SECTION 6.2

LOGIC

First Order Predicate Logic

"$\forall x \exists y \, [x > y \Rightarrow y < x]$"

FORMULAS

Strings with a certain syntax

UNIVERSE

RELATIONS

MODEL

Truth of a formula

SOME FORMULAS ARE TRUE

How to Prove?

AXIOMS, RULES OF INFERENCE, LOGICAL DEDUCTION.

CAN WE AUTOMATE THIS PROCESS?

IS THE SET OF TRUE FORMULAS DECIDABLE?

FIRST-ORDER PREDICATE LOGIC

$$\forall q\, \exists p\, \forall x,y \left[p > q \wedge x,y > 1 \Rightarrow x \cdot y \neq p \right]$$

"There are infinitely many prime numbers."

$$\forall a,b,c,n \left[(a,b,c > 0 \wedge n > 2) \Rightarrow a^n + b^n \neq c^n \right]$$

"Fermat's Last Theorem: $a^n + b^n = c^n$ has no integer solutions for $n > 2$."

$$\forall q\, \exists p\, \forall x,y \left[p > q \wedge \left(x,y > 1 \Rightarrow (x \cdot y \neq p \wedge x \cdot y \neq p+2) \right) \right]$$

"THE TWIN PRIME CONJECTURE: There are infinitely many prime pairs, eg, 29, 31."

ALPHABET:

$$\Sigma = \{ \forall \; \exists \; (\;) \; \wedge \; \vee \; \Rightarrow \; \neg \; x \; R_1 \; R_2 \cdots \}$$

BOOLEAN OPERATIONS

$\wedge$ AND

$\vee$ OR

$\neg$ NOT $\sim$ EBCDIC $\bar{A}$

$\Rightarrow$ IMPLIES

QUANTIFIERS

$\forall$ FOR ALL

$\exists$ THERE EXISTS

VARIABLES

$x \; y \; z \; \cdots$

$x_0 \; x_1 \; x_2 \; x_3 \cdots$

$xx \quad xxx \quad xxxx \quad xxxxx$

RELATIONS

$R_1 \; R_2 \cdots R_N$

$\leq \quad + \quad \neq \quad x \uparrow n$

$$x + y = z \equiv R_{ADD}(x, y, z)$$

FORMULAS

SYNTAX

- Each Relation symbol must have the right # of args.

  $R_{ADO}(x, y, z, w)$ ← NOT OKAY.

- A FORMULA IS..:
  - A relation ("atomic formula")

    $R(x, 4, 7)$

  - OF THE FORM:

    $\left.\begin{array}{l} F_1 \wedge F_2 \\ F_1 \vee F_2 \\ F_1 \Rightarrow F_2 \end{array}\right\}$ where F_1 and F_2 are smaller formulas.

    $\neg F_1$

    and x is any variable.

  - $\forall x [F_1]$

    $\exists x [F_1]$

    (F_1)

$\forall x. (\ldots)$

$\exists y. (\ldots)$

$\neg \equiv \sim$

CAN WE CHECK IF A STRING IS A LEGAL FORMULA?

(WFF = "Well Formed Formula")

Sure. Decidable. Simple Parsing problem.

Free Variables.

$$\forall x \left[R_1(x, y) \Rightarrow R_2(z, x) \right.$$

bound

FREE

$\boxed{\text{DEFN}}$

A "STATEMENT" is a formula with <u>NO</u> free variables.

All variables are quantified.

$\forall x \exists y \,.\, R(x, y)$ ← STATEMENT

$\forall x \,.\, R(x, y)$ ← NOT A "STATEMENT"

ALGEBRAIC MANIPULATIONS
(Don't change meaning)

$$\sim \exists x . P \equiv \forall x . \sim P$$

$$\sim \forall x . P \equiv \exists x . \sim P$$

$$\sim (P \land Q) \equiv \sim P \lor \sim Q$$

etc.

PRENEX FORM

Without loss of generality...
Assume all statements in PRENEX form.
All quantifiers are at the front.

$$\forall x \exists y \forall z . \left(\cdots \overset{\lor \; \land \; \neg \; \Rightarrow}{x, y, z} \cdots \right)$$

WHAT DOES A STATEMENT "MEAN"?

How do we **INTERPRET** it?

Is it TRUE or FALSE?

WE NEED...

- A <u>UNIVERSE</u> eg: $\mathbb{N} = \{0, 1, 2, \cdots\}$
- INTERPRETATIONS FOR THE RELATION SYMBOLS.

$$R_1(x, y) \equiv x \leq y$$

$$R_2(x, y, z) \equiv x + y = z$$

Symbols in the alphabet

Relations with meaning in the "UNIVERSE"

DEFN: A "MODEL" consists of $(\mathbb{U}, P_1, P_2, \cdots P_K)$

$$P_1 \equiv R_1, \quad P_2 \equiv R_2, \quad \cdots \quad P_K \equiv R_K$$

Universe

Relations in the Universe, e.g. $\leq$

Symbols in the formula.

TRUTH

IS A GIVEN STATEMENT TRUE?

Must specify which Model!

