $T_0 = \{\mathcal{G}_1, \ldots, \mathcal{G}_m\}$ is finite. Then $\vdash ((\mathcal{G}_1 \wedge \mathcal{G}_2 \wedge \ldots \wedge \mathcal{G}_m) \to \mathcal{F})$.

Notational convention: $(\mathcal{G}_1 \wedge \mathcal{G}_2 \wedge \ldots \wedge \mathcal{G}_m)$ means $((\ldots((\mathcal{G}_1 \wedge \mathcal{G}_2) \wedge \mathcal{G}_3) \wedge \ldots) \wedge \mathcal{G}_m)$ (parentheses associated from the left).

Sublemma: $V((\mathcal{G}_1 \wedge \ldots \wedge \mathcal{G}_m)) = T$ iff $V(\mathcal{G}_i) = T$ for $1 \leq i \leq m$.

Proof by induction on m:

Induction basis. $V(\mathcal{G}_1) = T$ iff $V(\mathcal{G}_1) = T$ (identity)

Induction step. Let $\mathcal{G}$ be $(\mathcal{G}_1 \wedge \ldots \wedge \mathcal{G}_{m-1})$.

Assume $V(\mathcal{G}) = T$ iff $V(\mathcal{G}_i) = T$ for $1 \leq i \leq m-1$.

$V((\mathcal{G} \wedge \mathcal{G}_m)) = T$ iff $V(\mathcal{G}) = T$ and $V(\mathcal{G}_m) = T$ (by definition of valuation),

i.e., iff $[V(\mathcal{G}_i) = T$ for $1 \leq i \leq m-1]$ and $V(\mathcal{G}_m) = T$,

i.e., iff $V(\mathcal{G}_i) = T$ for $1 \leq i \leq m$. □

Proof of lemma: Consider an arbitrary valuation V.

If $V(\mathcal{G}_i) = T$ for all i, $1 \leq i \leq m$, then:

$V((\mathcal{G}_1 \wedge \ldots \wedge \mathcal{G}_m)) = T$ by sublemma

$V(\mathcal{F}) = T$ by definition of $T_0 \vdash \mathcal{F}$.

$\therefore V(((\mathcal{G}_1 \wedge \ldots \wedge \mathcal{G}_m) \to \mathcal{F})) = T$ by definition of "$\to$". your defn?

If $V(\mathcal{G}_i) = F$ for some i, then:

$V((\mathcal{G}_1 \wedge \ldots \wedge \mathcal{G}_m)) = F$ by sublemma

$\therefore V(((\mathcal{G}_1 \wedge \ldots \wedge \mathcal{G}_m) \to \mathcal{F})) = T$ by definition of "$\to$".

Therefore all valuations of $((\mathcal{G}_1 \wedge \ldots \wedge \mathcal{G}_m) \to \mathcal{F})$ are T

i.e. $((\mathcal{G}_1 \wedge \ldots \wedge \mathcal{G}_m) \to \mathcal{F})$ is a tautology.

i.e. $\boxed{\vdash ((\mathcal{G}_1 \wedge \ldots \wedge \mathcal{G}_m) \to \mathcal{F})}$

Lemma 2.3 If $\vdash ((\mathcal{G}_0 \wedge \ldots \wedge \mathcal{G}_m) \rightarrow \mathcal{F})$ then
$\models \mathcal{H}_{CNF}$
where $\vdash ((\mathcal{G}_0 \wedge \ldots \wedge \mathcal{G}_m) \rightarrow \mathcal{F}) \Leftrightarrow \mathcal{H}_{CNF}$
and $\mathcal{H}_{CNF}$ is in conjunctive normal form.

Proof: By Sublemma 2.3.1 (CNF), there exists a WFF $\mathcal{H}_{CNF}$ in conjunctive normal form such that $\vdash (((\mathcal{G}_0 \wedge \ldots \wedge \mathcal{G}_m) \rightarrow \mathcal{F}) \Leftrightarrow \mathcal{H}_{CNF})$.

By Lemma 1, $\models (((\mathcal{G}_0 \wedge \ldots \wedge \mathcal{G}_m) \rightarrow \mathcal{F}) \Leftrightarrow \mathcal{H}_{CNF})$.

By definition of valuation of $\Leftrightarrow$, for an arbitrary V we have

$$V(((\mathcal{G}_0 \wedge \ldots \wedge \mathcal{G}_m) \rightarrow \mathcal{F}) \Leftrightarrow \mathcal{H}_{CNF})) = T \text{ iff}$$
$$V(((\mathcal{G}_0 \wedge \ldots \wedge \mathcal{G}_m) \rightarrow \mathcal{F})) = V(\mathcal{H}_{CNF}).$$

Since $\models ((\mathcal{G}_0 \wedge \ldots \wedge \mathcal{G}_m) \rightarrow \mathcal{F})$ by hypothesis and $\models (((\mathcal{G}_0 \wedge \ldots \wedge \mathcal{G}_m) \rightarrow \mathcal{F}) \Leftrightarrow \mathcal{H}_{CNF})$ By Lemma 2.3.1, we have:

$$T = T \text{ iff } T = V(\mathcal{H}_{CNF})$$
$$\therefore V(\mathcal{H}_{CNF}) = T$$
$$\therefore \models \mathcal{H}_{CNF}$$

—

Conjunctive Normal Form

Sublemma 2.3.1 (CNF) For any WFF $\mathcal{F}$, there exists a WFF $\mathcal{G}$ such that $\vdash(\mathcal{F}\Leftrightarrow\mathcal{G})$ and where $\mathcal{G}$ is a member of the set CNF of formulas defined recursively as follows:

First, define CNF "conjunct":
1. (A_n) is a conjunct, where A_n is an atomic letter.
2. $(\neg(A_n))$ " " " " " " " " " "
3. If C_1, C_2 are conjuncts then $(C_1 \vee C_2)$ is a conjunct.

Next, define the set CNF:
1. $C \in$ CNF, where C is a conjunct.
2. If $\mathcal{G}, \mathcal{H} \in$ CNF then $(\mathcal{G}\wedge\mathcal{H}) \in$ CNF.

Proof:

By sublemma 2.3.1.1 (NNF), $\mathcal{F}$ is equivalent to a formula $\mathcal{G}_{NNF}$ in negation normal form:

$$\vdash(\mathcal{F}\Leftrightarrow\mathcal{G}_{NNF})$$

If we show $\vdash(\mathcal{G}_{NNF}\Leftrightarrow\mathcal{G})$, then by

Rule $\dfrac{(\alpha\Leftrightarrow\beta),(\beta\Leftrightarrow\gamma)}{(\alpha\Leftrightarrow\gamma)}$

it follows that $\vdash(\mathcal{F}\Leftrightarrow\mathcal{G})$. Therefore we can assume without loss of generality that $\mathcal{F}$ is in NNF.

We use induction on the number of $\vee$ and $\wedge$ binary connectives, n, in $\mathcal{F}$. ($\neg$ irrelevant because $\mathcal{F}$ is in NNF).

$n=0$: $\mathcal{F}$ must be (A_n) or $\neg(A_n)$.
Let $\mathcal{G}$ be $\mathcal{F}$, then $\mathcal{G}$ is in CNF and $\vdash(\mathcal{F}\Leftrightarrow\mathcal{G})$ by Axiom $(\alpha\Leftrightarrow\alpha)$.

2.3.1 (cont.)

$n > 0$: We assume that if $\mathcal{F}$ has $< n$ binary connectives $\vee$'s $+ \wedge$'s, then $\exists \mathcal{G}_i \in CNF$ s.t. $\vdash (\mathcal{F}_i \leftrightarrow \mathcal{G}_i)$.

Case 1: $\mathcal{F}$ is of the form $(\mathcal{F}_1 \wedge \mathcal{F}_2)$. $\mathcal{F}_1$ and $\mathcal{F}_2$ each have less than n binary connectives. By the induction hypothesis, $\exists \mathcal{G}_1, \mathcal{G}_2 \in CNF$ s.t. $\vdash (\mathcal{F}_1 \leftrightarrow \mathcal{G}_1)$ and $\vdash (\mathcal{F}_2 \leftrightarrow \mathcal{G}_2)$.

By $\boxed{\text{Rule } \dfrac{(a_1 \leftrightarrow B_1), (a_2 \leftrightarrow B_2)}{((a_1 \wedge a_2) \leftrightarrow (B_1 \wedge B_2))}}$, we get

$$\vdash ((\mathcal{F}_1 \wedge \mathcal{F}_2) \leftrightarrow (\mathcal{G}_1 \wedge \mathcal{G}_2)).$$

Let $\mathcal{G}$ be $(\mathcal{G}_1 \wedge \mathcal{G}_2)$. Then $\mathcal{G} \in CNF$, and $\vdash (\mathcal{F} \leftrightarrow \mathcal{G})$.

Case 2: $\mathcal{F}$ is $(\mathcal{F}_1 \vee \mathcal{F}_2)$.

Subcase 2.1: $\mathcal{F}_1$ is $(\mathcal{F}_{11} \wedge \mathcal{F}_{12})$. $\mathcal{F}$ is $((\mathcal{F}_{11} \wedge \mathcal{F}_{12}) \vee \mathcal{F}_2)$.

By $\boxed{\text{Axiom } (((a \wedge B) \vee c) \leftrightarrow ((a \vee c) \wedge (B \vee c)))}$, we have $\vdash (\mathcal{F} \leftrightarrow ((\mathcal{F}_{11} \vee \mathcal{F}_2) \wedge (\mathcal{F}_{12} \vee \mathcal{F}_2)))$.

Note that $(\mathcal{F}_{11} \vee \mathcal{F}_2)$ and $(\mathcal{F}_{12} \vee \mathcal{F}_2)$ each have fewer binary connectives than $\mathcal{F}$. By the induction hypothesis, $\exists \mathcal{G}_1', \mathcal{G}_2' \in CNF$ s.t. $\vdash ((\mathcal{F}_{11} \vee \mathcal{F}_2) \leftrightarrow \mathcal{G}_1')$ and $\vdash ((\mathcal{F}_{12} \vee \mathcal{F}_2) \leftrightarrow \mathcal{G}_2')$.

By $\boxed{\text{Rule } \dfrac{(a_1 \leftrightarrow B_1), (a_2 \leftrightarrow B_2)}{((a_1 \wedge a_2) \leftrightarrow (B_1 \wedge B_2))}}$

we get $\vdash (((\mathcal{F}_{11} \vee \mathcal{F}_2) \wedge (\mathcal{F}_{12} \vee \mathcal{F}_2)) \leftrightarrow (\mathcal{G}_1' \wedge \mathcal{G}_2'))$.

By $\boxed{\text{Rule } \dfrac{(a \leftrightarrow B), (B \leftrightarrow C)}{(a \leftrightarrow C)}}$

we get $\vdash (\mathcal{F} \leftrightarrow (\mathcal{G}_1' \wedge \mathcal{G}_2'))$.

Let $\mathcal{G}$ be $(\mathcal{G}_1' \wedge \mathcal{G}_2')$. Then $\mathcal{G} \in CNF$, and $\vdash (\mathcal{F} \leftrightarrow \mathcal{G})$.

2.3.1 (cont.)

Subcase 2.2: $\mathcal{F}_2$ is $(\mathcal{F}_{21} \wedge \mathcal{F}_{22})$. $\mathcal{F}$ is $(\mathcal{F}_1 \vee (\mathcal{F}_{21} \wedge \mathcal{F}_{22}))$.

By Axiom $((\alpha \vee (\beta \wedge \gamma)) \leftrightarrow ((\alpha \vee \beta) \wedge (\alpha \vee \gamma)))$

we have $\vdash (\mathcal{F} \leftrightarrow ((\mathcal{F}_1 \vee \mathcal{F}_{21}) \wedge (\mathcal{F}_1 \vee \mathcal{F}_{22})))$.
Note that $(\mathcal{F}_1 \vee \mathcal{F}_{21})$ and $(\mathcal{F}_1 \vee \mathcal{F}_{22})$ each have fewer binary connectives than $\mathcal{F}$.
By the induction hypothesis, $\exists\, \mathcal{G}_1, \mathcal{G}_2 \in CNF$ s.t. $\vdash ((\mathcal{F}_1 \vee \mathcal{F}_{21}) \leftrightarrow \mathcal{G}_1)$ and $\vdash ((\mathcal{F}_1 \vee \mathcal{F}_{22}) \leftrightarrow \mathcal{G}_2)$.

By Rule $\dfrac{(\alpha_1 \leftrightarrow \beta_1),\ (\alpha_2 \leftrightarrow \beta_2)}{((\alpha_1 \wedge \alpha_2) \leftrightarrow (\beta_1 \wedge \beta_2))}$,

we get $\vdash ((\mathcal{F}_1 \vee \mathcal{F}_{21}) \wedge (\mathcal{F}_1 \vee \mathcal{F}_{22}) \leftrightarrow (\mathcal{G}_1 \wedge \mathcal{G}_2))$.

By Rule $\dfrac{(\alpha \leftrightarrow \beta),\ (\beta \leftrightarrow \gamma)}{(\alpha \leftrightarrow \gamma)}$

we get $\vdash (\mathcal{F} \leftrightarrow (\mathcal{G}_1 \wedge \mathcal{G}_2))$.
Let $\mathcal{G}$ be $(\mathcal{G}_1 \wedge \mathcal{G}_2)$. Then $\mathcal{G} \in CNF$, and
$\vdash (\mathcal{F} \leftrightarrow \mathcal{G})$.

Subcase 2.3: $\mathcal{F}_1$ and $\mathcal{F}_2$ are both CNF "conjuncts" (see CNF definition above): Let $\mathcal{G}$ be $(\mathcal{F}_1 \vee \mathcal{F}_2)$; $\mathcal{G} \in CNF$ and by Axiom $\alpha \leftrightarrow \alpha$, $\vdash (\mathcal{F} \leftrightarrow \mathcal{G})$.

i.e.: neither $\mathcal{F}_1$ nor $\mathcal{F}_2$ has a conjunction in its scope?

The only conjunction

Subcase 2.4: $\mathcal{F}_1$ or $\mathcal{F}_2$ (or both) is a disjunction with a conjunction in its scope. (This covers all remaining possibilities.)

Let $H = \{H_1, \ldots, H_m\}$ be the largest set of disjunction formulas that can be combined with $\vee$ only to result in $\mathcal{F}$.

e.g.: If $\mathcal{F}$ is $(\mathcal{F}_1 \vee \mathcal{F}_2) \vee (\mathcal{F}_3 \vee (\mathcal{F}_4 \wedge \mathcal{F}_5))$,
then $H = \{\mathcal{F}_1, \mathcal{F}_2, \mathcal{F}_3, (\mathcal{F}_4 \wedge \mathcal{F}_5)\}$.

2.3.1 (cont.)

By Sublemma 2.3.1.2,

$$\vdash (\mathcal{F} \Leftrightarrow (H_1 \vee \ldots \vee H_m))$$

Now by the hypothesis for this subcase, at least one of $\{H_1, \ldots, H_m\}$, say H_i, is in the form $(H_{i,1} \wedge H_{i,2})$. (Otherwise H would not be the largest set.)

If $i \neq m$, then move H_i to the end of $(H_1 \vee \ldots \vee H_m)$, to get $(H_1 \vee \ldots \vee H_m \vee H_i)$, called H_S.

If $i = m$, let H_S be H_i.

By Sublemma 2.4.2 ("scramble"),

$$\vdash ((H_1 \vee \ldots \vee H_m) \Leftrightarrow H_S).$$

H_S is of the form $((H_{S0}) \vee (H_{s,1} \wedge H_{s,2}))$ (see definition of $\vee \ldots \vee$, p.2 of H.W.) This form matches Subcase 2.2 above. Note that H_S has exactly as many binary connectives as $\mathcal{F}$. Therefore we can use the procedure in Subcase 2.2 to obtain

$$\vdash (H_S \Leftrightarrow \mathcal{G}) \quad \text{where } \mathcal{G} \in \text{CNF}.$$

With 2 applications of Rule $\dfrac{(\alpha \Leftrightarrow \beta), (\beta \Leftrightarrow \gamma)}{(\alpha \Leftrightarrow \gamma)}$

we obtain $\vdash (\mathcal{F} \Leftrightarrow \mathcal{G})$.

negation normal Form (NNF)

Sublemma 2.3.1.1 For any WFF $\mathcal{F}$, there exists a WFF $\mathcal{G}$ such that $\vdash(\mathcal{F}\Leftrightarrow\mathcal{G})$ and where $\mathcal{G}$ is a member of the set NNF of formulas defined recursively as follows:

1. $(A_n) \in NNF$, where A_n is an atomic letter.
2. $(\neg(A_n)) \in NNF$, where A_n is an atomic letter.
3. If $\mathcal{G}, \mathcal{H} \in NNF$ then $(\mathcal{G} \vee \mathcal{H}) \in NNF$
4. If $\mathcal{G}, \mathcal{H} \in NNF$ then $(\mathcal{G} \wedge \mathcal{H}) \in NNF$.

Proof by induction on the number of propositional connectives n in $\mathcal{F}$:

$n=0$: If $\mathcal{F}$ is (A_n), let $\mathcal{G}$ be (A_n). Then by [Axiom $(a\Leftrightarrow a)$], $\vdash(\mathcal{F}\Leftrightarrow\mathcal{G})$; and $\mathcal{G}$ is in NNF.

$n>0$: Suppose that for every $\mathcal{F}_i$ with fewer than n propositional connectives, there is a $\mathcal{G}_i$ such that $\vdash(\mathcal{F}_i\Leftrightarrow\mathcal{G}_i)$ and $\mathcal{G}_i$ is in NNF.

Case 1. $\mathcal{F}$ is $(\mathcal{F}_1 \vee \mathcal{F}_2)$. $\mathcal{F}_1$ and $\mathcal{F}_2$ have fewer than n propositional connectives. By the induction hypothesis, $\exists\ \mathcal{G}_1$ and $\mathcal{G}_2$ s.t. $\vdash(\mathcal{F}_1\Leftrightarrow\mathcal{G}_1)$ and $\vdash(\mathcal{F}_2\Leftrightarrow\mathcal{G}_2)$, and $\mathcal{G}_1, \mathcal{G}_2 \in NNF$.

By $\left[\text{Rule } \dfrac{(a_1\Leftrightarrow B_1),\ (a_2\Leftrightarrow B_2)}{((a_1\vee a_2)\Leftrightarrow(B_1\vee B_2))}\right]$,

we get $\vdash((\mathcal{F}_1\vee\mathcal{F}_2)\Leftrightarrow(\mathcal{G}_1\vee\mathcal{G}_2))$.
Let $\mathcal{G}$ be $(\mathcal{G}_1\vee\mathcal{G}_2)$. Then $\mathcal{G}\in NNF$, and $\vdash(\mathcal{F}\Leftrightarrow\mathcal{G})$.

