Logic, the natural numbers and computability

Adam Boult (www.bou.lt)

April 30, 2025

Contents

Preface 2

I Propositional logic 3

1 Propositional logic 4

2 Inference in propositional logic 10

3 Axioms for propositional logic 13

II First-order logic 15

4 First-order logic 16

5 Gödel's completeness theorem and the compactness theorem 22

III Complete first-order arithmetic of natural numbers 24

6 Natural numbers and the successor function 25

7 Presberger arithmetic 26

8 Orderings 27

9 Subtraction and division 28

10 Divisors and prime numbers 30

11 Modulus and remainders 32

12 GCD and LCM 34

13 Skolem arithmetic 36

14 Löwenheim-Skolem theorem 37

IV Peano first-order etc 38

15 Robinson arithmetic 39

16 First-order peano arithmetic 40

17 The fundamental theorem of arithmetic 43

18 Finite sequences of natural numbers 47

19 Powers, exponents and logarithms of natural numbers 52

20 Gödel numbering 56

21 The Gödel incompleteness theorems 57

V Second-order arithmetic of natural numbers 58

22 Second-order logic 59

23 Second-order peano arithmetic 60

VI General Set Theory (GST) 61

24 Axiom schema of specification and cardinal numbers 62

25 Set algebra 66

26 The axiom of extensionality 69

27 Axiom of adjunction 72

28 Algebra of cardinality 73

29 Orderings on sets and ordinal numbers 75

VII Zermelo-Fraenkel set theory (ZF) 76

30 Zermelo–Fraenkel set theory 77

31 Axiom of union 84

VIII Computable functions 85

32 The halting problem 86

33 Effective procedures 87

34 Proof theory 88

35 Model theory 89

36 The Entscheidungsproblem 90

37 Kleene's s-m-n Theorem 91

38 Primative recursive functions 92

39 Computable functions 93

40 General recursive functions 94

41 The Ackermann function 95

IX Lambda calculus and combinatory logic 96

42 The Lambda calculus 97

43 Church encoding and Church numerals 98

44 Combinatory logic 99

Preface

This is a live document, and is full of gaps, mistakes, typos etc.

Part I

Propositional logic

Chapter 1

Propositional logic

1.1 Introduction

1.1.1 True and False

We start off with two statements:

- True - T or $\top$
- False - F or $\bot$

1.1.2 Propositional variables

We can represent T or F using a symbol:

θ

1.2 Operators

1.2.1 Unary operators

A unary operator takes one input and returns another.

Only negation, $\neg$ is of interest.

The following statements are equivalent:

- T
- $\neg F$

1.2.2 Binary operators

A binary operator takes an additional input.

- If then - $\theta \rightarrow \gamma$
- Then if - $\theta \leftarrow \gamma$
- Iff - $\theta \leftrightarrow \gamma$
- And / Conjunction - $\theta \land \gamma$
- Or / Disjunction - $\theta \lor \gamma$

1.2.3 Truth tables

1.2.4 Brackets

Operators can be shown together, with brackets. For example:

$(\alpha \lor \beta) \land \gamma$

Is not the same as:

$\alpha \lor (\beta \land \gamma)$

1.2.5 Atomic formulae

Atomic formulae are those without operators taking more than one input.

Literals, and negative literals, are types of atomic formula.

A literal is a formula with no operators.

θ

These are also known as positive literals.

Negative literals are the negation of a literal.

$\neg\theta$

1.2.6 Well-formed formulae

A well-formed formula is one which can be given a truth value.

The following is not a well-formed formula:

$\theta\land$

1.2.7 Interpretations

An interpretation assigns meaning to propositional variables in a formula.

For example an interpretation of the formula $\theta \lor \gamma$ assigns values to each of θ and γ.

1.2.8 Satifisable

A formula is satisfisable if there is some interpretation where it is true.

For example θ is satisfisable but $\theta \wedge \neg\theta$ is not.

1.2.9 Tautology

A formula is a tautology if it is true in all interpretations.

Examples of tautologies include:

- $\theta \vee \neg\theta$

1.3 Multi-valued logic

1.3.1 Multi-valued logic

We can have logic with more than two states.