YES (eg: Statement of Infinite # of Primes)

NO

MAYBE/UNKNOWN (eg: Twin Prime Conjecture)

EXAMPLE

$$\forall x, y, z . \big(R(x,y) \land R(y,z) \Rightarrow R(x,z) \big)$$

TRUE

INTERPRETATION #1: $R \equiv <$ $\quad \mathcal{U} \equiv \mathbb{N}$

$$\forall x,y,z \, (x<y \land y<z \Rightarrow x<z)$$

FALSE

INTERPRETATION #2: $R \equiv$ SUCC $\quad \mathcal{U} \equiv \mathbb{N}$

$$\forall x,y,z \, (x+1=y \land y+1=z \Rightarrow x+1=z)$$

$\boxed{\text{TAUTOLOGY}}$

Always true

... IN ANY MODEL.

$$\forall x. \left(R_1(x) \land R_2(x) \Rightarrow R_1(x) \right)$$

TRADITIONAL APPROACH TO MATH PROOFS

Axioms

A given set of statements assumed to be true without proof.

Rules of inference/deduction

A set of rules for transforming one statement into another.

Preserves truth.

Each rule is an algebraic (i.e., Algorithmic, Computable) procedure.

Proof

A sequence of statements from axioms to theorems, using only the rules of inference.

Theorems

- Proof is found (creative search)
- Proof is verified (computer?) to make sure it is legit.

Interpretation?

"Intuition" about the model may guide the search for proofs.

Or: The search can be conducted WITHOUT ANY UNDERSTANDING.

The symbols in any statement are just that: MEANINGLESS SYMBOLS.

Validity of this approach?

How else can one define "TRUTH"?

CONSIDER THE TWIN PRIME CONJECTURE.

x and $x+2$ are both prime.

There are an infinite #
of these twin primes.

$$\boxed{\text{Either it is TRUE or it is NOT TRUE.}}$$

Let's fix the Universe and
interpretation of symbols.
(the Model).

EXAMPLE

UNIVERSE $= \mathbb{N} = \{0, 1, 2, \cdots\}$

Relations: $+ \quad - \quad * \quad < \quad = \quad \geq \ldots$

[This is "Number Theory"]

Let's ask about the
Set of true statements
(It's a language, after all!)

DEFN

Given a particular model, $\mathcal{M}$,
[eg: Numbers, +, *, ...]
the set of true statements
is called "The THEORY OF $\mathcal{M}$."

$$Th(\mathcal{M})$$

[EXAMPLE: Number Theory

$$Th(\mathbb{N}, +, *)$$

is the set of all True statements
you can make using
$+ \quad * \quad = \quad$ etc.

NOTE: THIS IS <u>NOT</u> NECESSARILY
THE SET OF PROVABLE STATEMENTS!
(eg With Axioms, Rules of inference).

THEOREM

If we limit ourselves to statements we can make only using + [that is, without *] Then, the set of true statements is decidable.

$\mathrm{Th}(\mathbb{N}, +)$ is DECIDABLE

Given a statement, there is a procedure to tell whether it is true or not.

$$\forall x, y, z, a, b, c\ \big((x+y=z \wedge x+x=a \wedge y+y=b \wedge z+z=c) \Rightarrow a+b=c\big)$$

$$\begin{array}{c} x+y=z \\ x+y=z \\ \hline a+b=c \end{array}$$

$Th(\mathbb{N}, +, *)$

THEOREM

Number Theory is Undecidable.

Considering the Universe to be

$$\mathcal{U} = \mathbb{N} = \{0, 1, 2, \dots\}$$

and limiting ourselves to simple operations like $+$ and $*$, the set of true statements is undecidable.

PROOF IDEA

REDUCE A_{TM} TO THE PROBLEM OF DECIDING $Th(\mathbb{N}, +, *)$.

KURT GÖDEL'S INCOMPLETENESS THEOREM

FORMAL PROOF

A SEQUENCE OF STATEMENTS.
- STARTING WITH AXIOMS.
- USING PRECISE RULES OF INFERENCE.
- ENDING WITH THEOREM.

PROOF OF ϕ: ← A STATEMENT (NOT $\{\}$)

$\pi = (S_1, S_2, \ldots, S_L = \phi)$

ASSUMPTION: CORRECTNESS

PROOFS CAN BE CHECKED/VERIFIED.

$\boxed{\{\phi, \pi \mid \pi \text{ is a proof of } \phi\} \text{ is decidable}}$

ASSUMPTION: SOUNDNESS (CONSISTENCY)

IF A PROOF EXISTS, THEN THE STATEMENT IS TRUE.

THEOREM

The set of provable statements in Number Theory

$$\mathrm{Th}(\mathbb{N}, +, *)$$

is Turing Recognizable.

So we can enumerate all the PROVABLE statements

PROOF

- Finite Set of Axioms.
- Finite Set of Rules-of-inference.
- Each proof is finite in length.
- Each formula is finite in length.
- Just start listing them all out.
  → Enumerate all Proofs.

THEOREM

Some statement ψ
is true but
is not provable!

[Some statement in $Th(\mathbb{N}, +, *)$
has no proof.]

"Simple arithmetic may contains
truths which are inaccessible."

"Number Theory is way-deep."

PROOF (By contradiction)

Assume all true statements are provable.

Here is an algorithm to <u>DECIDE</u> the truth of a statement:

Look for a proof of ϕ.
Look for a proof of $\neg\phi$.
Do these searches simultaneously, in parallel.
One or the other will be true.
Eventually we'll find a proof of either ϕ or $\neg\phi$.

But we know that Number Theory is Undecidable!
(We can't decide the TRUTH of statements.)

CONTRADICTION!

IDEA:

"This sentence is not provable".

$\psi_{\text{UNPROVABLE}}$ = an encoding of this sentence into a statement in Number Theory.

Is it true?

Find a proof $\Rightarrow$ contradiction!

Therefore, it must not be provable.

Therefore it is true!

PROBLEM:

The statement contains "this sentence".

SOLUTION:

The RECURSION THEOREM!