2.3.1.1 (cont.)-

Case 2. $\mathcal{F}$ is $(\mathcal{F}_1 \wedge \mathcal{F}_2)$. This is identical to case 1, with $\vee$ and $\wedge$ interchanged. We use the

$$\text{Rule } \frac{(A_1 \leftrightarrow B_1), (A_2 \leftrightarrow B_2)}{((A_1 \wedge A_2) \leftrightarrow (B_1 \wedge B_2))}$$

Case 3. $\mathcal{F}$ is $(\neg \mathcal{F}_0)$.

Subcase 3.1 $\mathcal{F}_0$ is atomic, i.e., (A_m). Let $\mathcal{G}$ be $(\neg (A_m))$. Then $\mathcal{G} \in$ NNF and by

axiom $(a \leftrightarrow a)$

we get $\vdash ((\neg \mathcal{F}_0) \leftrightarrow \mathcal{G})$

i.e. $\vdash (\mathcal{F} \leftrightarrow \mathcal{G})$.

Subcase 3.2. $\mathcal{F}_0$ is of the form $\neg \mathcal{F}_1$. Since $\mathcal{F}_1$ has $< n$ prop. conn., $\exists\, \mathcal{G}_1 \in$ NNF s.t. $\vdash (\mathcal{F}_1 \leftrightarrow \mathcal{G}_1)$.

By Axiom $((\neg(\neg a)) \leftrightarrow a)$,

$\vdash ((\neg(\neg \mathcal{F}_1)) \leftrightarrow \mathcal{F}_1)$.

By Rule $\frac{(a \leftrightarrow b), (b \leftrightarrow c)}{(a \leftrightarrow c)}$,

$\vdash ((\neg(\neg \mathcal{F}_1)) \leftrightarrow \mathcal{G}_1)$

i.e., $\vdash (\mathcal{F} \leftrightarrow \mathcal{G}_1)$, where $\mathcal{G}_1 \in$ NNF.

Subcase 3.3. $\mathcal{F}_0$ is of the form $(\mathcal{F}_1 \vee \mathcal{F}_2)$, i.e., $\mathcal{F}$ is $(\neg(\mathcal{F}_1 \vee \mathcal{F}_2))$. Note that important → $\mathcal{F}_1$ and $\mathcal{F}_2$ each have at most $n-2$ propositional connectives.

By Axiom $((\neg(a \vee b)) \leftrightarrow ((\neg a) \wedge (\neg b)))$,

$\vdash (\mathcal{F} \leftrightarrow ((\neg \mathcal{F}_1) \wedge (\neg \mathcal{F}_2)))$.

2.3.1.1 (cont.)

Now $(\neg \mathcal{F}_1)$ and $(\neg \mathcal{F}_2)$ each have at most $n-1$ prop. connectives, so by the induction hypothesis, there exist $\mathcal{G}_1, \mathcal{G}_2 \in NNF$ s.t. $\vdash ((\neg \mathcal{F}_1) \leftrightarrow \mathcal{G}_1)$ and $\vdash ((\neg \mathcal{F}_2) \leftrightarrow \mathcal{G}_2)$.

By $\boxed{\text{Rule } \dfrac{(\mathcal{A}_1 \leftrightarrow \mathcal{B}_1), (\mathcal{A}_2 \leftrightarrow \mathcal{B}_2)}{((\mathcal{A}_1 \wedge \mathcal{A}_2) \leftrightarrow (\mathcal{B}_1 \wedge \mathcal{B}_2))}}$,

$$\vdash (((\neg \mathcal{F}_1) \wedge (\neg \mathcal{F}_2)) \leftrightarrow (\mathcal{G}_1 \wedge \mathcal{G}_2)).$$

By $\boxed{\text{Rule } \dfrac{(\mathcal{A} \leftrightarrow \mathcal{B}), (\mathcal{B} \leftrightarrow \mathcal{C})}{(\mathcal{A} \leftrightarrow \mathcal{C})}}$,

$$\vdash (\mathcal{F} \leftrightarrow (\mathcal{G}_1 \wedge \mathcal{G}_2)).$$

Let $\mathcal{G}$ be $(\mathcal{G}_1 \wedge \mathcal{G}_2)$. Then $\mathcal{G}$ is in NNF, and $\vdash (\mathcal{F} \leftrightarrow \mathcal{G})$.

Subcase 3.4 $\mathcal{F}_0$ is of the form $(\mathcal{F}_1 \wedge \mathcal{F}_2)$. This is exactly like subcase 3.3 with "$\wedge$" and "$\vee$" interchanged. For completeness, we list the only new axiom involved:

$\boxed{\text{Axiom } ((\neg(\mathcal{A} \wedge \mathcal{B})) \leftrightarrow ((\neg \mathcal{A}) \vee (\neg \mathcal{B})))}$

see definition of $\vee \ldots \vee$ on p. 2 of H.W.

Sublemma 2.3.1.2 Consider a set of formulas $\{\mathcal{F}_1, \ldots, \mathcal{F}_m\}$. Let $\mathcal{F}$ be any formula which which combines $\mathcal{F}_1, \ldots, \mathcal{F}_m$ with disjunctions only, and in which each of $\mathcal{F}_1, \ldots, \mathcal{F}_m$ occurs exactly once. Then

$$\vdash (\mathcal{F} \leftrightarrow (\mathcal{F}_1 \vee \ldots \vee \mathcal{F}_m)).$$

Sub-sublemma: $\vdash ((\mathcal{Q} \vee (\mathcal{F}_1 \vee \ldots \vee \mathcal{F}_j)) \leftrightarrow (\mathcal{Q} \vee \mathcal{F}_1 \vee \ldots \mathcal{F}_j))$

Proof of sub-sub-lemma:

Let Rule (A) = $\text{Rule } \dfrac{(\alpha \leftrightarrow \beta)}{((\alpha \vee \gamma) \leftrightarrow (\beta \vee \gamma))}$

Let Rule (B) = $\text{Rule } \dfrac{((\alpha \vee \beta) \vee \gamma)}{((\alpha \vee \gamma) \vee \beta)}$

Let Rule (C) = $\text{Rule } \dfrac{(\alpha \leftrightarrow \beta), (\beta \leftrightarrow \gamma)}{(\alpha \leftrightarrow \gamma)}$

This is all more detail than I need to see. I appreciate your thoroughness, I do, but brevity has its advantages too.

Construct proof as follows*: * Could also be proved by induction, of course

$\vdash ((\mathcal{Q} \vee \mathcal{F}_1) \leftrightarrow (\mathcal{F}_1 \vee \mathcal{Q}))$	Axiom $(\alpha \vee \beta) \leftrightarrow (\beta \vee \alpha)$
$\vdash (((\mathcal{Q} \vee \mathcal{F}_1) \vee \mathcal{F}_2) \leftrightarrow ((\mathcal{F}_1 \vee \mathcal{Q}) \vee \mathcal{F}_2))$	Rule (A)
$\vdash ($ " $\leftrightarrow ((\mathcal{F}_1 \vee \mathcal{F}_2) \vee \mathcal{Q}))$	Rules (B), (C)
$\vdash (((\mathcal{Q} \vee \mathcal{F}_1) \vee \mathcal{F}_2) \vee \mathcal{F}_3) \leftrightarrow (((\mathcal{F}_1 \vee \mathcal{F}_2) \vee \mathcal{Q}) \vee \mathcal{F}_3))$	Rule (A)
$\vdash ($ " $\leftrightarrow (((\mathcal{F}_1 \vee \mathcal{F}_2) \vee \mathcal{F}_3) \vee \mathcal{Q})$	Rules (B), (C)
⋮	⋮
	Rule (A)
$\vdash (\mathcal{Q} \vee \mathcal{F}_1 \vee \ldots \vee \mathcal{F}_j) \leftrightarrow ((\mathcal{F}_1 \vee \ldots \vee \mathcal{F}_j) \vee \mathcal{Q})$	Rules (B), (C)

add on $\mathcal{F}_{j+1}$ until it is reached

Finally,

$$\vdash (\mathcal{Q} \vee \mathcal{F}_1 \vee \ldots \vee \mathcal{F}_j) \leftrightarrow (\mathcal{Q} \vee (\mathcal{F}_1 \vee \ldots \vee \mathcal{F}_j))$$

by $\text{Rule } \dfrac{\alpha \leftrightarrow (\beta \vee \gamma)}{\alpha \leftrightarrow (\gamma \vee \beta)}$

$$\vdash (\mathcal{Q} \vee (\mathcal{F}_1 \vee \ldots \vee \mathcal{F}_j)) \leftrightarrow (\mathcal{Q} \vee \mathcal{F}_1 \vee \ldots \vee \mathcal{F}_j)$$ by $\text{Rule } \dfrac{\alpha \leftrightarrow \beta}{\beta \leftrightarrow \alpha}$

2.3.1.2 (cont.)

Proof of main sublemma: Use induction on the number of formulas n in the set $\{\mathcal{F}_1, \ldots, \mathcal{F}_n\}$.

$n=1$: $\vdash(\mathcal{F} \Leftrightarrow \mathcal{F}_1)$ by Axiom $(a \Leftrightarrow a)$ since $\mathcal{F}$ can only be $\mathcal{F}_1$.

$n=2$: Either $\mathcal{F}$ is $(\mathcal{F}_1 \vee \mathcal{F}_2)$ or $\mathcal{F}$ is $(\mathcal{F}_2 \vee \mathcal{F}_1)$. Then either

$$\vdash((\mathcal{F}_1 \vee \mathcal{F}_2) \Leftrightarrow (\mathcal{F}_1 \vee \mathcal{F}_2)) \text{ by Axiom } (a \Leftrightarrow a)$$

or

$$\vdash((\mathcal{F}_1 \vee \mathcal{F}_2) \Leftrightarrow (\mathcal{F}_2 \vee \mathcal{F}_1)) \text{ by Axiom } ((a \vee \mathcal{B}) \Leftrightarrow (\mathcal{B} \vee a))$$

$n>2$: Assume sublemma true for $i<n$.

$\mathcal{F}$ must be of the form

$$(\mathcal{F}_a \vee \mathcal{F}_b)$$

by definition. By induction hypothesis,

$$\left.\begin{array}{l} \vdash(\mathcal{F}_a \Leftrightarrow (\mathcal{F}_{a_1} \vee \ldots \vee \mathcal{F}_{a_j})) \\ \text{and } \vdash(\mathcal{F}_b \Leftrightarrow (\mathcal{F}_{b_1} \vee \ldots \vee \mathcal{F}_{b_k})). \end{array}\right\} \mathcal{F}_{a_i}, \mathcal{F}_{b_i} \in \{\mathcal{F}_1, \ldots, \mathcal{F}_n\}$$

Therefore

$$\vdash((\mathcal{F}_a \vee \mathcal{F}_b) \Leftrightarrow ((\mathcal{F}_{a_1} \vee \ldots \vee \mathcal{F}_{a_j}) \vee (\mathcal{F}_{b_1} \vee \ldots \vee \mathcal{F}_{b_k})))$$

by Rule $\dfrac{(a_1 \Leftrightarrow \mathcal{B}_1), (a_2 \Leftrightarrow \mathcal{B}_2)}{((a_1 \vee \mathcal{B}_1) \Leftrightarrow (a_2 \vee \mathcal{B}_2))}$

By sub-sublemma then Rule © (previous page), and definition of $\vee \ldots \vee$,

$$\vdash (\mathcal{F}_a \vee \mathcal{F}_b) \Leftrightarrow ((\underbrace{\mathcal{F}_{a_1} \vee \ldots \vee \mathcal{F}_{a_j} \vee \mathcal{F}_{b_1} \vee \ldots \vee \mathcal{F}_{b_k}}_{\text{it is sub-sublemma}}))$$

Now $(\mathcal{F}_{a_1} \vee \ldots \vee \mathcal{F}_{b_k})$ must contain exactly one occurrence of each of $\mathcal{F}_1, \ldots, \mathcal{F}_n$ by definition of $\mathcal{F}$. We must simply put them in order. By Sublemma 2.4.2 ("Scramble") then Rule ©, we finally obtain

$$\vdash \underbrace{(\mathcal{F}_a \vee \mathcal{F}_b)}_{\mathcal{F}} \Leftrightarrow (\mathcal{F}_1 \wedge \ldots \wedge \mathcal{F}_n).$$

Lemma 2.4 If $\vDash H_{CNF}$ where H_{CNF} is in conjunctive normal form, then $\vdash H_{CNF}$.

Proof:

By the definition of CNF, H_{CNF} is in the form

$$(C_0 \wedge \ldots \wedge C_N)$$

By sublemma 2.4.1, each C_i must be a tautology (because H_{CNF} is), i.e., $\vDash C_i$.

Each C_i is a disjunction of atomic letters and negations of atomic letters, by definition. Since each C_i is a tautology, it must be the case that at least one atomic letter appear both with and without a negation in H_i (otherwise, the valuation V that assigns to each atomic letter without negation the value F and each atomic letter with negation the value T, will result in $V(C_i) = F$, contradicting $\vDash C_i$).

Now pick an atomic letter that occurs both with and without a negation in C_i; call it A_j. Let us move (A_j) and $(\neg(A_j))$ to the end of C_i, resulting in a new formula C_s: (s means "scrambled")

$$\underbrace{(((\text{rest of } C_i)}_{C_{i0}} \vee (A_j)) \vee (\neg(A_j))) \quad \} C_s$$

By sublemma 2.4.2, $\vdash (C_i \Leftrightarrow C_s)$. Now we can prove $\vdash C_i$ as follows:

$\vdash ((A_j) \vee (\neg(A_j)))$ by [Axiom $(a \vee (\neg a))$]

$\vdash (C_{i0} \vee ((A_j) \vee (\neg(A_j))))$ by [Rule $\frac{a}{B \vee a}$]

this is C_s $\rightarrow$ $\vdash (((C_{i0} \vee (A_j)) \vee (\neg(A_j)))$ by [Rule $\frac{(a \vee (B \vee c))}{((a \vee B) \vee c))}$]

$\vdash C_i$ by [Rule $\frac{a \Leftrightarrow B, B}{a}$] and sublemma 2.4.2

Lemma 2.4 (cont.):

At this point, we have shown

$$\vdash C_0, \vdash C_1, \ldots, \vdash C_n.$$

where C_i are the conjuncts of H_{CNF}.
By sublemma 2.4.3, from these
we can deduce by $\wedge$-INTRO

$$\vdash (C_0 \wedge C_1 \wedge \ldots C_n)$$

i.e. $\vdash H_{CNF}$.

Sublemma 2.4.1 · If $\vdash (C_0 \wedge \ldots \wedge C_n)$, then $\vdash C_i$, $0 \leq i \leq n$.

Proof: Same as proof of sublemma in Lemma 2.2.

Sublemma 2.4.2 Let $\mathcal{F}$ be the disjunction $(K_1 \vee \ldots \vee K_n)$. Let $\mathcal{G}$ be the same as $\mathcal{F}$ but with the disjuncts K_i scrambled in any order. Then $\vdash (\mathcal{F} \Leftrightarrow \mathcal{G})$.

Proof:

Sub-sub-lemma: Let $\mathcal{F}$ be the disjunction
$((\ldots((K_1 \vee K_2) \vee K_3) \vee \ldots) \vee K_n)$
Let $\mathcal{G}^{(1)}$ be the same as $\mathcal{F}$ with K_i and K_{i+1} swapped $(1 \leq i \leq n-1)$. Then
$\vdash (\mathcal{F} \Leftrightarrow \mathcal{G}^{(1)})$

Proof of sub-sub-lemma:

$\vdash ((K_i \vee K_{i+1}) \Leftrightarrow (K_{i+1} \vee K_i))$ by Axiom $((A \vee B) \Leftrightarrow (B \vee A))$

If $i > 1$, add the following steps:

$\vdash ((\underbrace{\ldots}_{K_1 \vee \ldots \vee K_{i-1}}) \vee (K_i \vee K_{i+1})) \Leftrightarrow ((\ldots) \vee (K_{i+1} \vee K_i))$

by Rule $\dfrac{A \Leftrightarrow B}{(C \vee A) \Leftrightarrow (C \vee B)}$

$\vdash (((\ldots) \vee K_i) \vee K_{i+1}) \Leftrightarrow (((\ldots) \vee K_{i+1}) \vee K_i)$

by Rule $\dfrac{((A \vee (B \vee C)) \Leftrightarrow (D \vee (E \vee F)))}{(((A \vee B) \vee C) \Leftrightarrow ((D \vee E) \vee F))}$

If $i+1 < n$, add successive layers of disjuncts $K_{i+2}, \ldots, K_n$ with repeated applications of

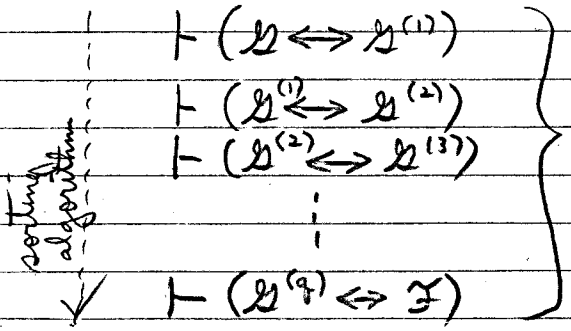
Rule $\dfrac{(A \Leftrightarrow B)}{((A \vee C) \Leftrightarrow (B \vee C))}$

Finally we will arrive at
$\vdash (\mathcal{F} \Leftrightarrow \mathcal{G}^{(1)})$.

Sublemma 2.4.12 - (cont.)

Proof of main sublemma:

$\mathcal{F}$ has the indices of its disjuncts K_i ordered (1 through n), whereas $\mathcal{G}$ has them scrambled. This suggests using an analog of a standard exchange-sort computer algorithm to figure out which (adjacent) indices of $\mathcal{G}$ to swap to make $\mathcal{G}$ transform into $\mathcal{F}$. Diagramatically, successively prove:



Now successively apply

$$\text{Rule } \frac{(a \Leftrightarrow b), (b \Leftrightarrow c)}{a \Leftrightarrow c}$$

to get $\vdash (\mathcal{G} \Leftrightarrow \mathcal{F})$.

Finally, use

$$\text{Rule } \frac{a \Leftrightarrow b}{b \Leftrightarrow a}$$

to get $\vdash (\mathcal{F} \Leftrightarrow \mathcal{G})$.

Sublemma 2.4.3 - If $\vdash C_0, \ldots, \vdash C_m$, then $\vdash (C_0 \wedge \ldots \wedge C_m)$

Proof:

Apply the Rule $\dfrac{\alpha, \beta}{(\alpha \wedge \beta)}$ successively to $\vdash C_0, \ldots, \vdash C_m$ to give

$\vdash (C_0 \wedge C_1)$

$\vdash ((C_0 \wedge C_1) \wedge C_2)$

$\vdash (((C_0 \wedge C_1) \wedge C_2) \wedge C_3)$

$\vdots$

$\vdash (C_0 \wedge C_1 \wedge \ldots \wedge C_m)$ ← see def. of $\wedge \ldots \wedge$ on p. 2 of HW

Lemma 2.5 If $\vdash H_{CNF}$ and $\vdash (((\mathcal{G}_0 \wedge \ldots \wedge \mathcal{G}_m) \to \mathcal{F}) \leftrightarrow H_{CNF})$ then $\vdash ((\mathcal{G}_0 \wedge \ldots \wedge \mathcal{G}_m) \to \mathcal{F})$.