1.4 Semantic consequence

1.4.1 Semantic consequence

A formula, A, semantically implies another, B, if for every interpretation of A, B is true.

We show this with:

$A \vDash B$

Formula B is satisfisable if there is some A where this is true.

For example: $A \wedge B \vDash A$

Formula B is a tautology if this is true for any A. We can also write this as $\vDash B$.

1.4.2 Logical equivalence

If $A \vDash B$ and $B \vDash A$ we say that A and B are logically equivalent.

This is shown as $A \Leftrightarrow B$.

1.4.3 How many unique operators are there?

An arbitrary operator takes n inputs are returns T or F.

With 0 inputs there is one posible permutation. For every additional input the number of possible permutations doubles. Therefore there are 2^n possible permutations.

For the operator with one permutation there are two operators. For every additional permutation the number of operator doubles. Therefore there are $2^{(2^n)}$ possible operations.

With 0 inputs, we need 2 different operators to cover all outputs. For 1 input we need 4 and for 2 inputs we need 16.

1.4.4 We don't need 0-ary operators

There are two unique 0-ary operators. One always returns T and the other always returns F. These are already described.

1.4.5 We need one unary operator

For the operators with 1 input we have:

- one which always returns T
- one which always returns F
- one which always returns the same as the input
- one which returns the opposite of the input

It is this last one, negation, shown as $\neg$ and is of most interest.

1.4.6 We can use a subset of binary operators

The full list of binary operators are included below.

Of these, the first two are 0-ary operators, and so are not needed. The next four are unary operators, and so are not needed.

The non-implications can be rewritten using negation.

1.4.7 Brackets replace the need for n-ary operators

N-ary operators contain 3 or more inputs.

N-ary operators can be defined in terms of binary operators.

As an example if we want an operator to return positive if all inputs are true, we can use:

$(\theta \land \gamma) \land \beta$

1.4.8 De Morgan's Laws

- $\neg(A \lor B) \Leftrightarrow (\neg A \land \neg B)$
- $\neg(A \land B) \Leftrightarrow (\neg A \lor \neg B)$

This expresses the duality of normal form.

Duality is the principle that binary operators have inverses, and when they are swapped with their inverse, the truth value of the statement is unaffected.

1.4.9 Normal form

This is where a formula is shown using only:

- And / Conjunction- $\wedge$
- Or / Disjunction - $\vee$
- Negation - $\neg$

The conjunctive normal form (CNF) is where a formula is converted to a normal form with the following layout:

$a \wedge b \wedge c \wedge d$

These letters can represent complex sub-formulae, in normal form.

Statements in this form are easier to evaluate, as each subformula can be evaluated separately. The statement is true only if all formulaes within are also true.

The disjunctive normal form (DNF) is similar for $\vee$.

$a \vee b \vee c \vee d$

1.4.10 Properties of the normal form

The normal binary operators are commutitive - $A \wedge B \Leftrightarrow B \wedge A$ and $A \vee B \Leftrightarrow B \vee A$

Both binary operators are associative - $(A \wedge B) \wedge C \Leftrightarrow A \wedge (B \wedge C)$ and $(A \vee B) \vee C \Leftrightarrow A \vee (B \vee C)$

Negation is complementary.

$A \wedge \neg A \Leftrightarrow F$

$A \vee \neg A \Leftrightarrow T$

Normal binary operators are absorbative.

$A \wedge (A \vee B) \Leftrightarrow A \; A \vee (A \wedge B) \Leftrightarrow A$

Identity.

$A \wedge T \Leftrightarrow A$

$A \vee F \Leftrightarrow A$

Distributivity.

$A \wedge (B \vee C) \Leftrightarrow (A \wedge B) \vee (A \wedge C)$

$A \vee (B \wedge C) \Leftrightarrow (A \vee B) \wedge (A \vee C)$

Chapter 2

Inference in propositional logic

2.1 Inference

2.1.1 Substitution

If we have a tautology, then we can substitute the formula of any propositional variable with any formula to arrive at any other tautology.

For example, we know that $\theta \vee \neg\theta$ is a tautology. This means that an arbitrary formula for θ is also a tautology.

An example is $(\gamma \wedge \alpha) \vee \neg(\gamma \wedge \alpha)$, which we know is a tautology, without having to examine each variable.

2.1.2 Syntactic consequence

Let us call the first formula A and the second B. We can then say:

$A \vdash B$

This says that: if A is true, then we can deduce that B is true using steps such as substitution.

2.1.3 Modus Ponens

Modus Ponens is a deduction rule. This allows us to use stpes other than substitution to derive new tautologies.

If A implies B, and A is true, then B is also true.

$(\theta \rightarrow \gamma) \wedge \theta \Rightarrow \gamma$

That is, if we can show that the following are true:

$\theta \rightarrow \gamma$

θ

We can infer that the following is also true:

γ

2.1.4 Theory

Results derived from substitution or induction are called theorems. Theorems often divided into:

- Theorems - important results
- Lemmas - results used for later theorems
- Corollaries - readily deduced from a theorem

We take a set of axioms, as true, and a deduction rule which enables us to derive additional formulae, or theorems. The collection of axioms and theorems is known as the theory.

2.1.5 Principle of explosion

If axioms contradict each other then it is possible to derive anything. That is:

$P \land \neg P \vdash Q$

We can prove this. If P and $\neg P$ are true, then the following is also true:

$P \lor Q$

We can then use $P \lor Q$ and $\neg P$ to imply Q.

This works for any proposition Q, including $\neg Q$.

As we can derive Q and $\neg Q$, our axioms are not consistent.

2.1.6 Resolution rule

Proof by resolution

If we have a string of or statements, $A \lor B \lor C$, and another which contains the completement of one element $X \lor \neg B \lor Y$, we can infer:

$A \lor C \lor X \lor Y$

If the second statement has only one formula, then we have:

$A \lor B \lor C$ and $\neg B$ implying $A \lor C$

2.1.7 Clauses and horn clauses

A clause is a disjunction of atomic formulae.

$A \vee \neg B \vee C$

This can be written in implicative form.

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

$\neg(A \vee \neg B) \rightarrow C$

$(\neg A \wedge B) \rightarrow C$

A horn clause is a clause where there is at most one positive literal. This means the implicative takes the form.

$(A \wedge B \wedge C) \rightarrow X$.

2.1.8 Inference with horn clauses

If the horn clause is true, and so is the normal form part, then X is also true.

As all inference with horn clauses uses Modus Ponens, it is sound.

Inference with horn clauses is also complete.

Chapter 3

Axioms for propositional logic

3.1 Axioms for propositional logic

3.1.1 Motivation for axioms for propositional logic

We discussed in the previous section the ability to derive new tautologies from others using substitution and Modus Ponens.

We now aim to identify a group of axioms from which all tautologies can be derived.

3.1.2 The axioms

The first is known as "Simplification". In words, this is "if it is cloudy, then if it is a Tuesday it is also cloudy."

$\theta \rightarrow (\gamma \rightarrow \theta)$

The second is called "Frege".

$(\alpha \rightarrow (\beta \rightarrow \gamma)) \rightarrow ((\alpha \rightarrow \beta) \rightarrow (\alpha \rightarrow \gamma))$

The third is "Transposition". Consider the statement "If there are no clouds in the sky, it is not raining." If this is true then it is also true that "If it is raining there are clouds in the sky."

$(\neg\theta \rightarrow \neg\gamma) \rightarrow (\gamma \rightarrow \theta)$

3.1.3 Independence of axioms

These axioms are independent. That is, if you take one away, you cannot derive it from the others.

These axioms are also effective. One could define all true formulae as axioms, however this is not effective.

3.1.4 Soundness of axioms

Soundness implies that all theories are true.

$T \vdash A \Rightarrow T \vDash A$

These axioms and the deduction rule are sound. We know that the axioms are tautologies, and we know that the inference rule is valid.

As the axioms are sound, the theories are consistent. That is, it is not possible for both θ and $\neg\theta$ to be theories.

3.1.5 Completeness of axioms

Completeness implies that all true formulae are theories.

$T \vDash A \Rightarrow T \vdash A$

3.1.6 Axioms and definitions

A definition is a conservative extension of the language. A definition statement, for example that a new symbol Z is always evaluated as false allows us to make additional statements, but it does not allow us to make additional statements in the original language.