Proof: Apply the Rule $\dfrac{\alpha, \alpha \leftrightarrow \beta}{\beta}$ to hypotheses to get $\vdash ((\mathcal{G}_0 \wedge \ldots \wedge \mathcal{G}_m) \to \mathcal{F})$

Lemma 2.6 If $\vdash ((\mathcal{G}_0 \wedge \ldots \wedge \mathcal{G}_m) \to \mathcal{F})$ then $\{\mathcal{G}_0, \ldots, \mathcal{G}_m\} \vdash \mathcal{F}$

First, a sublemma: $\{\mathcal{G}_0, \ldots, \mathcal{G}_m\} \vdash (\mathcal{G}_0 \wedge \ldots \wedge \mathcal{G}_m)$

Proof of sublemma by induction on m:

$m = 0$: $\{\mathcal{G}_0\} \vdash \mathcal{G}_0$ (one of the deduction rules)

$m > 0$: Assume $\{\mathcal{G}_0, \ldots, \mathcal{G}_{m-1}\} \vdash (\mathcal{G}_0 \wedge \ldots \wedge \mathcal{G}_{m-1})$
We can add a new hypothesis without changing the deduction (see Lemma 2.7), so $\{\mathcal{G}_0, \ldots, \mathcal{G}_m\} \vdash (\mathcal{G}_0 \wedge \ldots \wedge \mathcal{G}_{m-1})$.
By Rule $\dfrac{\alpha, \beta}{(\alpha \wedge \beta)}$, $\{\mathcal{G}_0, \ldots, \mathcal{G}_m\} \vdash (\mathcal{G}_0 \wedge \ldots \wedge \mathcal{G}_m)$

↑ see def. of $\wedge \ldots \wedge$ on p. 2 of HW

I reader. Such abbreviations are standard

Proof of main lemma:

Assume $\vdash ((\mathcal{G}_0 \wedge \ldots \wedge \mathcal{G}_m) \to \mathcal{F})$. We can add hypotheses without changing the deduction (see Lemma 2.7), so $\{\mathcal{G}_0, \ldots, \mathcal{G}_m\} \vdash ((\mathcal{G}_0 \wedge \ldots \wedge \mathcal{G}_m) \to \mathcal{F})$.
By the sublemma and

Rule $\dfrac{\alpha, \alpha \to \beta}{\beta}$,

$\{\mathcal{G}_0, \ldots, \mathcal{G}_m\} \vdash \mathcal{F}$.

Lemma 2.7. If $T_0 \vdash \mathcal{F}$ and $T_0 \subseteq T$, then $T \vdash \mathcal{F}$.

Proof: Consider the formulas $\mathcal{F}_0, \mathcal{F}_1, \ldots$ in the deduction of $\mathcal{F}$. If $\mathcal{F}_i \in T_0$, then $\mathcal{F}_i \in T$ since $T_0 \subseteq T$. For any other $\mathcal{F}_i$, T_0 and T are irrelevent. ∴ Therefore $T \vdash \mathcal{F}$.

Exhaustive,

24/24

n. megill

Addendum to HW #4:

Outside of Sublemma 2.3.1, assume H_{CNF} has been converted to the form

$$(C_0 \wedge \ldots \wedge C_m)$$

using Sublemma 2.3.1.2.

Norman D. Megill
18.511 HW
Assigned: 10/17/89
Due: 10/24/89

HW #5 Let F_n be the unique linear ordering with n elements. Let $F_\omega = \frac{\prod_{n\in\omega} F_n}{D}$ (ultraproduct) where D is non-trivial. (1) Show F_ω is ω. (2) Show $\mathbb{Q}$ (linear ordering of the rationals) can be embedded in F_ω. (3) Show $\mathbb{Z}$ (linear ordering of pos. & neg. integers) can be embedded in F_ω.

~~You should get to $\mathbb{Q}$ — F_ω is a [illegible]~~

Note: I am assuming that we should show $\exists$ a non-trivial D for which this is true. (I did not show that it is true for an arbitrary non-trivial D.)

I assume a trivial ultrafilter is one generated by a singleton, i.e., $(\{i\})$ where $i\in\omega$. (Not clear from my class notes.) In this case, F_ω will "reduce" to a single "factor" F_i, as shown in class.

(1) Show F_ω is ω.

By definition, $\prod_{n\in\omega} F_n = \{h \mid h : \omega \to \bigcup_{n\in\omega} A_n \text{ s.t. } h(n)\in F_n\}$

(Hypothesis) Let $F_n = \{a_i^n \mid 1\le i\le n\}$

Define: $a_i^n <_n a_j^n$ iff $i<j$ ("English" $<$ = Natural ordering of pos. integers.)

$F_1 = \{a_1^1\}$
$F_2 = \{a_1^2\ a_2^2\}$
$F_3 = \{a_1^3\ a_2^3\ a_3^3\}$
$\vdots$

a — size of set
i — element # in set

the upshot of F_n being unique is that $a_1^k = a_1^{k+1}$ for $k\ge 1$;

else $<^{F_n}\restriction\{F_{n-1}\} \neq <^{F_{n-1}}$, but there are linear orders of $n-1$ elements

$F_n = \{a_1, \ldots, a_n\}$.

$f \in \left(\prod_{n \in \omega} F_n\right) \iff \mathrm{Dom}(f) = \omega \wedge f(n) \in F_n$

Let $m > n$. There is no restriction on $f(m)$, but this must exist. Let $a_n \in F_n$ (for convenience)

Because the F_n's are finite sets, the set of functions in $\prod_{n \in \omega} F_n$ are countable. Arrange these functions in the following order: Let $n = 1, m = 2$. The number of f's $\in \prod_{n \in \omega} F_n$ s.t. $\mathrm{Dom}(f) = \omega$ ~~$\mathrm{Ran}(f) \subseteq \omega$~~ $f(1) = 1$ is clearly uncountable $\Rightarrow$

Call the h's in $\prod_{n \in \omega} F_n$ by the names h_{ij}, $i = 1, 2, 3, \ldots$, and $1 \le j \le (i-1)!$

h_{ij}	$h_{ij}(1)$	$h_{ij}(2)$	$h_{ij}(3)$	$h_{ij}(4)$	...
h_{11}	a_1^1	a_1^2	a_1^3	a_1^4	
h_{21}	a_2^1	a_2^2	a_2^3	a_2^4	
2 possibilities → h_{31}, h_{32}	a_3^1	a_1^2 or a_2^2	a_3^3	a_3^4	
$2 \cdot 3 = 6$ poss. → $h_{41}, \ldots, h_{46}$	a_4^1	a_1^2 or a_2^2	a_1^3, a_2^3, or a_3^3	a_4^4	

$$h_{ij}(k) = \begin{cases} a_i^k & \text{if } k \ge i \\ \text{one of } a_1^k, \ldots, a_k^k & \text{if } k < i \end{cases}$$ ← size of F_k; covers all combinations $1, \ldots, (i-1)!$

By convention, choose $h_{i1}(k) = a_1^k$ if $k < i$.

We want to find a D such that the equivalence class of h_{i1} is the h_{ij}'s:

$$[h_{i1}] = \{h_{ij} \mid 1 \le j \le (i-1)!\}$$

Define D Let F be the set of all co-finite subsets of ω. It was shown in class that F is a filter ("dual ideal"). Using the Maximal (Dual) Ideal Theorem, extend F to a maximal filter D. (By Chang + Kiesler Model Theory 4.1.2, p. 166) D is therefore an ultrafilter.

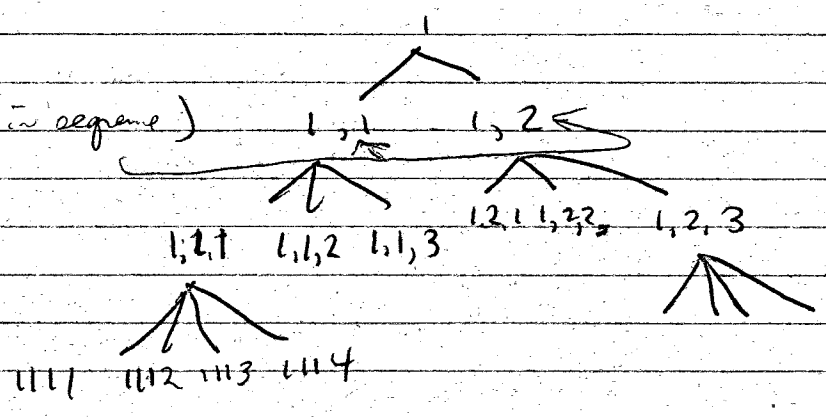
(This D is non-trivial.)
i.e. $-F$ is already maximal

Note ~~$\omega \in F$~~ ~~$\emptyset \notin F$~~
Suppose $I \notin F$
Then I is cofinite, so $\omega - I$ is finite, so $\omega - I \notin F$
Likewise if $\omega - I \in F$, then $\omega - I$ is finite, so I is infinite & hence $I \notin F$

I see you already discussed this

That was pretty messy.

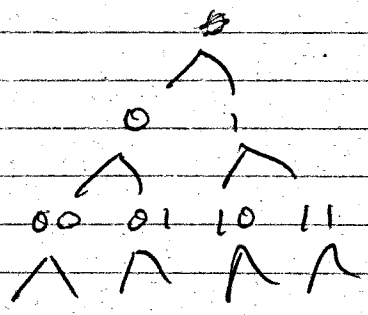
The functions f w/ domain $= \omega$ and range $\subseteq \bigcup_n F_n \subseteq \omega$ (ie let $a_n = n$) correspond to paths in this tree



Note that $f(n) \leq n$ for any f some path this tree, and that

$f(n) \leq n$ correspond to $f(n) \in F_n$

The ~~possible~~ paths are ~~infinite since~~ ~~countable~~ uncountable since even in the binary tree (a subset of A) the paths are uncountable



Each path corresponds to a subset of natural numbers (in the obvious way) and so is uncountable (unlike the nodes).

But! You by no means need to enumerate all the elements of F_2 for your purpose.

Assuming this D, what is $[h_{i1}]$?

By definition,

$$[h_{i1}] = \{g \mid \underbrace{g \in \prod_{n\in\omega} F_n}_{g(n)\in F_n} \;\&\; \underbrace{g \sim h_{i1}}_{\{k \mid g(k) = h_{i1}(k)\} \in D}\}$$

$g(n) \in F_n$: covers all h_{ij}

$\{k \mid g(k) = h_{i1}(k)\} \in D$: we must look at this

Case 1. Show: If $g = h_{ij}$, then $g \in [h_{i1}]$

Proof:

If $j=1$, $h_{i1}(k) = h_{i1}(k)$ for all k, and $\{1,2,3,\ldots\} = \omega \in D$.

If $j \neq 1$, $h_{i1}(k) = h_{ij}(k)$ for none or some $k < i$ and for all $k \geq i$. The set of k where $h_{i1}(k) \neq h_{ij}(k)$ is finite. Therefore the set of k where $h_{i1}(k) = h_{ij}(k)$ is co-finite, i.e., $\in D$.

Case 2. Show: If $g = h_{lj}$, $l \neq i$, then $g \notin [h_{i1}]$.

Proof:

If $k > \max(i,l)$, then $f_{lj}(k) = a^k_l \neq a^k_i = f_{ij}(k)$.

Therefore the set of k (call it M) where $h_{lj} = h_{ij}$ is finite. $\omega - M$ is cofinite, $\therefore \omega - M \in D$. Since D is an ultrafilter, the complement of $\omega - M$, i.e. M, is $\notin D$. (By definition of ultrafilter)!

Therefore $[h_{i1}] = \{h_{ij} \mid 1 \leq j \leq (i-1)!\}$, which is what we want.

Now look at the definition of the ultraproduct:

$$F_\omega = \frac{\prod_{n\in\omega} F_n}{D} = \left\{ [h] \mid h \in \prod_{n\in\omega} F_n \right\}$$

We have shown that when D = maximal extension of cofinite subsets of ω, then for every $i \in \omega$, $[h_{i1}]$ is defined, finite, and different from $[h_{j1}]$ if $i \neq j$.

Therefore the # of $[h_{i1}]$'s, i.e. the # of elements of F_ω, is infinite.

(2) Show Q can be embedded in F_∞.

First we must establish a 1-1 correspondence of rationals with the integers: Use a diagonal zig-zig method and cross out the ones that are equal to a previous member of the list:

p/q	p → 0	1	-1	2	-2	3	-3	4	-4
q ↓ 1	0/1	1/1	-1/1	2/1	-2/1	3/1	-3/1		
2	~~0/2~~	1/2	-1/2	~~2/2~~	-2/2				
3	~~0/3~~	1/3	-1/3	2/3	-2/3				
4	~~0/4~~	1/4	-1/4	2/4	-2/4				
5	~~0/5~~	1/5	-1/5	2/5	-2/5				
6	0/6	1/6	-1/6	2/6					
7	0/7								

START

← cross out duplicates

This leads to the sequence: $0/1, 1/1, 1/2, -1/1, 2/1, -1/2, 1/3, 1/4, -1/3, \ldots$

Define a sequence number $n_{p/q}$ = $1, 2, 3, 4, 5, 6, 7, 8, 9, \ldots$

Thus every rational $\frac{p}{q}$ has an associated integer $n_{p/q}$.

Now consider a mapping from a finite ordering of those rationals whose sequence numbers are 1 thru n, to the linear ordering F_n:

$$\{0/1\} \rightarrow \{a_1^1\} = F_1$$
$$\{0/1 \;\; 1/1\} \rightarrow \{a_1^2 \;\; a_2^2\} = F_2$$
$$\{0/1 \;\; 1/2 \;\; 1/1\} \rightarrow \{a_1^3 \;\; a_2^3 \;\; a_3^3\} = F_3$$
$$\{-1/1 \;\; 0/1 \;\; 1/2 \;\; 1/1\} \rightarrow \{a_1^4 \;\; a_2^4 \;\; a_3^4 \;\; a_4^4\} = F_4$$

one-to-one mapping in order listed

note that we have ordered the rationals within this set

More formally, define q_i : a function $q_i : Q \rightarrow \{a_j^i \in F_i\}$

$$q_i\left(\frac{p}{q}\right) = \begin{cases} a^i_{j_{p/q}} & \text{if } i \geq n_{p/q}, \text{ where } j_{p/q} < j_{p'/q'} \text{ iff } \frac{p}{q} < \frac{p'}{q'} \\ \text{undefined} & \text{if } i < n_{p/q} \end{cases}$$

usual arithmetic definition of <

this orders the list

takes care of p/q not in the list.

Before proceeding, we must prove a lemma:

$[h_{i1}] <_{F_\infty} [h_{j1}]$ iff $i < j$

Proof:

Definition of $<_{F_\infty}$ is:

$[h_{i1}] <_{F_\infty} [h_{j1}] \iff \{n \mid h_{i1}(n) <_n h_{j1}(n)\} \in D$

We want to find this set of n (Call it $\{n \mid <_n\}$)

Case 1: $i < j$

$n < j$: $h_{j1}(n) = a_1^n$ by def.
Since a_1^n is least number of F_n, $\not<_n a_1^n$ for all $x \in F_n$
$\therefore n < j$ is not in set

$n \geq j$: $h_{j1}(n) = a_j^n$, $h_{i1}(n) = a_i^n$ (by def.)
Since $i < j$, $a_i^n <_n a_j^n$ (def. of $<_n$)
so $h_{i1}(n) <_n h_{j1}(n)$
$\therefore n \geq j$ is in set

$\therefore \{n \mid <_n\} = \underbrace{\{j, j+1, j+2, \ldots\}}_{\text{cofinite}} \in D \quad \Leftarrow T$

Case 2: $i \geq j$

$n < j$: Same as Case 1, i.e., $n < j$ is not in set

$n \geq j$: Same analysis as Case 1, but since $i \geq j$ we conclude $h_{i1}(n) \not<_n h_{j1}(n)$ $\therefore n \geq j$ is not in set

$\therefore \{n \mid <_n\} = \emptyset \notin D \quad \Leftarrow F$

Conclusion:

$[h_{i1}] <_{F_\infty} [h_{j1}]$ is T if $i < j$
F if $i \geq j$

(End of Lemma)

↳ refers to symbol used to denote $[h_{i1}]$.
↳ refers to relation used to interpret symbol "$<$"

Observe that $q_m\left(\frac{p}{q}\right)$ defines sets of rationals that can be interpreted as elements a^m_i of linear orderings F_m.

If a rational $\frac{p}{q}$ corresponds to element a^m_i and $\frac{p'}{q'}$ to a^m_j,

then $\frac{p}{q} <_Q \frac{p'}{q'} \Leftrightarrow i < j \Leftrightarrow a^m_i <_m a^m_j$.

($\Leftrightarrow$ by def q_m; $\Leftrightarrow$ by def $<_m$)

In the Lemma, we used the fact that $a^n_i <_n a^n_j$ iff $i<j$ to show $[h_{i1}] <_{F_\omega} [h_{j1}]$ iff $i<j$. (In other words, we could repeat the Lemma using the special case of rationals in place of the more general a^n_i's.) Therefore

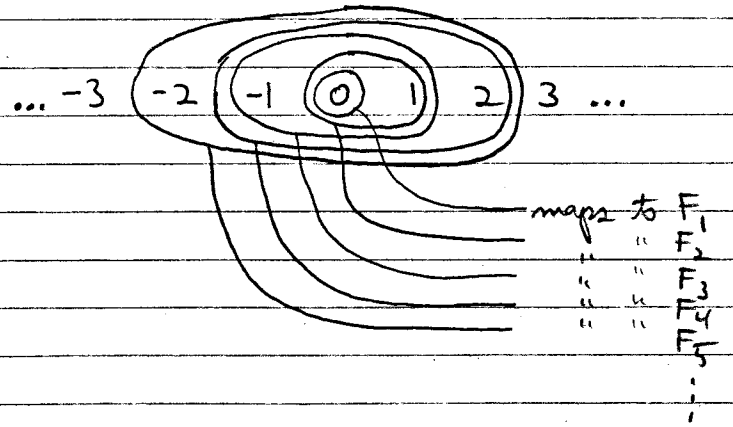
$$\frac{p}{q} <_Q \frac{p'}{q'} \Rightarrow [h_{i1}] <_{F_\omega} [h_{j1}]$$

when the a^m_i's in h_{i1} are substituted with rationals according to function $q_m\left(\frac{p}{q}\right)$.