An axiom allows us to generate additional statements in the original language, a definition does not.

Part II

First-order logic

Chapter 4

First-order logic

4.1 Zero-order logic

4.1.1 Terms and predicates

Predicates

Zero-order logic adds predicates. Like propositional variables, these have truth values. Unlike propositional variable, predicates take terms as inputs.

For example using propositional logic we can write the statement ”you are 25” as θ.

With preterites we can write this as $P(you, 25)$.

A propositional variable can be considered a special case of a predicate variable, where the number of inputs is 0.

4.1.2 Relations and equality

Relations

A special type of predicates is a relation. These take two terms and can be written differently: $P(x, y) \Leftrightarrow x \oplus y$

Equality

In preterite logic we define the relation for equality.

$a = b$

It is defined by the following:

- Reflexivity : $x = x$

- Symmetry: $x = y \leftrightarrow y = x$
- Transivity: $x = y \wedge y = z \rightarrow x = z$
- Substitution for functions: $x = y \rightarrow f(x) = f(y)$
- Substitution for formulae: $x = y \wedge P(x) \rightarrow P(y)$

4.1.3 Functions and brackets

Functions (or maps)

Functions take other terms, and are themselves terms. For example if we wanted to know if someone can legally drive in a specific country, we could use:

$P(you, age(UK))$

A function may not be able to produce an output for all inputs. For examples $age(green)$ has no interpretation.

Functions can also take different numbers of inputs. Constants, such as "you" and "UK" can be shown as functions with 0 inputs. As a result we could instead write:

$P(you(), age(UK()))$

We generally denote functions with a lower case letter, so would instead write:

$P(y(), a(b()))$

Functions are also called maps.

4.1.4 Signatures

Structures

A logical structure consists of:

- Domain
- Interpretation
- Signature

Domain

The domain is the set of variables in the structure.

We include an infinite number of variables.

Interpretation

The interpretation assigns values to propositional and predicate variables.

Signature

A logical signature describes the language of the logic which is used to construct statements. This includes:

- Functions
- Relations
- Operators

The language of a signature is all possible sentences, or formulae which can be constructed from this signature.

We include an infinite number of functions, relations and all operators.

4.1.5 Completeness of zero-order logic

A theory is complete if all true formulae are included.

Note that there are three types of formulae in a theory.

- Tautologies (always true)
- Refutable formulae (always false)
- Satisfiable formulae which are not tautologies (true in some, but not all, interpretations).

4.1.6 Injective, bijective and surjective functions

Injective functions

$f(a) = f(b) \rightarrow a = b$

Surjective functions

All points in codomain have at least one matching point in domain

Mapping info, details

Bijective

Both injective and surjective

Other

Identity function

The identity function maps a term to itself.

Idempotent

An idempotent function is a function which does not change the term if the function is used more than once. An example is multiplying by 0.

Inverse functions

An inverse function of a function is one which maps back onto the original value.

$g(x)$ is an inverse function of $f(x)$ if

$g(f(x)) = x$

Properties of binary functions

Binary functions can be written as:

$f(a, b) = a \oplus b$

A function is commutative if:

$x \oplus y = y \oplus x$

A function is associative if:

$(x \oplus y) \oplus z = x \oplus (y \oplus z)$

A function $\otimes$ is left distributive over $\oplus$ if:

$x \otimes (y \oplus z) = (x \otimes y) \oplus (x \otimes z)$

Alternatively, function $\otimes$ is right distributive over $\oplus$ if:

$(x \oplus y) \otimes z = (x \otimes z) \oplus (y \oplus z)$

A function is distributive over another function if it both left and right distributive over it.

4.1.7 Binary functions

Properties of binary functions

Binary functions can be written as:

$f(a, b) = a \oplus b$

A function is commutative if:

$x \oplus y = y \oplus x$

A function is associative if:

$(x \oplus y) \oplus z = x \oplus (y \oplus z)$

A function $\otimes$ is left distributive over $\oplus$ if:

$x \otimes (y \oplus z) = (x \otimes y) \oplus (x \otimes z)$

Alternatively, function $\otimes$ is right distributive over $\oplus$ if: $(x \oplus y) \otimes z = (x \otimes z) \oplus (y \oplus z)$

A function is distributive over another function if it both left and right distributive over it.