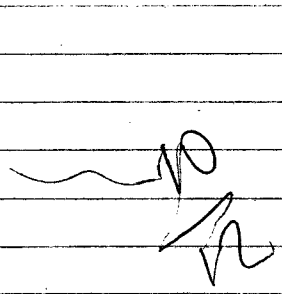
(3) **Show $\mathbb{Z}$ can be embedded in F_∞.**

This is obviously a special case of (2). not in spirit of question.

Alternately, one could obtain a simpler more direct development by mapping subsets of $\mathbb{Z}$ to F_n as follows:



(This development would be simpler because the integers mapped to F_n are already in order.)



N. Megill 10/26/89

Addendum to HW#5

In the homework, I stated that I did not show the results for an arbitrary non-trivial D. However the only fact I assumed about D was that it contained all cofinite subsets of ω. By virtue of the following theorem, the results do apply to an arbitrary non-trivial D.

(I'm assuming "trivial" means "generated by a singleton".)

Theorem: An ultrafilter D on 2^I (I infinite) is non-trivial iff D contains all cofinite subsets of I.

Proof: $\Leftarrow$ Suppose D is trivial. Then it contains the singleton $\{a\}$ which generates it. The cofinite set $I-\{a\}$ is therefore $\notin D$ because D is an ~~ultra~~filter. $\{a\} \cap I-\{a\} = \emptyset$ so D does not contain all cofinite subsets of I. ($\emptyset \notin D$)

$\Rightarrow$ Suppose D does not contain all cofinite subsets of I. Then it contains a finite subset of I.

As an example, suppose D contains the 2-element set $\{a\ b\}$. Now assume D is non-trivial; show this leads to a contradiction: If D is non-trivial, it cannot contain either $\{a\}$ or $\{b\}$. Then it must contain both $I-\{a\}$ and $I-\{b\}$. Because of finite intersection property, we must have

$$(I-\{a\}) \cap (I-\{b\}) \cap \{a\ b\} \neq \emptyset,$$

which is not true. Therefore D must contain either $\{a\}$ or $\{b\}$ and is therefore trivial.

(Argument is easily generalized from 2 elements to n elements.)

Norman D. Megill
18.511 Homework
Assigned: 10/19/89
Due: 10/26/89

HW #6 Consider $\frac{\omega^N}{D}$ where D is non-trivial.

Virtually perfect. 12/12

(a) Show $\frac{\omega^N}{D}$ is a linear ordering. (Work on naming convention.)

Definitions: $\omega = \langle N, \leq, 0 \rangle$ ($\leq$: linear ordering) $N = \{0, 1, 2, 3, \ldots\}$
D = ultrafilter on 2^N

We are given that ω is a linear ordering (by definition); this means

$$\omega \models \mathcal{F}$$

when $\mathcal{F}$ is one of the axioms of linear ordering:

$\omega \models \forall x \neg (x < x)$

$\omega \models \forall x \forall y (x <_y \vee x =_y \vee y <_x)$

$\omega \models \forall x \forall y \forall z ((x \leq_y \wedge y <_z) \Rightarrow x <_z)$

The Fundamental Theorem of Ultraproducts states:

$$\frac{\prod_{i \in I} a_i}{D} \models \mathcal{F} \iff \{i \mid a_i \models \mathcal{F}\} \in D$$

Let a_i be ω and I be N:

$$\frac{\omega^N}{D} \models \mathcal{F} \iff \underbrace{\{i \mid \omega \models \mathcal{F}\}}_{=N} \in D$$

true because D is a filter

Therefore $\frac{\omega^N}{D} \models \mathcal{F}$,

i.e., $\frac{\omega^N}{D}$ is a linear ordering.

excellent ~~all but 4/4~~

(b) Show $\frac{\omega^N}{D}$ has an infinite element.

Note: $\frac{\omega^N}{D}$ is a structure; $\{\frac{N^N}{D}, <_\omega, 0_\omega\}$ → maps to equiv. class $[[0,0,0,\ldots]]$

we really want to show that the set $\frac{N^N}{D}$ (an ultrapower) has an infinite element.

$\frac{N^N}{D}$ is a set of equivalence classes:

$$\frac{N^N}{D} = \{[f] \mid f \in N^N\}$$

Define $f_0, f_1, \ldots$ $\quad f_n(i) = n$

$f_0 = [0, 0, 0, \ldots]$
$f_1 = [1, 1, 1, \ldots]$
$\vdots$
$f_n = [n, n, n, \ldots]$
$\vdots$

Now f_i and f_j are equal nowhere if $i \neq j$, so they must be members of different equivalence classes. We can establish a 1-1 mapping from integer n to $[f_n]$.

Define f_∞: $\quad f_\infty(i) = i$

$f_\infty = [0, 1, 2, 3, \ldots]$

"$[f_n]$" is a name too, but one uses "$[f_n]$" as a name in the language

Claim: $[f_n] <_\infty [f_\infty]$ for arbitrary n

Proof: $\{i \mid f_n(i) < f_\infty(i)\} = \{n+1, n+2, \ldots\}$

$= $ (a cofinite set)

$\in D$ since D is non-trivial (see "addendum to HW #5")

$\therefore [f_\infty]$ is infinite.

In fact this shows you are not speaking in the language, but of it; so the convention is not called for here.

$[f_n]$ is a name for the same set $[f_n]$ etc.

(c) Show there is no least infinite element. sorry - ok

~~Your argument needs to be generalized;~~ you ~~have only~~

Let $[f_\infty]$ be any infinite element. We want to find s.t. ~~$[f_\infty]$ is not the least infinite element,~~ another infinite element $[f_{\infty-1}]$ such that

$$[f_{\infty-1}] <_\omega [f_\infty].$$

Define: $$f_{\infty-1}(i) = \begin{cases} f_\infty(i)-1 & \text{if } 0 < f_\infty(i) \\ 0 & \text{if } 0 = f_\infty(i) \end{cases}$$

① $[f_{\infty-1}] <_\omega [f_\infty]$.

Proof: $f_{\infty-1}(i) \nless f_\infty(i)$ only when $f_\infty(i) = 0$.

Let $s_{\nless} = \{i \mid f_{\infty-1}(i) \nless f_\infty(i)\} = \{0\}$ ← This is the set of i's where f_∞ is 0.

Let $s_< = \{i \mid f_{\infty-1}(i) < f_\infty(i)\}$ ← this is cofinite.

Since $[f_\infty]$ is infinite, $[f_0] <_\omega [f_\infty]$, i.e., $f_\infty \neq f_0$.

Since $f_0(i) = 0$ everywhere, $\{i \mid f_\infty(i) = 0\} \notin D$, i.e., $s_{\nless} \notin D$.

$s_< = N - s_{\nless}$, so $s_< \in D$ ← (by def. of ultrafilter). Therefore $[f_{\infty-1}] <_\omega [f_\infty]$. ✓

② $[f_{\infty-1}]$ is infinite.

Proof: Let $s_{<_\infty} = \{i \mid f_{n+1}(i) < f_\infty(i)\}$. For any finite $n \geq 0$, $s_{<_\infty} \in D$ because $[f_{n+1}] <_\omega [f_\infty]$.

Let $s_{<_{\infty-1}} = \{i \mid f_n(i) < f_{\infty-1}(i)\}$. From def. of $f_{\infty-1}$, $s_{<_\infty} = s_{<_{\infty-1}}$. Therefore $s_{<_{\infty-1}} \in D$, so $[f_n] <_\omega [f_{\infty-1}]$ for any (i.e., all) n.

(d) Show there is no greatest infinite element.

Let $[f_\omega]$ be any infinite element.

Define $f_{\omega+1}(i) = f_\omega(i) + 1$

① $[f_\omega] <_w [f_{\omega+1}]$.

Proof: $\{i \mid f_\omega(i) < f_{\omega+1}(i)\} = N$

$\in D$

② $[f_{\omega+1}]$ is infinite

Proof: $[f_\omega]$ is greater than any finite element. Since $\frac{\omega^N}{D}$ is a linear ordering, from the axiom $(x \leq y \wedge y < z) \to x < z$ we conclude that $[f_{\omega+1}]$ is greater than any finite element. ✓

(e) Show that if x is an infinite element, then $\exists$ an infinite element y s.t. $x < y$ and there is nothing in between.

Let $x = [f_\omega]$ be any infinite element.

Define $f_{\omega+1}(i) = f_\omega(i) + 1$. In part (d), we showed $[f_\omega] <_\omega [f_{\omega+1}]$ and that $[f_{\omega+1}] - x$ is infinite.

Now, assume $\exists$ an element $[f_{\omega+1/2}]$ between x and y. We will show this leads to a contradiction.

Let $S_\omega = \{i \mid f_\omega(i) < f_{\omega+1/2}(i)\}$.

Let $S_{\omega+1} = \{i \mid f_{\omega+1/2}(i) < f_{\omega+1}(i)\}$.

① If $[f_\omega] <_\omega [f_{\omega+1/2}]$, then $S_\omega \in D$.

② If $[f_{\omega+1/2}] <_\omega [f_{\omega+1}]$, then $S_{\omega+1} \in D$.

An integer n cannot exist such that $f_\omega(i) < n < f_\omega(i)+1$, so the sets S_ω and $S_{\omega+1}$ are disjoint, i.e., $S_\omega \cap S_{\omega+1} = \phi \notin D$.

Therefore ① and ② can't both be true.

(f) Show $\exists$ infinite elements a and b such that there are infinitely many elements between them.

Let $f_\omega(i) = i$, and $a = [f_\omega]$.

Let $f_{\omega^2}(i) = i^2$, and $b = [f_{\omega^2}]$.

Let $f_{\omega+n}(i) = i+n$.

① $[f_\omega]$ and $[f_{\omega^2}]$ are infinite.

Proof: That $[f_\omega]$ is infinite was shown earlier.

$[f_{\omega^2}]$ is infinite because it is greater than $[f_\omega]$,

i.e., $\{i \mid f_\omega(i) < f_{\omega^2}(i)\} = \{2,3,4,\dots\}$ is cofinite, $\therefore \in D$.

② For all finite $n>1$, $[f_\omega] <_\omega [f_{\omega+n}]$.

Proof: $\{i \mid f_\omega(i) < f_{\omega+n}(i)\} = N$, and $N \in D$.

③ For all finite $n>1$, $[f_{\omega+n}] <_\omega [f_{\omega^2}]$.

Proof: For any fixed n, there is an integer i_T (threshold) such that $i^2 > i+n$ for all $i \geq i_T$. Therefore

$\{i \mid f_{\omega+n}(i) < f_{\omega^2}(i)\} = \{i_T, i_T+1, i_T+2, \dots\}$ is cofinite, $\therefore \in D$.

Norman D. Megill
18.511 Homework
Assigned: 10/24/89
Due: 10/31/89

HW #7 a) Derive compactness from Fundamental Theorem.

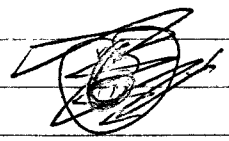
We must prove the compactness theorem:
Let S be a set of sentences s.t. each finite $S_0 \subseteq S$ has a model. Then S has a model.

Proof: ~~6~~ 6 for prt a

Assume each $S_0 \subseteq S$ has a model. Then there is a structure a_0 that makes each $\mathcal{F} \in S_0$ true. If a_0 makes $\mathcal{F}$ true, it will make $\neg\mathcal{F}$ false. Therefore $\neg\mathcal{F} \notin S_0$. Therefore each $S_0 \subseteq S$ is consistent.

Next, suppose S is not consistent. Then there exists a formula $\mathcal{F}$ such that $\mathcal{F}$ and $\neg\mathcal{F}$ are both deducible from S. Pick a finite subset S_0 of S containing $\mathcal{F}$ and $\neg\mathcal{F}$. Then S_0 is inconsistent (contradiction). Therefore S is consistent.
which yields.

Since S is consistent, by the Fundamental Theorem S has a model.



Norman D. Megill

This is a revision of part (b) of HW #7.

HW #7 b) Derive completeness (Gödel) from the Fundamental Theorem.

Completeness theorem: If a sentence $\mathcal{F}$ is true in every $\mathcal{L}$-structure, then $\mathcal{F}$ is provable.

Proof: We wanted ~~this~~ "strong" completeness $\Gamma \vdash \mathcal{F} \Leftrightarrow \Gamma \models \mathcal{F}$.

Assume $\mathcal{F}$ is true in every $\mathcal{L}$-structure.

Let S be the set of provable sentences. Since the axioms of logic are consistent, and the rules "preserve truth", S is consistent.

Consider any consistent set of sentences S that does not contain $\mathcal{F}$, but contains the logical axioms used in the proof of the Fundamental Theorem (i.e., excludes the Henkin axioms).

Let S' be the set of sentences provable from S, using the rules used in the proof of the Fundamental Theorem. Since the rules "preserve truth", it is impossible to derive both $\mathcal{G}$ and $\neg\mathcal{G}$ from S (S is consistent), so S' must also be consistent.

Suppose S doesn't contain $\mathcal{F}$, i.e., that $\mathcal{F}$ is not provable. Then we can add $\neg\mathcal{F}$ to S to obtain a consistent set of sentences $S' = S \cup \{\neg\mathcal{F}\}$. By the Fundamental Theorem, S' has a model $\mathcal{A}'$, i.e., $\mathcal{A}'$ is an $\mathcal{L}$-structure that makes all of S' true, in particular $\neg\mathcal{F}$. Thus $\mathcal{A}'$ makes $\mathcal{F}$ false. However, we assumed $\mathcal{F}$ is true in every $\mathcal{L}$-structure (contradiction). Therefore S must contain $\mathcal{F}$, i.e., $\mathcal{F}$ must be provable.

I will give you 2/6 for this part, and you can submit a proof of the generalized result to increase your mark.

Total (temp.) 8/12

Norman D. Megill
18.511 Homework
11/21/89

Revision of part (b) of HW #7

HW #7 b) Derive completeness from the Fundamental Theorem

Completeness (strong form): Let T be a set of sentences, and $\mathcal{F}$ a sentence. Then

$$T \vdash \mathcal{F} \iff T \models \mathcal{F}.$$

Proof:

($\Rightarrow$) Assume $T \vdash \mathcal{F}$.
Then there is a finite subset of sentences of T, $\{\mathcal{A}_0, \ldots, \mathcal{A}_n\}$, used in the deduction of $\mathcal{F}$; therefore

$$\{\mathcal{A}_0, \ldots, \mathcal{A}_n\} \vdash \mathcal{F}$$

By the deduction theorem,

$$\vdash \mathcal{A}_0 \to (\mathcal{A}_1 \to \ldots (\mathcal{A}_n \to \mathcal{F}) \ldots),$$

the proof of which uses only logical axioms and rules. Since logical axioms are true in every model and logical rules preserve truth, we have

$$\models \mathcal{A}_0 \to (\mathcal{A}_1 \to \ldots (\mathcal{A}_n \to \mathcal{F}) \ldots);$$ adding T doesn't change truth:

$$T \models \mathcal{A}_0 \to (\mathcal{A}_1 \to \ldots (\mathcal{A}_n \to \mathcal{F}) \ldots)$$

Since $\mathcal{A}_0, \ldots, \mathcal{A}_n$ are members of T, any model of T must make $\mathcal{A}_0, \ldots, \mathcal{A}_n$ true:

$$T \models \mathcal{A}_0$$
$$\vdots$$
$$T \models \mathcal{A}_n$$

By the definition of a structure, $T \models (H \to K)$ requires either $T \not\models H$ or $T \models K$; that is, if $T \models H$, then $T \models K$.
Applying this definition, we can successively eliminate $\mathcal{A}_0, \ldots, \mathcal{A}_n$ from

$$T \models \mathcal{A}_0 \to (\mathcal{A}_1 \to \ldots \to (\mathcal{A}_n \to \mathcal{F}) \ldots)$$

If a single model $\mathcal{A}$ of T has $\mathcal{A} \models H \to K$, then $\mathcal{A} \not\models H$ or $\mathcal{A} \models K$

But isn't it (I don't know) possible that some model of T might $\models H$, yet $\not\models K$

to obtain

$\boxed{\Gamma \vDash \mathcal{F}.}$

(⇐) · Assume $\Gamma \vDash \mathcal{F}$.
Then any model of Γ makes $\mathcal{F}$ true (by definition).
Therefore $\Gamma \cup \{\neg\mathcal{F}\}$ has no model; for if it did, it would also be a model of Γ, which would make $\mathcal{F}$ true, and no model can make both $\mathcal{F}$ and $\neg\mathcal{F}$ true.
Therefore by the Fundamental Theorem, $\Gamma \cup \{\neg\mathcal{F}\}$ is inconsistent.
Therefore

$\Gamma \cup \{\neg\mathcal{F}\} \vdash$ contradiction (because it's inconsistent)

$\Gamma \vdash \neg\mathcal{F} \rightarrow$ contradiction (deduction theorem)

$\boxed{\Gamma \vdash \mathcal{F}}$ (tautology)

6/6

Norman V. Meyer

This is a revision of part (b) of HW #7.

HW #7 b) Derive completeness (Gödel) from the Fundamental Theorem.

Completeness theorem: If a sentence $\mathcal{F}$ is true in every $\mathcal{L}$-structure, then $\mathcal{F}$ is provable.

Proof: We wanted "strong" completeness $\Gamma \vdash \mathcal{F} \Leftrightarrow \Gamma \models \mathcal{F}$.

Assume $\mathcal{F}$ is true in every $\mathcal{L}$-structure.

Let S be the set of provable sentences. Since the axioms of logic are consistent, and the rules "preserve truth", S is consistent.

Consider any consistent set of sentences S that does not contain $\mathcal{F}$, but contains the logical axioms used in the proof of the Fundamental Theorem (i.e., excludes the Henkin axioms).

Let S' be the set of sentences provable from S, using the rules used in the proof of the Fundamental Theorem. Since the rules "preserve truth", it is impossible to derive both $\mathcal{Q}$ and $\neg\mathcal{Q}$ from S (S is consistent), so S' must also be consistent.

Suppose S doesn't contain $\mathcal{F}$, i.e., that $\mathcal{F}$ is not provable. Then we can add $\neg\mathcal{F}$ to S to obtain a consistent set of sentences $S' = S \cup \{\neg\mathcal{F}\}$. By the Fundamental Theorem, S' has a model $\mathcal{A}'$, i.e., $\mathcal{A}'$ is an $\mathcal{L}$-structure that makes all of S' true, in particular $\neg\mathcal{F}$. Thus $\mathcal{A}'$ makes $\mathcal{F}$ false. However, we assumed $\mathcal{F}$ is true in every $\mathcal{L}$-structure (contradiction). Therefore S' must contain $\mathcal{F}$, i.e., $\mathcal{F}$ must be provable.

I will give you 2/6 for this part, and you can submit a proof of the generalized result to increase your mark.

Total 6/12

12/12

Norman D. Megill
18.511 HW
Assigned: 10/26/89
Due: 11/2/89

HW #8 Show S_ω is a conservative extension of S.

An extension T of S is said to be conservative if for each sentence $\mathcal{F}$ in the language of S, $T \vdash \mathcal{F}$ only if $S \vdash \mathcal{F}$.