4.2 First-order logic

4.2.1 Writing first-order logic

Existential quantifier

We introduce a shorthand for "at least one term satisfies a predicate", that is:

$P(x_0) \lor P(x_1) \lor P(x_2) \lor P(x_2) \lor P(x_3)...$

The short hand is:

$\exists x P(x)$

niversal quantifier

We introduce another shorthand, this time for:

$P(x_0) \land P(x_1) \land P(x_2) \land P(x_2) \land P(x_3)...$

The shorthand is

$\forall x P(x)$

Free and bound variables

A bound variable is one which is quantified in the formula. A free variable is one which is not. Consider:

$\forall x P(x, y)$

In this, x is bound while y is free.

Free variables can be interpreted differently, while bound variables cannot.

We can also bind a specific variable to a value. For example 0 can be defined to be bound.

Ground terms

A ground term does not contain any free variables. A ground formula is one which only includes ground terms.

$\forall x$ x is a ground term.

$\forall x P(x)$ is a ground formula.

4.2.2 Inference rules for first-order logic

Existential instantiation

If P is true for a specific input, then there exists an input for P where P is true.

$P(r) \Rightarrow \exists x P(x)$

Existential generalisation

$\exists x P(x) \Rightarrow P(r)$

Where r is a new symbol.

Universal instantiation

If P is true for all values of x, then P is true for any input to P.

$\forall x P(x) \Rightarrow P(a/x)$

Where a/x represents substituting a for x within P.

Universal generalisation

If there is a derivation for $P(x)$, then there is a derivation for $\forall x P(x)$.

$\vdash P(x) \Rightarrow \vdash \forall x P(x)$

4.2.3 Duality of first-order logic

The dual of:

$\exists x \neg P(x)$

Is:

$\neg \forall x P(x)$

Chapter 5

Gödel's completeness theorem and the compactness theorem

5.1 Gödel's completeness theorem

5.1.1 Completeness of first-order logic

We previously showed that zero-order logic was complete. What about first-order logic?

Gödel's' completeness theorem says that for first order logic, a theory can include all tautologies, the first category.

If the completeness theorem is true and a formula is not in the theory, then the formula is either refutable or satisfiable under some, but not all interpretations.

That is, either the theory will contain θ, $\neg\theta$, or θ will be satisfiable in some but not all interpretations, and neither will be in the in theory.

To prove this we look for a proof that every formula is either refutable or true under some structure. So for an arbitrary formula θ we want to show it is either refutable or satisfiable under some interpretation.

5.1.2 Part 1: Converting the form of the formula

Remove free variables, functions

Note that if this is true, all valid formulae of the form below are provable:

$\neg\theta$

This means that there is no interpretation where the following is true:

θ

Conversely if $\neg\theta$ is not in the theory, then θ must be true under some interpretation.

That is, if all valid formulae are provable, then all

Reformulating the question:

This is the most basic form of the completeness theorem. We immediately restate it in a form more convenient for our purposes:

Theorem 2. Every formula θ is either refutable or satisfiable in some structure.

"$\theta$is refutable" means by definition "$\neg\theta$ is provable".

5.1.3 Decidability

Given a formula, can we find out if can be derived from the axioms? We can follow a process for doing so which would inform us if the formula was or was not a theorem. Alternative, the process could carry on forever.

If the process never carries on forever the system is decidable: there is a finite process to determine whether the formula is in or out. If the process halts for true formulas, but can carry on forever for false formulas, the system is semi-decidable. If the process takes a long time, we do not know if it is looping infinitely, or approaching its halt point.

Intuitively, use of axioms can make an existing formula shorter or longer, so finding all short formulas can require going forwards and backwards an infinite number of times.

Part III

Complete first-order arithmetic of natural numbers

Chapter 6

Natural numbers and the successor function

6.1 Gödel's completeness theorem

Chapter 7

Presberger arithmetic

7.1 Introduction

7.1.1 Addition

Just addition, no multiplication.