Let $\mathcal{F}$ be any sentence in the language $\mathcal{L}$ of S. Assume $S_\omega \vdash \mathcal{F}$. We must show $S \vdash \mathcal{F}$.

Each step in the proof of $S_\omega \vdash \mathcal{F}$ must be a logical axiom, a non-logical (i.e., Henkin) axiom, or the result of a rule.... Let k be the number of Henkin axioms used in the proof of $S_\omega \vdash \mathcal{F}$.

If $k=0$, then each step in the proof of $S_\omega \vdash \mathcal{F}$ can be duplicated in the language, axioms, and rules of S, so $S \vdash \mathcal{F}$.

A subtle point here is that Henkin constants don't exist in S_ω however, and can replace a constant c_i with a never-used variable y_i anywhere in a purely logical proof of $\mathcal{F}$; all arguments follow.

Suppose $k>0$. Let $H_1, \ldots, H_k$ be the Henkin axioms used in the proof of $S_\omega \vdash \mathcal{F}$. Since the Henkin axioms have no free variables, we can use the Deduction Theorem to construct a proof of

$$S_\omega - \{H_1, \ldots, H_k\} \vdash H_1 \to (H_2 \to \ldots (H_k \to \mathcal{F}) \ldots)$$

in this new proof, no Henkin axioms are used (only logical axioms and rules).

Notation: If H_i is $\exists x \mathcal{G} \to \mathcal{G}^x_{c_i}$, define $H_{y_i} \equiv \exists x \mathcal{G} \to \mathcal{G}^x_{y_i}$ where y_i is a new variable not used anywhere in the proof of $\mathcal{F}$, and $y_i \neq y_j$ if $i \neq j$.

Now, in the proof of $S_\omega - \{H_1, \ldots, H_k\} \vdash H_1 \to (H_2 \to \ldots (H_k \to \mathcal{F}) \ldots)$, only logical axioms are used. If a Henkin constant c_i is replaced with variable y_i in a logical axiom, the form of the axiom remains the same, so it is still an axiom. (The logical axioms are really axiom schemes that specify the general form of an axiom.)

I do not have the time or mind to quibble over whether this is so in our FOL, but it is perfectly possible in other systems.

Therefore we can replace all occurrences of Henkin constants c_i with variables y_i in the above proof to obtain a proof of

$$S_\infty - \{H_1, \dots, H_k\} \vdash H_{y_1} \to (H_{y_2} \to \dots (H_{y_k} \to \mathcal{F}) \dots)$$

In this proof, only the language of S is used, so this is also a proof of

$$S \vdash H_{y_1} \to (H_{y_2} \to \dots (H_{y_k} \to \mathcal{F}) \dots)$$

Next we want to eliminate the H_{y_i}'s. First look at H_{y_1}. Suppose $H_{y_1} = \exists x \mathcal{Q} \to \mathcal{Q}^x_{y_1}$. Then

$$S \vdash (\exists x \mathcal{Q} \to \mathcal{Q}^x_{y_1}) \to (H_{y_2} \to \dots \to (H_{y_k} \to \mathcal{F}) \dots)$$

$$S \vdash \forall y_1 \left((\exists x \mathcal{Q} \to \mathcal{Q}^x_{y_1}) \to (H_{y_2} \to \dots \to (H_{y_k} \to \mathcal{F}) \dots) \right) \quad \text{Gen. rule}$$

(y_1 allowed because y_1 is not in elements of Γ used in proof)

$$S \vdash \exists y_1 (\exists x \mathcal{Q} \to \mathcal{Q}^x_{y_1}) \to (H_{y_2} \to \dots \to (H_{y_k} \to \mathcal{F}) \dots)$$

from logic theorem $\forall x (P \to Q) \to (\exists x P \to Q)$ (x not free in Q) then modus ponens

Lemma: $\vdash \exists y_1 (\exists x \mathcal{Q} \to \mathcal{Q}^x_{y_1})$

Proof: $\vdash \exists x \mathcal{Q} \to \exists y_1 \mathcal{Q}^x_{y_1}$ (logic theorem)

$\vdash (\exists x \mathcal{Q} \to \exists y_1 \mathcal{Q}^x_{y_1}) \to \exists y_1 (\exists x \mathcal{Q} \to \mathcal{Q}^x_{y_1})$ (y_1 not free in $\exists x \mathcal{Q}$) (logic theorem; y_1 not free in $\exists x \mathcal{Q}$)

$\therefore \vdash \exists y_1 (\exists x \mathcal{Q} \to \mathcal{Q}^x_{y_1})$ (modus ponens)

$\therefore S \vdash (H_{y_2} \to \dots (H_{y_k} \to \mathcal{F}) \dots)$ Lemma, then modus ponens

We have eliminated H_{y_1}. Similarly, we eliminate $H_{y_2}, \dots, H_{y_k}$ one at a time, to end up with

$$\boxed{S \vdash \mathcal{F}}.$$

Norman D. Megill
18.511 HW
assigned: 10/26/89
Due: 11/2/89

HW #9 Give a nice proof of the fundamental theorem.

Fundamental theorem: If S is a consistent set of sentences, then S has a model. (We also assume that the language $\mathcal{L}$ of S is a fixed, countable 1st-order language.)

Outline of proof

1. Extend S to S_ω with Henkin axioms and constants.
2. Show S_ω is still consistent
3. Extend S_ω to $S_{\omega\omega}$ (maximally consistent set)
4. Define an $\mathcal{L}$-structure $\mathcal{A}$ based on $S_{\omega\omega}$
5. Show $\mathcal{A}$ is a model for S

1. Extend S to S_ω with Henkin axioms and constants. 1R / 12

Let $\mathcal{L}$ be the language of S.

Define, recursively, extensions (Henkinizations) of S and $\mathcal{L}$:

Let $\mathcal{L}_0 = \mathcal{L}$

Let $\mathcal{L}_{i+1} = h(\mathcal{L}_i)$, where $h(\mathcal{L}_i)$ is $\mathcal{L}_i$ plus a set of new constant symbols $\{c_{i,0}, c_{i,1}, \ldots\}$, one for each formula in $\mathcal{L}_i$ which has exactly one free variable: i.e., one for each element of $\{\mathcal{F}_{i,0}(x_{i,0}), \mathcal{F}_{i,1}(x_{i,1}), \ldots\}$

(this refers to whatever variable is free in $\mathcal{F}_{i,1}$, not to the $i+1$-th variable in the list of atomic symbols)

Notes: (1) The Henkinization $\mathcal{L}_1 = h(\mathcal{L})$ creates new formulas with one free variable because we added new constants to the language. This explains the need for $\mathcal{L}_2, \mathcal{L}_3, \ldots$ (2) The assumption that $\mathcal{L}$ is countable (has a countable # of non-logical symbols) permits us to enumerate $\mathcal{F}_{i,0}(x_{i,0}), \mathcal{F}_{i,1}(x_{i,1}), \ldots$

Let $S_0 = S$.

Let $S_{i+1} = h(S_i)$, where $h(S_i)$ is S_i plus a set of new axioms $\exists x_{ij} \mathcal{F}_{ij}(x_{ij}) \to \mathcal{F}_{ij}(c_{ij})$, $j = 0, 1, 2, \ldots$, one for each formula in the language with one free variable, previously enumerated.

Define the complete Henkinization of S:

$$\mathcal{L}_\infty \equiv \bigcup_i \mathcal{L}_i$$

$$S_\infty \equiv \bigcup_i S_i$$

2. Show S_∞ is consistent.

By HW #8, S_∞ is a conservative extension of S. Thus for any $\mathcal{F}$ in the language $\mathcal{L}$ of S, $S_\infty \vdash \mathcal{F} \Rightarrow S \vdash \mathcal{F}$.

Now if S_∞ is inconsistent, then $S_\infty \vdash \mathcal{G} \wedge \neg \mathcal{G}$ for some $\mathcal{G} \in S_\infty$, and by tautological reasoning (i.e., $\vdash (\mathcal{G} \wedge \neg \mathcal{G}) \to \mathcal{H}$ then modus ponens), $S_\infty \vdash \mathcal{F} \wedge \neg \mathcal{F}$ for any $\mathcal{F} \in S_\infty$. Pick an $\mathcal{F} \in S$. Then

$$S_\infty \vdash \mathcal{F} \wedge \neg \mathcal{F} \Rightarrow S \vdash \mathcal{F} \wedge \neg \mathcal{F} \quad \text{(since } S_\infty \text{ is conservative ext.)}$$

which is a contradiction, since we assumed S is consistent.

Therefore S_∞ is consistent.

3. Extend S_ω to $S_{\omega\omega}$ (maximally consistent set)

Define by recursion: (let $\mathcal{F}_1, \mathcal{F}_2, \ldots$ be an enumeration of sentences of $\mathcal{L}_\omega$)

$S_{\omega 0} = S_\omega$

$$S_{\omega,n+1} = \begin{cases} S_{\omega n} \cup \{\mathcal{F}_n\} & \text{if } S_\omega \cup \{\mathcal{F}_n\} \text{ is consistent} \\ S_{\omega n} \cup \{\neg\mathcal{F}_n\} & \text{otherwise} \end{cases}$$

Define $S_{\omega\omega} = \bigcup_n S_{\omega n}$

Note that $S_{\omega\omega}$ is consistent.

Proof: First, we show $S_{\omega n}$ is consistent by induction on n.

$S_{\omega 0} = S_\omega$ is consistent.

If $S_{\omega n}$ is consistent, then

if $S_{\omega n+1} = S_\omega \cup \{\mathcal{F}_n\}$, $S_{\omega n+1}$ is consistent by definition; otherwise

if $S_{\omega n} \cup \{\mathcal{F}_n\}$ is not consistent it must be the case that $S_{\omega n} \vdash \neg\mathcal{F}_n$. But in this case, we can add $\{\neg\mathcal{F}_n\}$ to $S_{\omega n}$ and $S_{\omega n+1}$ will be consistent.

Next, assume $S_{\omega\omega}$ is inconsistent. Then for some $\mathcal{F}$, $S_{\omega\omega} \vdash (\mathcal{F} \wedge \neg\mathcal{F})$; however, $\mathcal{F}$ has a finite proof so for some n, $S_{\omega n} \vdash (\mathcal{F} \wedge \neg\mathcal{F})$ (contradiction).

$\therefore$ **$S_{\omega\omega}$ is consistent**

Note that the language of $S_{\omega\omega}$ is still $\mathcal{L}_\omega$.

4. Define an $\mathcal{L}$-structure $\mathcal{A}$ based on $S_{\infty\infty}$

Let c and d be Henkin constants.

$c \sim d$ is defined as $S_{\infty\infty} \vdash c=d$, i.e., $(c=d) \in S_\infty$

($S_{\infty\infty}$ is maximal, so all derivations have length one.)

Show "$\sim$" is an equivalence relation.

Axiom 1: $\vdash \forall x (x=x)$
Axiom 2: $\vdash \forall x \forall y (x=y \to y=x)$
Axiom 3: $\vdash \forall x \forall y \forall z (x=y \to (y=z \to x=z))$
Axiom 4: $\vdash \forall x \mathcal{F} \to \mathcal{F}^x_t$, where t is variable free in t is bound in $\mathcal{F}$.

Reflexivity
1. $c \sim c$ because $\vdash \forall x (x=x)$ axiom 1
$\vdash c=c$ axiom 4, MP (modus ponens)

Symmetry
2. $c \sim d \Rightarrow d \sim c$ because $\vdash \forall x \forall y (x=y \to y=x)$ Ax. 2
$\vdash \forall y (c=y \to y=c)$ Ax. 4, MP
$\vdash (c=d \to d=c)$ Ax. 4, MP
$S_{\infty\infty} \vdash (c=d)$ assumption
$S_{\infty\infty} \vdash (d=c)$ MP

Transitivity
3. $c \sim d,\ d \sim e \Rightarrow c \sim e$
$\vdash c=d \to (d=e \to c=e)$ Ax. 3, MP, 4, MP, 4, MP, 4, MP
$S_{\infty\infty} \vdash c=d$ assumption
$S_{\infty\infty} \vdash d=e$ "
$\therefore S_{\infty\infty} \vdash c=e$ MP, MP

$\therefore$ "$\sim$" is an equivalence relation.

Define $[c] = \{c' \in \mathcal{L}_\infty \mid c \sim d\}$ (equivalence class of c)

Let the universe A of structure $\mathcal{A}$ be $\{[c] \mid c \text{ is a Henkin constant}\}$

Define constants: If d is an individual constant in $\mathcal{L}$, define

$$d^{\mathcal{A}} \overset{\text{def}}{\equiv} [c]$$

where c is the Henkin constant in the Henkin axiom $\exists x (x=d) \to c=d$.

To show that $c \sim d$:

$\vdash \forall x \neg(x=d) \to \neg(d=d)$	Ax. 4
$\vdash d=d \to \neg\forall x \neg(x=d)$	tautology
$\vdash d=d$	Ax. 1, Ax. 4, MP
$\vdash \neg\forall x \neg(x=d)$	MP
$\vdash \exists x (x=d)$	def
$S_{\infty\infty} \vdash \exists x (x=d) \to c=d$	Henkin axiom
$S_{\infty\infty} \vdash c=d$	MP
$c \sim d$	def.

Therefore $d^{\mathcal{A}} = [d]$

Define functions: If f is a function symbol in $\mathcal{L}$, define

$$f^{\mathcal{A}}([c_1], \ldots, [c_m]) \overset{\text{def}}{\equiv} [f(c_1, \ldots, c_m)]$$ where c_i are terms with no variables (constant terms)

To justify this definition, (to show it is unique) we must show that the equivalence class of a function is the same if its arguments are in the same equivalence class.

Axiom 5: $\vdash \forall x_1 \ldots \forall x_m \forall y_1 \ldots \forall y_m \big((x_1=y_1) \& \ldots \& (x_m=y_m)) \to f(x_1, \ldots, x_m) = f(y_1, \ldots, y_m)\big)$

Suppose $c_1 \sim d_1, \ldots, c_m \sim d_m$. Then

$S_{\infty\infty} \vdash f(c_1, \ldots, c_m) = f(d_1, \ldots, d_m)$ Ax5, repeated Ax.4, tautologies

i.e., $f(c_1, \ldots, c_m) \sim f(d_1, \ldots, d_m)$

Define relations: If R is a relation symbol in $\mathcal{L}$, define

$$R^a([c_1], \ldots, [c_n]) \overset{\text{def}}{\Leftrightarrow} R(c_1, \ldots, c_n) \in S_{\infty\infty}$$

$$[\text{i.e., } S_{\infty\infty} \vdash R(c_1, \ldots, c_n)]$$

To justify this definition, we must show that the R remains the same if its arguments are in the same equivalence class.

Axiom 6: $\vdash \forall x_1 \ldots \forall x_n \forall y_1 \ldots \forall y_n \left((x_1 = y_1 \& \ldots \& x_n = y_n) \rightarrow \left(R(x_1, \ldots, x_n) \leftrightarrow R(y_1, \ldots, y_n) \right) \right)$

Suppose $c_1 \sim d_1, \ldots, c_n \sim d_n$. Then

$$S_{\infty\infty} \vdash R(c_1, \ldots, c_n) \leftrightarrow R(d_1, \ldots, d_n)$$

by Ax. 6, repeated Ax. 4, tautology

i.e., $R(d_1, \ldots, d_n) \in S_{\infty\infty}$

5. Show $\mathcal{A}$ is a model for S.

We must show: $\mathcal{F} \in S \Rightarrow \mathcal{A} \vDash \mathcal{F}$.

Since $\mathcal{F} \in S \Rightarrow \mathcal{F} \in S_{\omega\omega}$, it will be sufficient to show $\mathcal{F} \in S_{\omega\omega} \Rightarrow \mathcal{A} \vDash \mathcal{F}$, i.e., that $\mathcal{A}$ is a model for $S_{\omega\omega}$. We will actually show $\mathcal{F} \in S_{\omega\omega} \Leftrightarrow \mathcal{A} \vDash \mathcal{F}$.

We will do this by induction on the number of logical connectives, n, in sentence $\mathcal{F}$.

$n=0$: (Note: $c, d, c_1, \ldots, c_m$ are constant terms)

Case 1: $\mathcal{F}$ is $c=d$

$c=d \in S_\omega \Leftrightarrow S_\omega \vdash c=d$ — all theorems are in S_ω

$\Leftrightarrow c \sim d$ — def.

$\Leftrightarrow [c]=[d]$ — (names of same elements in universe of $\mathcal{A}$)

$\Leftrightarrow \mathcal{A} \vDash c=d$ — def of any structure (def. of $\mathcal{A} \vDash \mathcal{F}$)

Case 2: $\mathcal{F}$ is $R(c_1, \ldots, c_m)$

$R(c_1, \ldots, c_m) \in S_{\omega\omega} \Leftrightarrow R^{\mathcal{A}}([c_1], \ldots, [c_m])$ — def of this structure

$\Leftrightarrow \mathcal{A} \vDash R(c_1, \ldots, c_m)$ — def. of any structure (def. of $\mathcal{A} \vDash \mathcal{F}$)

$n>0$:

Case 1: $\mathcal{F}$ is $\neg\mathcal{G}$, where $\mathcal{G} \in S_{\omega\omega} \Leftrightarrow \mathcal{A} \vDash \mathcal{G}$

$\mathcal{F} \in S_{\omega\omega} \Leftrightarrow \neg\mathcal{G} \in S_{\omega\omega}$ — def

$\Leftrightarrow \mathcal{G} \notin S_{\omega\omega}$ — ($\Rightarrow$) ($\Leftarrow$) $S_{\omega\omega}$ is consistent and maximal

$\Leftrightarrow \mathcal{A} \nvDash \mathcal{G}$ — induction hypothesis

$\Leftrightarrow \mathcal{A} \vDash \neg\mathcal{G}$ — a structure makes either $\mathcal{G}$ or $\neg\mathcal{G}$ true, the other false.

$\Leftrightarrow \mathcal{A} \vDash \mathcal{F}$ — def.

Case 2: $\mathcal{F}$ is $\mathcal{F}_1 \wedge \mathcal{F}_2$

$\mathcal{F} \in S_{\infty\infty} \Rightarrow \mathcal{F}_1 \wedge \mathcal{F}_2 \in S_{\infty\infty}$ def.

$\Rightarrow \mathcal{F}_1 \in S_{\infty\infty}$ and $\mathcal{F}_2 \in S_{\infty\infty}$

Since: $S_{\infty\infty} \vdash \mathcal{F}_1 \wedge \mathcal{F}_2$
$\Downarrow$ taut
$S_{\infty\infty} \vdash \mathcal{F}_1$, $S_{\infty\infty} \vdash \mathcal{F}_2$
$\Downarrow$ $S_{\infty\infty}$ maximal
$\mathcal{F}_1 \in S_{\infty\infty}$, $\mathcal{F}_2 \in S_{\infty\infty}$

$\Rightarrow a \vDash \mathcal{F}_1$ and $a \vDash \mathcal{F}_2$ ind. hyp.

$\Rightarrow a \vDash \mathcal{F}_1 \wedge \mathcal{F}_2$ if a structure makes $\mathcal{F}_1$ true and $\mathcal{F}_2$ true, it makes both true (def. of $\vDash$)

$\Rightarrow a \vDash \mathcal{F}$ def.

$a \vDash \mathcal{F} \Rightarrow a \vDash \mathcal{F}_1 \wedge \mathcal{F}_2$ def

$\Rightarrow a \vDash \mathcal{F}_1$ and $a \vDash \mathcal{F}_2$ property of (i.e., def. of $\vDash$) any structure

$\Rightarrow \mathcal{F}_1 \in S_{\infty\infty}$ and $\mathcal{F}_2 \in S_{\infty\infty}$ ind. hyp.

$\Rightarrow \mathcal{F}_1 \wedge \mathcal{F}_2 \in S_{\infty\infty}$ taut.; $S_{\infty\infty}$ is maximal

$\Rightarrow \mathcal{F} \in S_{\infty\infty}$ ✓ def

Since the set of propositional connectives $\{\neg, \wedge\}$ is complete, we can handle $\{\vee, \rightarrow, \leftrightarrow\}$ with definitions.

Case 3: $\mathcal{F}$ is $\exists x \mathcal{G}$, where $\mathcal{G}$ has a single free variable, x.

Induction hypothesis: $\mathcal{G}_c^x \in S_{\omega\omega} \Leftrightarrow a \vdash \mathcal{G}_c^x$

$\mathcal{F} \in S_{\omega\omega} \Rightarrow \exists x \mathcal{G} \in S_{\omega\omega}$ def.

$\Rightarrow S_{\omega\omega} \vdash \exists x \mathcal{G}$ one-step deduction from assumptions

$\Rightarrow S_{\omega\omega} \vdash \mathcal{G}_c^x$, where c is a Henkin const.

because: $\begin{cases} S_{\omega\omega} \vdash \exists x \mathcal{G} \rightarrow \mathcal{G}_c^x & \text{Henkin ax.} \\ \therefore S_{\omega\omega} \vdash \mathcal{G}_c^x & \text{MP} \end{cases}$

$\Rightarrow \mathcal{G}_c^x \in S_{\omega\omega}$ maximality of $S_{\omega\omega}$

$\Rightarrow a \vdash \mathcal{G}_c^x$ induction hyp. (which is true for an arbitrary c, including a Henkin const.)

$\Rightarrow a \vdash \exists x \mathcal{G}$ from def. of $a \vdash \exists x \mathcal{G}$

$\Rightarrow a \vdash \mathcal{F}$ def.

Conversely,

$a \vdash \mathcal{F} \Rightarrow a \vdash \exists x \mathcal{G}$ def.

$\Rightarrow a \vdash \mathcal{G}_c^x$ from def. of $a \vdash \exists x \mathcal{G}$

$\Rightarrow \mathcal{G}_c^x \in S_{\omega\omega}$ induction hypothesis

$\Rightarrow S_{\omega\omega} \vdash \mathcal{G}_c^x$ one-step deduction

$\Rightarrow S_{\omega\omega} \vdash \exists x \mathcal{G}$

because: $\begin{cases} \vdash \forall x \neg \mathcal{G} \rightarrow \neg \mathcal{G}_c^x & \text{Ax. 4} \\ \vdash \mathcal{G}_c^x \rightarrow \neg \forall x \neg \mathcal{G} & \text{taut.} \\ \vdash \mathcal{G}_c^x \rightarrow \exists x \mathcal{G} & \text{def.; taut.} \\ S_{\omega\omega} \vdash \exists x \mathcal{G} & \text{MP} \end{cases}$

$\Rightarrow \exists x \mathcal{G} \in S_{\omega\omega}$ maximality of $S_{\omega\omega}$

$\Rightarrow \mathcal{F} \in S_{\omega\omega}$ def.

This case also covers $\forall x$ quantifier, since we can define $\forall x \mathcal{F} \equiv \neg \exists x \neg \mathcal{F}$

Final note: In this proof, we did not (directly) use the following standard axioms + rules:

1. $\forall x(\mathcal{F} \to \mathcal{G}) \to (\forall x \mathcal{F} \to \forall x \mathcal{G})$
2. $\mathcal{F} \to \forall x \mathcal{F}$ if x is not free in $\mathcal{F}$
3. If $\mathcal{F}$ is an axiom, $\forall x \mathcal{F}$ is an axiom

(Bell + Machover)

However, we used the result from HW #8 that S_ω is a conservative extension of S. HW #8 used theorems of logic that require the use of these axioms and rules.

Philosophical Comment

This proof is nonconstructive because of the step which asks us to "construct" a maximally consistent set S_∞, i.e., for each sentence $\mathcal{F}$ (in a countable list), "decide" whether or not $S_{on} \vdash \neg\mathcal{F}$, and based on the result add either $\neg\mathcal{F}$ or $\mathcal{F}$ to S_{on}. I'll grant that $S_{on} \vdash \neg\mathcal{F}$ is either true or false. If it is true, we will eventually run into its proof by mere scanning all possible proofs. But if it is false, there is no guarantee that a procedure exists to determine it's false; a simple-minded scan of all possible proofs would get us "stuck" in an "infinite loop". Thus the proof is asking us to imagine the construction of something that may be theoretically impossible to construct. It is asking us to assume the existence of a construction which may in fact not exist. (I suppose this is an example of the philosophical issues related to the Axiom of Choice?)

this

this doesn't

AC not involved here; your observation hangs on ~~proof~~ effectiveness of deciding $S_\infty \vdash \neg\mathcal{F}$ is false

If we assume the AC, how does this become easier?

Norman D. Megill
18.511 HW
Assigned: 11/21/89
Due: 11/28/89

HW #11 Show consistency of the scheme, i.e., $\{e\}(a_0,\ldots,a_n)$ has at most one value.

Consider the computation tree of $\{e\}(a_0,\ldots,a_n)$. We assume that if $\{e\}$ is not the code of one of the schemes 1-5, or if the number of arguments required by $\{e\}$ is not $n+1$, then the predecessor (successor?) of $\{e\}(a_0,\ldots,a_n)$ is itself, forming an infinite path; this forces the tree to be infinite.

The computation tree is either finite or infinite. It is finitely branching by virtue of schemes 4 (composition) and 5 (enumeration).

If the tree is infinite, then some path on the tree is infinite (by König's lemma), so by definition it does not converge, i.e., has no value.

Assume the tree is finite. We will show that it yields a single value by induction on the depth d of the tree.

Basis: $d=0$. The tree must be a "terminal node", i.e., one of the schemes 1-3 (constant, projection, or successor). Each of these schemes yields a unique value.

Induction step: Assume that all finite trees with depth $< d$ $(d>0)$ yield a single value. If $d>0$, the tree must branch or continue to nodes of a lesser depth; only schemes 4 and 5 have this property.

Look at scheme 4 (composition):

$e = \langle 4, m+1, \langle\rangle, \underbrace{\langle\rangle, \ldots, \langle\rangle}_{h_1 \ldots h_m} \rangle$ ($\langle\rangle$ under g)

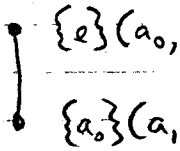
The functions defining $\{e\}$ all have a lesser depth and therefore have a unique value; by the definition of $\{e\}$,

single values → single value

$$\{e\}(a_0, \ldots, a_m) = g(h_1(a_0, \ldots, a_m), \ldots, h_m(a_0, \ldots, a_m)),$$

$\{e\}(a_0, \ldots, a_m)$ has a unique value.

Look at scheme 5 (enumeration):



$e = \langle 5, m+1 \rangle$

$\{a_0\}(a_1, \ldots, a_m)$ has a lesser depth than $\{e\}(a_0, \ldots, a_m)$ and therefore has a unique value by the induction hypothesis. Since $\{e\}(a_0, \ldots, a_m)$ and $\{a_0\}(a_1, \ldots, a_m)$ have the same value by definition, $\{e\}(a_0, \ldots, a_m)$ has a unique value.

Norman D. Megill
18.511 HW
assigned: 11/30/89
Due: 12/7/89

HW #12 Find a set A such that A is recursively enumerable but A is not recursive.

Consider the set A defined by

$$\forall n \left(n \in A \leftrightarrow \{n\}(n)\downarrow \right)$$

$\{n\}(n) = \{\langle 5,1\rangle\}(n,n)$ is partial recursive, so A is recursively enumerable by definition.

Suppose A is recursive. Then there exists a recursive characteristic function $c_A(n)$ such that

① $$c_A(n) = \begin{cases} 1 \text{ if } n \in A \text{ ; i.e., if } \{n\}(n)\downarrow \\ 0 \text{ if } n \notin A \text{ ; i.e., if } \{n\}(n)\uparrow \end{cases}$$

Define a function f derived from c_A:

② $$f(n) = \{\langle 5,1\rangle\}\left(2^6 \cdot c_A(n) \cdot \langle 1,1,1\rangle \,,\, n\right)$$

$$= \begin{cases} \{\langle 1,1,1\rangle\}(n) = 1 & \text{if } c_A(n) = 0 \\ \{\langle 7,1,1\rangle\}(n) = \text{undefined } (\uparrow) & \text{if } c_A(n) = 1 \end{cases}$$

$\therefore$ $f(n)$ is partial recursive since it is built from rec. fn's.

Let e_f be the index of f. Evaluate $f(e_f) \equiv \{e_f\}(e_f)$:

Case 1: Suppose $\{e_f\}(e_f)\downarrow$. Then $c_A(e_f) = 1$ by ①.
Then $\{e_f\}(e_f) = f(e_f)$ diverges by ②. (contradiction)

Case 2: Suppose $\{e_f\}(e_f)\uparrow$. Then $c_A(e_f) = 0$ by ①.
Then $\{e_f\}(e_f) = 1$ (converges) by ②. (contradiction)

$\therefore$ A cannot be recursive

Norman D. Megill
18.511 HW
Assigned: 12/7/89
Due: 12/14/89

HW #13 Find a pair of recursively inseparable r.e. sets

Let $A = \{n \mid \{n\}(n) = 0 \ \& \ \{n\}(n)\downarrow\}$
$B = \{n \mid \{n\}(n) = 1 \ \& \ \{n\}(n)\downarrow\}$
(redundant?)

① $A \cap B = \phi$ (by construction)

② $\neg\exists$ recursive R s.t. $A \subseteq R$ & $R \cap B = \phi$.

Proof: Suppose such an R exists. Let c_R be its characteristic function. Let e_R be the index of c_R, i.e., $c_R(n) = \{e_R\}(n)$.

Then
$e_R \in R \rightarrow c_R(e_R) = 1$ def. c_R
$e_R \in R \rightarrow \{e_R\}(e_R) = 1$ def. index
$e_R \in R \rightarrow e_R \in B$ def. of B

∴ Since $R \cap B = \phi$, $\boxed{e_R \notin R}$.

Also,
$e_R \notin R \rightarrow c_R(e_R) = 0$ def. c_R
$e_R \notin R \rightarrow \{e_R\}(e_R) = 0$ def. index
$e_R \notin R \rightarrow e_R \in A$ def. of A

∴ Since $A \subseteq R$, $\boxed{e_R \in R}$. (contradiction)

(end of proof)

HW #14 Prove: Any 2 disjoint co-r.e. sets can be separated by a recursive set.

Let the sets be called A and B.
We know: cA is r.e.
cB is r.e.
$A \cap B = \emptyset$

Note that $A \cap B = \emptyset \Rightarrow cA \cup cB = \mathbb{N}$. This means that if we enumerate cA and cB simultaneously, any natural number will eventually show up in either the enumeration of cA or cB.

Define a (total) recursive function f, with values assigned during the simultaneous enumeration

$$f(n) = \begin{cases} 1 & \text{if } n \text{ appears in the enumeration of } cB \text{ before it appears in the enumeration of } cA \\ 0 & \text{otherwise} \end{cases}$$

before: i.e., in fewer # of steps than

$f(n)$ will be total because $cA \cup cB = \mathbb{N}$.

Let $f(n)$ be the characteristic function of a set R. Then R is recursive because it has a recursive characteristic function.

Any element x in R is an element of cB, i.e., $x \notin B$, so $R \cap B = \emptyset$
Any element x not in R is an element of cA, i.e., $x \notin A$, so $A \subseteq R$.
$\therefore R$ separates A and B.

Norman D. Megill
18.511 HW
Assigned: 12/8/89
Due: 12/14/89

HW#15 (a) Prove Craig's lemma from the joint consistency theorem.

Craig's interpolation lemma: If $\vdash (\mathcal{F} \to \mathcal{G})$, then there is an $\mathcal{L}$ such that $\vdash (\mathcal{F} \to \mathcal{L})$ and $\vdash (\mathcal{L} \to \mathcal{G})$ and every non-logical symbol of $\mathcal{L}$ occurs in both $\mathcal{F}$ and $\mathcal{G}$. (Assume $\mathcal{F}$ and $\mathcal{G}$ have at least one non-logical symbol in common. Assume $\not\vdash \neg\mathcal{F}$ and $\not\vdash \mathcal{G}$. Otherwise let $\mathcal{L}$ be $\forall x(x=x)$.) (so T_1 and T_2 will be theories = consistent sets of sentences)

Proof: Let theory T_1 be $\{\mathcal{F}\}$, and T_2 be $\{\neg\mathcal{G}\}$.

$T_1 \cup T_2$ is inconsistent because:

$\mathcal{F}, \neg\mathcal{G} \vdash \neg\mathcal{G}$	ass.
$\mathcal{F}, \neg\mathcal{G} \vdash \mathcal{F}$	ass.
$\mathcal{F}, \neg\mathcal{G} \vdash \mathcal{F} \wedge \neg\mathcal{G}$	taut.
$\mathcal{F}, \neg\mathcal{G} \vdash \neg(\mathcal{F} \to \mathcal{G})$	taut.

but we assumed $\vdash (\mathcal{F} \to \mathcal{G})$.

Therefore, by joint consistency theorem, there does exist an $\mathcal{L}$ in the common language of T_1 and T_2 (i.e., $\mathcal{F}$ and $\mathcal{G}$) such that

$$T_1 \vdash \mathcal{L} \qquad T_2 \vdash \neg\mathcal{L}$$

This $\mathcal{L}$ is the interpolant because:

$T_1 \vdash \mathcal{L}$	$T_2 \vdash \neg\mathcal{L}$
$\mathcal{F} \vdash \mathcal{L}$	$\neg\mathcal{G} \vdash \neg\mathcal{L}$
$\vdash \mathcal{F} \to \mathcal{L}$	$\vdash \neg\mathcal{G} \to \neg\mathcal{L}$ ded. theorem
	$\vdash \mathcal{L} \to \mathcal{G}$ taut'ology

HW #15 (b) Prove the joint consistency theorem

Robinson's joint consistency theorem:
Let T_1 be a theory in the language $\mathcal{L}_1$
Let T_2 be a theory in the language $\mathcal{L}_2$
Then (a) and (b) are equivalent:
(a) $T_1 \cup T_2$ is consistent
(b) T_1 and T_2 agree on $\mathcal{L}_1 \cap \mathcal{L}_2$ (i.e., there does not exist an $\mathcal{F}$ in $\mathcal{L}_1 \cap \mathcal{L}_2$ such that $T_1 \vdash \mathcal{F}$ and $T_2 \vdash \neg\mathcal{F}$).

Proof:

(a)→(b): Suppose $T_1 \cup T_2$ is consistent.
Suppose there does exist an $\mathcal{F}$ in $\mathcal{L}_1 \cap \mathcal{L}_2$ such that $T_1 \vdash \mathcal{F}$ and $T_2 \vdash \neg\mathcal{F}$. Adding T_2 as additional assumptions to T_1, and vice-versa, we have $T_1 \cup T_2 \vdash \mathcal{F}$ and $T_1 \cup T_2 \vdash \neg\mathcal{F}$.
But this is inconsistent (contradiction).

(b)→(a) Suppose that T_1 and T_2 agree on $\mathcal{L}_1 \cap \mathcal{L}_2$.
We want to build a model for $T_1 \cup T_2$. This will show that $T_1 \cup T_2$ is consistent (because in a model, a sentence will evaluate to either true or false — not both)

We will use the Henkin method to build the model.
We start by building the models for T_1 and T_2 separately but in parallel:

1. Henkinize T_1, obtain $T_{1\infty}$; $\mathcal{L}_{1\infty}$	Henkinize T_2, obtain $T_{2\infty}$; $\mathcal{L}_{2\infty}$ (use different set of Henkin constants from $\mathcal{L}_{1\infty}$)

$T_{1\infty}$ and $T_{2\infty}$ agree on $\mathcal{L}_{1,\infty} \cap \mathcal{L}_{2,\infty}$ because Henkinization is a conservative extension of a set of formulas; so if $\nexists \mathcal{F}$ s.t. $T_1 \vdash \mathcal{F}$ and $T_2 \vdash \neg\mathcal{F}$, then $\nexists \mathcal{F}$ s.t. $T_{1\infty} \vdash \mathcal{F}$ and $T_{2\infty} \vdash \neg\mathcal{F}$.

2. Let $J_0, J_1, \ldots$ be a list of all sentences in $\mathcal{L}_{1\infty} \cap \mathcal{L}_{2\infty}$, i.e., $\mathcal{L}_1 \cap \mathcal{L}_2$.

(basis) First, we want either to add J_0 to both $T_{1\infty}$ and $T_{2\infty}$ so $T_{1\infty} \cup \{J_0\}$ and $T_{2\infty} \cup \{J_0\}$ agree on $\mathcal{L}_1 \cap \mathcal{L}_2$, or to add $\neg J_0$ to both $T_{1\infty}$ and $T_{2\infty}$ so that $T_{1\infty} \cup \{\neg J_0\}$ and $T_{2\infty} \cup \{\neg J_0\}$ both agree on $\mathcal{L}_1 \cap \mathcal{L}_2$. Suppose neither case is possible. Then there must be a formula $\mathcal{F}$ in $\mathcal{L}_1 \cap \mathcal{L}_2$ such that

$$T_{1\infty} \cup \{J_0\} \vdash \mathcal{F} \quad \text{and} \quad T_{2\infty} \cup \{J_0\} \vdash \neg\mathcal{F}$$

and a formula $\mathcal{G}$ in $\mathcal{L}_1 \cap \mathcal{L}_2$ such that

$$T_{1\infty} \cup \{\neg J_0\} \vdash \mathcal{G} \quad \text{and} \quad T_{2\infty} \cup \{\neg J_0\} \vdash \neg\mathcal{G}$$

Using the deduction theorem and tautologies,

$$T_{1\infty} \vdash (J_0 \to \mathcal{F}) \wedge (\neg J_0 \to \mathcal{G})$$
$$T_{2\infty} \vdash (J_0 \to \neg\mathcal{F}) \wedge (\neg J_0 \to \neg\mathcal{G})$$

Using the tautology

$$((J_0 \to \mathcal{F}) \wedge (\neg J_0 \to \mathcal{G})) \leftrightarrow \neg((J_0 \to \neg\mathcal{F}) \wedge (\neg J_0 \to \neg\mathcal{G})),$$

we conclude

$$T_{1\infty} \vdash \mathcal{H}$$
$$T_{2\infty} \vdash \neg\mathcal{H} \quad \text{where } \mathcal{H} \text{ is } ((J_0 \to \mathcal{F}) \wedge (\neg J_0 \to \mathcal{G}))$$

which contradicts the hypothesis that T_1 and T_2 (and hence $T_{1\infty}$ and $T_{2\infty}$) agree on $\mathcal{L}_1 \cap \mathcal{L}_2$.

(induction) Next, suppose $T_{1\infty} \cup \{K_0, \ldots, K_{i-1}\}$ and $T_{2\infty} \cup \{K_0, \ldots, K_{i-1}\}$ agree on $\mathcal{L}_1 \cap \mathcal{L}_2$, where each K_j is either J_j or $\neg J_j$. By exactly the same reasoning (wherein $T_{1\infty}$ is replaced by $T_{1\infty} \cup \{K_0, \ldots, K_{i-1}\}$ and $T_{2\infty}$ by $T_{2\infty} \cup \{K_0, \ldots, K_{i-1}\}$ in argument above) we can add either J_i or $\neg J_i$ to both of $T_{1\infty} \cup \{K_0, \ldots, K_{i-1}\}$ and $T_{2\infty} \cup \{K_0, \ldots, K_{i-1}\}$

In this manner, add all of $J_0, J_1, \ldots$ (or their complements) to $T_{1\infty}$ and $T_{2\infty}$.

Call the results $T_{1\infty\infty}$ and $T_{2\infty\infty}$.

3. Finally, extend $T_{1\infty\infty}$ and $T_{2\infty\infty}$ to maximally consistent sets with the remaining sentences. Since the remaining sentences are not in the common language, this extension will not affect the agreement between $T_{1\infty\infty}$ and $T_{2\infty\infty}$. Call the results $T_{1\infty\infty\infty}$ and $T_{2\infty\infty\infty}$.

By Henkin theory, we can now "read off" models for T_1 and T_2 from $T_{1\infty\infty\infty}$ and $T_{2\infty\infty\infty}$. Call the models $\mathcal{M}_1$ and $\mathcal{M}_2$.

The models must have the same (size) universe M, because any statements defining the size of the universe (e.g., $\exists x_1 \exists x_2 (x_1 \neq x_2)$) are in the common language.

Any relations or functions in the common language must be the same in both $\mathcal{M}_1$ and $\mathcal{M}_2$ because the maximal extensions of the common language sentences were performed identically in parallel.

Any relations or functions in T_1, not the common language, are irrelevant to T_2, and vice-versa.

Therefore we can combine the models for T_1 and T_2 to define a model for $T_1 \cup T_2$. Therefore $T_1 \cup T_2$ is consistent.

10/6/89 ~~((((P→Q)→(~R→~S)→R)→T)→((T→P)→(S→P)))~~ tautology

$(\mathcal{F} \to \mathcal{G}) \to ((\mathcal{G} \to \mathcal{H}) \to (\mathcal{F} \to \mathcal{H}))$

$\mathcal{F} \to (\mathcal{G} \to \mathcal{F})$

$(\neg\mathcal{F} \to \neg\mathcal{G}) \to (\mathcal{G} \to \mathcal{F})$

} intuitionism:
$\bot \to \mathcal{F}$ is axiom
"$\neg\mathcal{F}$" defined as $\mathcal{F} \to \bot$

≡ model thm. th.

PA $\mathcal{M} \models \mathcal{F}$ $PA \not\vdash \mathcal{F}$ ∨ $PA \not\vdash \neg\mathcal{F}$

By Peano Arith. if $PA' = PA \cup \{\mathcal{F}\}$, then $\exists \mathcal{G}$, $\mathcal{M} \models \mathcal{G}$ ←

WFT

(1) $A_1 - A_n$ $\overline{A}$ is ...

Norman Megill
Oct. 12, 1989

Mr. Picard - One of the axiom systems presented in the tutorial didn't seem quite right so I explored it further.

Theorem The following set of 3 axioms for P.C. is not complete, assuming the only rule is modus ponens.

1. $((\mathcal{F} \to \mathcal{G}) \to ((\mathcal{G} \to \mathcal{H}) \to (\mathcal{F} \to \mathcal{H})))$
2. $(\mathcal{F} \to (\mathcal{G} \to \mathcal{F}))$
3. $((\neg\mathcal{F}) \to (\neg\mathcal{G})) \to (\mathcal{G} \to \mathcal{F}))$

Proof: We will show that the WFF $(((\neg\mathcal{F}) \to \mathcal{F}) \to \mathcal{F})$ cannot be proved from these axioms. Since this WFF is a tautology, it follows that the axiom set is not complete.

To show that $(((\neg\mathcal{F}) \to \mathcal{F}) \to \mathcal{F})$ cannot be proved from the axioms, we show that it is "independent" from the axioms using the many-valued truth-table method in Mendelson, Intro. to Math. Logic, pp. 38-39. Consider the following tables:

A	¬A
0	1
1	0
2	2

A	B	A→B
0	0	0
1	0	0
2	0	0
0	1	1
1	1	0
2	1	2
0	2	2
1	2	0
2	2	0

If all assignments of 0, 1, or 2 to the letters of a WFF cause the WFF to evaluate to 0, then the WFF is called "select". Note that the table for A→B preserves "selectness" under modus ponens: if A is "select" and A→B is "select", so is B. (see 1st line of table).

It can be verified that all assignments to the letters of Axioms 1, 2, and 3 yield a value of 0, so the axioms are all "select".
For example, consider the assignment $\mathcal{F}=1$ and $\mathcal{G}=2$ in Axiom 3 (when $\mathcal{F}$ and $\mathcal{G}$ are propositional letters):

— why not wff?

$$(((\neg\mathcal{F})\rightarrow(\neg\mathcal{G}))\rightarrow(\mathcal{G}\rightarrow\mathcal{F}))$$

$$1 \quad 2 \quad 2 \quad 1$$

$$0 \quad 2 \quad 2$$

$$2$$

$$0$$

(For Axiom 1, there are 27 cases to verify; for Axioms 2 and 3, there are 9 cases each.)

On the other hand, $(((\neg\mathcal{F})\rightarrow\mathcal{F})\rightarrow\mathcal{F})$ is not "select". Consider $\mathcal{F}=2$:

$$(((\neg\mathcal{F})\rightarrow\mathcal{F})\rightarrow\mathcal{F})$$

$$2 \quad 2 \quad 2$$

$$2$$

$$0$$

$$2$$

This WFF evaluates to 2, so it is not "select". Since modus ponens preserves "selectness", this WFF cannot be deduced from Axioms 1, 2, and 3.

excellent!

Mendelson, Intro. to Math. Logic

5. Independence. Many-Valued Logics.

Given an axiomatic theory, a subset X of the axioms is said to be *independent* if some wf in X cannot be proved by means of the rules of inference from the set of those axioms not in X.

PROPOSITION 1.16. *Each of Axiom Schemas* (A1)–(A3) *is independent.*

PROOF.

(a) Independence of (A1). Consider the following tables.

A	$\sim A$
0	1
1	1
2	0

A	B	$A \supset B$
0	0	0
1	0	2
2	0	0
0	1	2
1	1	2
2	1	0
0	2	2
1	2	0
2	2	0

Given any assignment of the values 0, 1, 2 to the statement letters of a wf $\mathfrak{A}$, these tables determine a corresponding value of $\mathfrak{A}$. If it always takes the value 0, $\mathfrak{A}$ is called *select*. Now, modus ponens preserves selectness. Check that, if $\mathfrak{A} \supset \mathfrak{B}$ and $\mathfrak{A}$ are select, so is $\mathfrak{B}$. Verify also that all instances of Axioms (A2) (A3) are select. Hence, any wf derivable from (A2)–(A3) by modus ponens is select. However, $A_1 \supset (A_2 \supset A_1)$, which is an instance of (A1), is not select, since it takes the value 2 when A_1 is 1 and A_2 is 2.

(b) Independence of (A2). Consider the following tables.

A	$\sim A$
0	1
1	0
2	1

A	B	$A \supset B$
0	0	0
1	0	0
2	0	0
0	1	2
1	1	2
2	1	0
0	2	1
1	2	0
2	2	0

Let us call a wf which always takes the value 0 according to these tables *grotesque*. Modus ponens preserves grotesqueness, and all instances of Axioms

(A1) and (A3) are grotesque. (Exercise.) However, the instance $A_1 \supset (A_2 \supset A_3) \supset ((A_1 \supset A_2) \supset (A_1 \supset A_3))$ of (A2) takes the value 2 when A_1 is 0, A_2 is 0, and A_3 is 1, and, therefore, is not grotesque.

(c) Independence of (A3). If $\mathfrak{A}$ is any wf, let $h(\mathfrak{A})$ be the wf obtained by erasing all negation signs in $\mathfrak{A}$. For each instance $\mathfrak{A}$ of Axioms (A1)—(A2), $h(\mathfrak{A})$ is a tautology. Also, modus ponens preserves the property of a wf $\mathfrak{A}$ that $h(\mathfrak{A})$ is a tautology; for, if $h(\mathfrak{A} \supset \mathfrak{B})$ and $h(\mathfrak{A})$ are tautologies, then $h(\mathfrak{B})$ is a tautology. (Just note that $h(\mathfrak{A} \supset \mathfrak{B})$ is $h(\mathfrak{A}) \supset h(\mathfrak{B})$.) Hence, every wf $\mathfrak{A}$ derivable from (A1)–(A2) by modus ponens has the property that $h(\mathfrak{A})$ is a tautology. But $h((\sim A_1 \supset \sim A_1) \supset ((\sim A_1 \supset A_1) \supset A_1))$ is $(A_1 \supset A_1) \supset ((A_1 \supset A_1) \supset A_1)$, which is not a tautology. Hence, $(\sim A_1 \supset \sim A_1) \supset ((\sim A_1 \supset A_1) \supset A_1)$, an instance of (A3), is not derivable from (A1)–(A2) by modus ponens.

A	$\sim A$
0	0
1	1

A	B	$A \supset B$
0	0	0
1	0	0
0	1	1
1	1	0

EXERCISE 1.43. *Prove the independence of Axiom Schema* (A3) *by constructing tables for the connectives* $\sim$ *and* $\supset$.

The idea used in the proof of independence of Axiom Schemas (A1)–(A2) may be generalized to the notion of a many-valued logic. Call the numbers 0, 1, 2, . . . , "truth values", and let $0 \leqslant m < n$. The numbers 0, 1, . . . , m are called *designated values*. Take a finite number of "truth tables" representing functions from sets of the form $\{0, 1, \ldots, n\}^k$ into $\{0, 1, \ldots, n\}$. For each truth table, introduce a sign, called the corresponding *connective*. Using these connectives and statement letters, we may construct "statement forms", and every such statement form containing j distinct letters defines a "truth function" from $\{0, 1, \ldots, n\}^j$ into $\{0, 1, \ldots, n\}$. A statement form whose corresponding truth function takes only designated values is said to be *exceptional*. The numbers m, n and the basic truth tables are said to define a (finite) *many-valued logic* M. An axiomatic theory involving statement letters and the connectives of M is said to be *suitable* for M if and only if the theorems of the theory coincide with the exceptional statement forms of M. All these notions obviously can be generalized to the case of an infinite number of truth values. If $n = 1$ and $m = 0$, and the truth tables are those given for $\sim$ and $\supset$ in §1, the corresponding 2-valued logic is that studied in this chapter. The exceptional wfs in this case were called tautologies. The system L is suitable for this logic, as proved in Propositions 1.11 and 1.13. In the proofs of the independence of Axiom Schemas (A1)–(A2), two three-valued logics were used.

EXERCISES

1.44. (McKinsey-Tarski) Consider the axiom system P in which there is exactly one binary connective $*$, the only rule of inference is modus ponens (i.e., $\mathfrak{B}$ follows from $\mathfrak{A}$ and $\mathfrak{A} * \mathfrak{B}$), and the axioms are all wfs of the form $\mathfrak{A} * \mathfrak{A}$. Show that P is not suitable for any (finite) many-valued logic.

10/13/89
Tutorial

Axiom of choice.

$$\forall x \; \exists y \; \varphi(x,y) \rightarrow \exists f \; \varphi(x, fx)$$

f is the i^{th}.

for an n-place symbol R,

$R^{\prod_{i \in I} a_i}$ is defined as

$$\{ \langle h_1, \ldots, h_m \rangle : h_1(i), \ldots, h_m(i) \in R^{a_i} \text{ for } i \in I \}$$

h_1 evaluated at i

Tutorial
10/20/89

Skolem — nonstd mod of arith
(16th Hw prob.)

J N Krowski

Compactness th.

T is a set of sentences

if every $T_0 \subseteq T$ T_0 finite has a model,
then T has a model

I = set of finite subsets of T

$\{T_0 : T_0 \subseteq T, T_0 \text{ finite}\}$

---

dual ideal (= filter) over I

D is a filter over $I \equiv D \subseteq \mathcal{P}(I)$

$\emptyset \notin D \quad I \in D$

$\forall x, y \in D \quad x \wedge y \in D$

$\forall x \in D \quad x \subseteq y \subseteq I \Rightarrow y \in D$

"upwardly closed up to I"

D is maximal =
$\forall$ filter D' $\quad D \subseteq D' \Rightarrow D = D'$

$\Leftrightarrow$ D is ultrafilter = $\forall x \subseteq I \quad (x \in D \vee I - x \in D)$

---

consider $\{A_i : i \in I\}$ where $A_i \neq \emptyset$

let D = filter over I

$$\prod_{i \in I} A_i = \left\{ h \mid h : I \to \bigcup_{i \in I} A_i \text{ s.t. } h(i) \in A_i \right\}$$

we want a reduced product

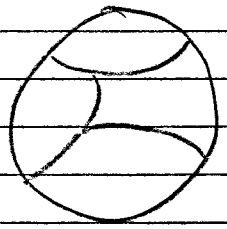
$$\frac{\prod_{i\in I} A_i}{D} \qquad \frac{\prod_{i\in I} a_i}{D}$$

↑ is the ← domain of the

equivalence classes of f's

$$f \sim g \equiv \{i : f(i) = g(i)\} \in D$$

$[h]$ = equivalence class of h



$$\frac{\prod_{i\in I} A_i}{D} = \{[h] : h \in \prod_{i\in I} A_i\}$$

reduced product

$\frac{\prod_{i\in I} A_i}{D}$ is an ultraproduct iff D is an ultrafilter over I

$$E = (D \subseteq D' \subseteq D'' \subseteq \dots)$$

$x, y \in E \qquad x \in D^n$

$x \notin D^m$

$x \in D^m$

ultrapowers and to generate new models from other ones

$$R([h_1], \ldots, [h_n]) \Leftrightarrow \{i : R^{a_i}(h_1(i), \ldots, h_n(i))\} \in \mathcal{D}$$

$$f([h_1], \ldots, [h_n]) = [h_{n+1}]$$

$$\Leftrightarrow \{i : f^{a_i}(h_1(i), \ldots, h_n(i)) = h_{n+1}(i)\} \in \mathcal{D}$$

Tutorial 10/27/89

18.511

$\{\wedge, \neg, \exists, x_0, x_1, \ldots\}$

$\mathcal{L} = \{\varepsilon\}$

$\mathcal{L} = \{S, 0, +, \cdot\}$

Let S be a consistent set of sentences
Then S has a model

$S \vdash \exists$ wff $\mathcal{F}$ $S \vdash (\mathcal{F} \wedge \neg \mathcal{F})$

Tutorial 11/3/89

Henkin's method

K countable 1st° language
Σ be a set of sentences of K

$h(K)$ $\quad F = \{\mathcal{F}_i(x) : i = 0, 1, 2 \ldots\}$ set of all formulas with 1 free variable (x is whatever variable it happens to be)
$h(\Sigma)$

$h(K)$ = Henkinization of language K
= K + for each i, c_i s.t. $c_i \notin K$ $\quad i \neq j \to c_i \neq c_j$

$\exists x \mathcal{F}_i(x) \to \mathcal{F}_i(c_i)$ Henkin axiom of language $h(K)$

$h(\Sigma) = \Sigma$ + Henkin axioms for each $\mathcal{F}_i(x) \in F$

Fix 1st° language $\mathcal{L}$ (countable)
T = set of sentences of $\mathcal{L}$

Fundamental Th $\quad T$ consistent $\Rightarrow$ T has a model

[T consistent $\Leftrightarrow$ $T \not\vdash \mathcal{F} \wedge \neg\mathcal{F}$, for no $\mathcal{F}$ in $\mathcal{L}$]

$\Leftrightarrow$ not($T \vdash \mathcal{F}$ for all $\mathcal{F}$)

$\mathcal{L}_\infty = \bigcup_i \mathcal{L}_i$
$\mathcal{L}_0 = \mathcal{L}$
$\mathcal{L}_{i+1} = h(\mathcal{L}_i)$ ← Henkinization of a language will add more formulas with a single free variable. So we need to Henkinize again.

$\Sigma_0 = \Sigma$
$\Sigma_{i+1} = h(\Sigma_i)$ $\quad \Sigma_\infty = \bigcup_i \Sigma_i$

There is a now Henkin axiom for every formula

$$\Gamma_{\omega\omega} = \Gamma_{\omega\omega_0} = \Gamma_\omega$$

$$\left.\begin{aligned} \Gamma_{\omega n+1} &= \Gamma_{\omega n} + \mathcal{F}_n \text{ if this is consistent} \\ &= \Gamma_{\omega n} + \neg\mathcal{F}_n \text{ otherwise} \end{aligned}\right\} \text{where } \mathcal{F}_n \text{ is a sentence of } \mathcal{L}_\omega$$

$c \approx d \equiv \Gamma_{\omega\omega} \vdash \underline{c} = \underline{d}$ $\quad c, d$ Henkin constants

$$\mathcal{F} \in \Gamma_{\omega\omega} \Leftrightarrow \Gamma_{\omega\omega} \vdash \mathcal{F}$$

Tutorial 11/3/89

We assume a finite system FOL of axiom-schemes and rules for 1st order logic.

$\Gamma \vdash \mathfrak{Z}$ ≡ There is a finite sequence $\mathfrak{Z}_1,\ldots\mathfrak{Z}_n$ s.t.
(i) $\mathfrak{Z}$ is $\mathfrak{Z}_n$, and
$(0\leq i\leq n)$ (ii) $\mathfrak{Z}_i\in\Gamma$ or $\mathfrak{Z}_i\in$FOL or $\mathfrak{Z}_i$ is the result of application of a rule of FOL to the $\mathfrak{Z}_j$'s, $j<i$.

Γ is *consistent* ≡ for no $\mathfrak{Z}$ does $\Gamma\vdash \mathfrak{Z}\wedge\neg\mathfrak{Z}$.

Henkin's method, from his 1947 thesis, for producing structures:

Let K be a countable 1st-order language and Σ a set of sentences of K.
Let $F=\{\mathfrak{Z}_i(x)\colon i=0,1,\ldots\}$ be the set of all formulae of K with just x free.
For each $\mathfrak{Z}_i\in F$, create a *Henkin constant* c_i, i.e., $c_i\notin K$ and $i\neq j \Rightarrow c_i\neq c_j$.
For each $\mathfrak{Z}_i\in F$, call $\exists x\mathfrak{Z}_i(x)\rightarrow\mathfrak{Z}_i(c_i)$ the Henkin axiom for $\mathfrak{Z}_i$.

Define: $h(K)$ = K + all Henkin constants for $\mathfrak{Z}_i\in F$; (i.e., $K\cup\{c_i\colon i=0,1,\ldots\}$)
Define: $h(\Sigma)$ = Σ + all Henkin axioms for $\mathfrak{Z}_i\in F$.

Define $\mathfrak{L}_i$ by recursion on i: $\mathfrak{L}_0 = \mathfrak{L}$;
$\mathfrak{L}_{i+1} = h(\mathfrak{L}_i)$. Define: $\mathfrak{L}_\omega = \bigcup_i \mathfrak{L}_i$

Define Σ_i by recursion on i: $\Sigma_0 = \Sigma$;
$\Sigma_{i+1} = h(\Sigma_i)$. Define: $\Sigma_\omega = \bigcup_i \Sigma_i$.

note: for every $\mathfrak{Z}(x)$ expressed in $\mathfrak{L}_\omega$, $\exists x\mathfrak{Z}(x)\rightarrow\mathfrak{Z}(c)$ is a member of Σ_ω, where c does not occur in $\mathfrak{Z}(x)$.

Fundamental Theorem: Suppose $\mathfrak{L}$ is a fixed, countable 1st-order language.
Then Γ is a consistent set of sentences $\Rightarrow$ Γ has a model.

Lemma: Γ_ω is consistent.
Induction on i.
$\Gamma_0=\Gamma$ is consistent by hypothesis.
Suppose Γ_i is consistent but $\Gamma_{i+1}\vdash\bot$.
Thus Γ_i + n Henkin axioms $\vdash\bot$.
This is impossible by sub-induction on n.
For n=1, Γ_i, $\exists x\mathfrak{Z}(x)\rightarrow\mathfrak{Z}(c)\vdash\bot$.
So $\Gamma_i\vdash\exists x\mathfrak{Z}(x)\rightarrow\mathfrak{Z}(c)\rightarrow\bot$, or
$\Gamma_i\vdash\neg(\exists x\mathfrak{Z}(x)\rightarrow\mathfrak{Z}(c))$,
$\Gamma_i\vdash\exists x\mathfrak{Z}(x)\wedge\neg\mathfrak{Z}(c)$, so
$\Gamma_i\vdash\exists x\mathfrak{Z}(x)\wedge\forall x\neg\mathfrak{Z}(x))$, by Rule of Constants (and tautology).
But now $\Gamma_i\vdash\neg\forall x\neg\mathfrak{Z}(x)\wedge\forall x\neg\mathfrak{Z}(x)$ by definition of $\exists$. $\bot$
For n>1, suppose Γ_i + n Henkin axioms $\nvdash\bot$ but Γ_i + n+1 Henkin axioms $\vdash\bot$.
Then Γ_i + those n Henkin axioms $\vdash H\rightarrow\bot$, where H is the n+1st H-axiom.
Then Γ_i + those n Henkin axioms $\vdash\bot$ by an argument similar to above.

Returning to proof of theorem, we now extend Γ_ω to a maximally conistent set $\Gamma_{\omega\omega}$:
$\Gamma_{\omega 0} = \Gamma_\omega$
$\Gamma_{\omega n+1} = \Gamma_{\omega n}\cup\{\mathfrak{Z}_n\}$ if such union is consistent
$= \Gamma_{\omega n}\cup\{\neg\mathfrak{Z}_n\}$ otherwise.

$\mathfrak{Z}_n$ is a sentence

Next, we define the domain for a model $\mathfrak{A}$ of Γ as the set of certain equivalence classes of Henkin constants defined in terms of provability in $\Gamma_{\omega\omega}$.

Define: $c \approx d \equiv$ c,d are Henkin constants & $c=d \in \Gamma_{\omega\omega}$ (i.e., $\Gamma_{\omega\omega} \vdash c=d$).
claim: $\approx$ is an equivalence relation.

(i) $c \in \Gamma_{\omega\omega} \Rightarrow \Gamma_{\omega\omega} \vdash c=c$, for $\forall x(x=x)$ is an axiom of FOL and $\forall x(\check{x}=x) \rightarrow c=c$ is an axiom (since no variable free in c (there are none) is bound in c=c)

(ii) $c \approx d \Rightarrow d \approx c$, for similar reasons (i.e., symmetry axiom of =).

(iii) $c \approx d \& d \approx e \Rightarrow c \approx e$, for similar reasons (i.e., transitivity axiom of =).

Let $[c]=\{d: d \approx c\}$. Let the domain A of $\mathfrak{A}$ be $\{[c]: c$ is a Henkin constant$\}$.

First show $\mathfrak{A}$ is an $\mathfrak{L}$-structure:

(1) $R^{\mathfrak{A}}([c_1],\ldots,[c_n])$ holds in $\mathfrak{A}$ iff $R(c_1,\ldots,c_n) \in \Gamma_{\omega\omega}$

(2) $f^{\mathfrak{A}}([c_1],\ldots,[c_n])$ holds in $\mathfrak{A}$ iff $f(c_1,\ldots,c_n) \in \Gamma_{\omega\omega}$

(3) $d^{\mathfrak{A}} = [c]$, where d is an individual constant of $\mathfrak{L}_1$, and c a H-constant.
The sentence "$\exists x(x=d) \rightarrow c=d$" $\in \Gamma_{\omega\omega}$.
If "$\exists x(x=d)$" $\in \Gamma_{\omega\omega}$, then "$c=d$" $\in \Gamma_{\omega\omega}$.

Next show $\mathfrak{A}$ is a model of Γ: prove: $\mathfrak{A} \models \exists \Leftrightarrow \exists \in \Gamma_{\omega\omega}$ by cases.

11/17/89
Tutorial
18.511

THEORY OF RECURSIVE FUNCTIONS

Original attempted definitions of recursive functions (the desire for which came out of David Hilbert's (1862-1943) formalist foundational program) always left out some functions which were intuitively recursive (=effectively computable) by not recursive according to the proposed definition. Probably Kurt Gödel (1906-1978) first understood why, although Gödel attributes a suggestion for the resulting definition of *general*[1] *recursive function* to Jacques Herbrand (1908-1931). Gödel believe that all previous definitions failed because they were too effective.

So the notion of an *effectively computable function* is intuitive. The formal definition of a recursive functions is, at least potentially, a correct formal characterization of the intuitive notion. The formalization of Turing machines and that of functions definable in the λ-calculus turn out to be equivalent to Gödel's notion of general recursive functions. This situation lent the first important support to Church's Thesis: the effectively computable functions are just the general recursive functions (hence functions which have Turing machines, etc.). We use "computable" for "effectively computable."

Intuitive Level:
Gödel: cannot effectively define the class of computable functions (of 1 vrbl).
pf: (diagonal argument)

Imagine some such definition, and suppose
$f_0(x)$, $f_1(x)$,..., $f_k(x)$,...
are the recursive functions according to the definition.
Now let $g(x) = f_x(x)+1$, which (intuitively) is effective.
So if the definition is correct, $g(x)=f_k(x)$ for some k.
But $g(k)=f_k(k)+1=f_k(k)$, contradiction.
So the diagonal function g(x) is effective but not recursive,
since $\forall k\ g \neq f_k$.
The imagined definition is inadequate, falls short.

Gödel pointed out that one *can* effectively define all computable partial functions. A computation of a partial function f is effective just in case, given any argument x, the computation yields the correct value $f(x)$ whenever that value exists, but when f(x) does not exist the computation yields nothing. (Thus if we try to determine if some f is partial by computing f at each possible value, we may never succeed; the computation may not end. Note: it follows from this that there is no effective procedure for deciding whether or not an arbitrary function is partial.)

---

[1]The adjective "general" is used because the notion of recursive itself is demonstrably not exhausted by that of primitive recursive function, and this demonstration is not the diagonal argument mentioned below. The standard example of a function that is recursive but not primitive recursive is the (generalized) Ackermann exponential, defined by the double recursion:

$f(0,0,y)=y$
$f(0,x+1,y)=f(0,x,y)+1$
$f(1,0,y)=0$
$f(z+2,0,y)=1$
$f(z+1,x+1,y)=f(z,f(z+1,x,y),y)$.

dard)

Definition of Partial Recursive Function:
A function (possibly partial) is *recursive* just in case it can be obtained by a finite number of applications of (4), (5′) and (6′) from (1)-(3):

(1) Constant Functions:
$f(x_1,\ldots,x_n)=c$, where c is some constant.

Note: f's arguments are irrelevant to the value of f.

(2) Projection (or Identity) Functions:
$f(x_1,\ldots,x_n)=x_j$, for $1\leq j\leq n$.

(3) Successor Function:
$f(x_1,\ldots,x_n)=x_1+1=x'$

Note: Besides x_1, f's arguments are irrelevant to the value of f.

primitive recursive functions

(4) Composition Function-Scheme
$f(x_1,\ldots,x_n)=g(h_1(x_1,\ldots,x_n),\ \ldots,\ h_m(x_1,\ldots,x_n))$.

Cf.: calling up programs to yield some input (value at an argument). The m-place function g and the n place functions h_j are here understood to be recursive.

(5′) Primitive Recursion Functions:
$f(0,x_2,\ldots,x_n)=g(x_2,\ldots,x_n)$
$f(x_1',x_2,\ldots,x_n)=h(x_1,f(x_1,\ldots,x_n),x_2,\ldots,x_n)$

Note: again, g and h are already known to be general recursive.

(6′) Minimalization Functions:
$f(x_1,\ldots,x_n)\simeq\mu y(g(y,x_1,\ldots,x_n)=0)$.

Note: "t≃s" means: either "t" and "s" are defined and t=s or neither are defined.
μ-operator is to be read "the least..."; "μy..." means "the least y such that ..."
g is assumed recursive.

partial equality

Friedman's def
$\{f_0^c\}$ language $\quad f^n c = \overbrace{f f \cdots f}^{n} c$

$A\subseteq N$
$n\in A \Leftrightarrow T\vdash \varphi(f^n c)$

A is rec. enum. iff A is expressible in some finite theory T

A is rec $\Leftrightarrow$ A is r.e. & $N-A$ is r.e.
compl. of A

Sack's Definition of Recursive Partial Functions:

A function (possible partial) is *recursive* just in case it has an index (i.e., according to the following assignment).

Note: indices are also called code numbers or gödel numbers. "{e}" will be used to designate the function with index e.

We begin by coding all the functions (1)-(4) via coding functions:

(0) Coding Functions:

$\langle a_1,\ldots,a_n\rangle = 2^{a_0}\cdot 3^{a_1}\cdot\ldots\cdot P_n^{a_n}$, where P_n is the n-th prime.

note: $\langle x_1,\ldots,x_n\rangle$ is a function of n arguments; $\langle a_1,\ldots,a_n\rangle$ is the value of $\langle x_1,\ldots,x_n\rangle$ at arguments $a_1,\ldots,a_n$

$\langle 1,n,c\rangle$ encodes the n-ary constant function equal everywhere to c.
$\langle 2,n,x_j\rangle$ encodes the n-ary function equal to x_j.
$\langle 3,n\rangle$ encodes the successor function of n arguments.
$\langle 4,n,e_0,e_1,\ldots,e_m\rangle$, where e_0 is the code of an m-place function g, and $e_1,\ldots,e_m$ are the codes of m n-ary functions $h_1,\ldots h_n$, encodes the n-ary function obtained by composition of g over the h's (as in (4) above).
$\langle 5,n???\rangle$ $\langle 5,n,\#\rangle$ (probably)

In Sack's treatment, we do not use (5') and (6'). Instead we use (5) below; I am uncertain how to state the coding for (5).

(5) Closure Condition:

$f(e,x_1,\ldots,x_n)$=the result of applying the e-th computable to $x_1,\ldots,x_n$. $\simeq\{e\}(x_1,\ldots,x_n)$.

Note: In (5) we do not call up the results of other programs, but the programs themselves; the presence of "e" in f is bound, and ranges over every recursive function (index).

$\tilde{x} \equiv x_1,\ldots,x_m$ $\quad f' \; e_f$

$f(e,\tilde{x}) = \{e\}(\tilde{x})$ $\quad\longrightarrow\quad \forall e\, g(e,\tilde{x}) \simeq \{e\}(\tilde{x})$

$\forall \tilde{x}\forall e \left(f(e,\tilde{x}) = \underbrace{\{e\}(\tilde{x})}_{\text{value of the partial recurs. fn. whose coding is } e}\right)$

{e : {e}e↓}

tutorial 12/1/89

Meet Next Friday at 2:30 in 2-142

Recursion Theory

Df.
$f(x_1,\ldots,x_n)$ is *partial recursive* ≡ for some e, $f(x_1,\ldots,x_n) \simeq \{e\}(x_1,\ldots,x_n)$.

To compute a partial recursive function f at arguments $n_1,\ldots,n_m$, associate $f(n_1,\ldots,n_m)$ with a computation tree, i.e., a tree all of whose nodes are expressions of the form $\{e\}(a_1,\ldots,a_i)$. Note: Nodes have no variables.

If a node is $\{e\}(a_1,\ldots,a_i)$, where e is not the index of a partial recursive function, then it has an immediate successor node, which is again $\{e\}(a_1,\ldots,a_i)$.

A node is *terminal* if it is the expression (the value of) of a coding, constant, projection or successor function. A node branches if it is the expression of (the value of) a computation or enumeration function. Note: Computation trees are finitely branching.

Df.
$f(n_1,\ldots,n_m)$ *converges* (written: $f(n_1,\ldots,n_m)\downarrow$) ≡ every path on its computation tree is finite.

Lemma: ∃ total rec f'n, t, s.t. $\forall e\ \{t(e)\} \simeq \begin{cases} \{\{e\}(e)\}, & \text{if } \{e\}(e)\downarrow \\ \text{null f'n}, & \text{if } \{e\}(e)\uparrow \end{cases}$

I.e., to compute $\{t(e)\}(x)$, try to compute $\{e\}(e)$. If $\{e\}(e)\uparrow$, then $\{t(e)\}(x)$ is the null function; if $\{e\}(e)\downarrow$ and $=m$, then $\{t(e)\}(x)\simeq\{m\}(x)$.

Proof:

Kleene Fixed Point Theorem (FPT):

Let f be total recursive. Then ∃e $\{e\}\simeq\{f(e)\}$.

Proof: Fix f and suppose t satisfies the lemma. f and t are total, so $f(t(x))\downarrow$ for arbitrary x. So there is an index c of f•t; i.e., $\{c\}(x)=f(t(x))$ for all x. Applying f•t to its own gödel number c, we have $\{c\}(c)\downarrow$ and $=f(t(c))$. Now by the lemma, $\{t(c)\}\simeq\{\{c\}(c)\}$, which is to say $\{t(c)\}\simeq\{f(t(c))\}$; i.e., t(c) is a fixed point.

To prove the equivalence of the above definition (which I call "ours") of partial recursive function with the usual Kleene definition it we need to show (i) that every function obtained via Kleene's primitive recursion (5′) and minimalization (6′) schemes can be obtained via our definition; and (ii) that the enumeration scheme can be obtained via the Kleene definition.

(ii) is shown by proving the Enumeration Theorem for the Kleene definition. The Enumeration Theorem is as follows:

$$\exists z\ \forall x,y_1,\ldots,y_n\ \{z\}(x,y_1,\ldots,y_n) \simeq \{x\}(y_1,\ldots,y_n).$$

(i) is shown as follows. We show that from our definition and the FPT we can derive the course-of-values recursion (the terminology ultimately derives from Frege, inventor of modern formal logic), and that from this (5′) is forthcoming.

Minimalization (6') comes from something called Selection, the argument for which involves "dovetailing" the computations of various partial recursive functions. Selection is obtained via the FPT.

The S-M-N theorem is used for (i), also due to Kleene:
S-M-N Theorem:

$\exists$ recursive f'n s $\forall e,x, y_1,\ldots,y_n$, $\{e\}(x,y_1,\ldots,y_n)\simeq\{s(e,x)\}(y_1,\ldots,y_n)$.

n.b.: the more general theorem holds when x is replaced by $x_1,\ldots,x_m$, thus its name: there is a m+1-place rec. f'n s whose values are the indices of an n-place function whose values equal those of an arbitrary m+n-place function {e}.

Df. $g\mathfrak{l}x \equiv \{\langle u,v\rangle: u<x \wedge v=g(u)\}$
Df. $g\mathfrak{l}x \equiv \Pi_{i<x}\, p_i^{1+g(i)}$ (which is =1 if x=0).

n.b.: $g\mathfrak{l}x$ is a sequence number for $g\mathfrak{l}x$; length of $g\mathfrak{l}x$ (written $/g\mathfrak{l}x/$ is x.

Lemma: For each total recursive I, there is a total recursive I_0 s.t. for all e, $\{I_0(e)\}\simeq I(\{e\}(x))$.
Idea: for variable e, if e is the method of computation for arguments less than x, then $I_0(e)$ is the method used at x.

Course-of-Values Recursion Scheme:
For each total I, there is a unique g s.t. $g(x)=I(g\mathfrak{l}x)$.

Proof: I_0 from the lemma has a fixed point, c, by FPT. So $\{c\}(x)\simeq\{I_0(e)\}(x)\simeq I(\{c\}(x))$. Let g(x) be $\{c\}(x)$; then $g(x)=I(g(x))$. I is total, so by induction, g is.

Selection:
$\exists$ partial recursive f'n t s.t for all e
(i) $\exists n(\{e\}(n)\downarrow) \Leftrightarrow t(e)\downarrow$
(ii) $\exists n(\{e\}(n)\downarrow) \rightarrow \{e\}(t(e))\downarrow$.

Pre-Selection: (dovetailing)
$\exists$ partial recursive f'n f s.t for all c,d
(i) $\{(c)_0((c)_1)\downarrow \vee \{(d)_0((d)_1)\downarrow \Leftrightarrow f(c,d)\downarrow$
(ii) $\{(c)_0((c)_1)\downarrow \vee \{(d)_0((d)_1)\downarrow \rightarrow f(c,d)\in\{c,d\} \wedge \{(f(c,d))_0\}((f(c,d))_1)\downarrow$