Chapter 8

Orderings

8.1 Ordering

8.1.1 Inequalities

Less than or equal

Orderings define relations between elements in a set, where one element can preceed the other.

Orderings are antisymmetric. That is, the only case where the relation is satisfied in both directions is if the elements are equal.

$(a \leq b) \land (b \leq a) \rightarrow (a = b)$

Orderings are transitive. That is:

$(a \leq b) \land (b \leq c) \rightarrow (a \leq c)$

Greater than or equal

Less than and greater than

The relation $\leq$ is refered to as non-strict.

There is a similar strict relation relation, $<$:

$(a \leq b) \land \neg(b \leq a) \rightarrow (a < b)$

Chapter 9

Subtraction and division

9.1 Integers

9.1.1 Subtraction of natural numbers

We have inverse functions for addition. This is subtraction.

For function $\oplus$, its inverse is $\oplus'$, as defined below:

$a \oplus b = c$

$b = c \oplus' a$

$f(a, b) = c \rightarrow f^{-1}(c, b) = a$

Subtraction

$a + b = c \rightarrow b = c - a$

There is no natural number b that satisfies:

$3 + b = 2$

While addition and multiplication are defined across all natural numbers, subtraction is not.

Properties of subtraction

Subtraction is not commutative:

$x - y \neq y - x$

Subtraction is not associative:

$x - (y - z) \neq (x - y) - z$

9.1.2 Division

Introduction

We have inverse functions for multiplication. This is division.

These will not necessarily have solutions for natural numbers or integers.

Division of natural numbers

$a.b = c \rightarrow b = \frac{c}{a}$

Division is not commutative

Division is not commutative:

$\frac{x}{y} \neq \frac{y}{x}$

Division is not associative

$\frac{\frac{x}{y}}{z} \neq \frac{\frac{x}{y}}{z}$

Division is not left distributive

Division is not left distributive over subtraction:

$\frac{a}{b-c} \neq \frac{a}{b} - \frac{a}{c}$

Division is right distributive

Division is right distributive over subtraction:

$\frac{a-b}{c} = \frac{a}{b} - \frac{b}{c}$

Division of integers

Chapter 10

Divisors and prime numbers

10.1 Prime numbers

10.1.1 Prime numbers and composite numbers

Definition

A prime number is a number which does not have any divisors other than 1 and itself.

By convention we do not refer to 0 or 1 as prime numbers.

Identifying prime numbers

Divisors must be smaller than the number. As a result it is easy to identify early prime numbers, as we can try to divide by all preceding numbers.

Examples of prime numbers

$[2, 35, 7, 11, 13, ...]$

Composite numbers

Composite numbers are numbers that are made up through the multiplication of other numbers.

They are not prime.

10.1.2 Relatively prime numbers

10.1.3 Euler's totient function

This functions counts numbers up to n which are relatively prime eg for 10 we have 1, 3, 7, 9.

So $\phi(10) = 4$

10.1.4 Euler's theorem

10.1.5 Fermat's little theorem

10.1.6 Pseudoprimes

10.2 Other

10.2.1 Frobenius number

Given a set of nautral numbers, the Frobenius number is the biggest number which can't be made as linear combination of the set.

Chapter 11

Modulus and remainders

11.1 Modulus and remainders

11.1.1 Remainders

Division is defined between natural numbers. However there are many cases where this division does not map to a natural number. For example:

$\frac{7}{3}$

We can divide 6 of the 7 by 3, giving 2 with 1 remaining.

Alternatively we can divide 3 of the 7 by 3, giving 1 with 4 remaining

Or we could divide 0 of the 7 by 3 giving 0 with 7 remaining.

The remainder refers to the lowest possible number - in this case 1.

11.1.2 Residue systems

Least residue system modulo n

This is the set of numbers from 0 to $n-1$.

Complete residue system

This a set of numbers none of which are congruent $\mod n$. That is, for no pair $\{a, b\}$ does $a \mod (n) = bmod(n)$

Reduced residue system

This is a complete residue system where all numbers are relatively prime to n.

11.1.3 Congruence

5 and 11 are congrument $\mod 3$

If $a \mod (n) = bmod(n)$ then a and b are congruent mod n.

Chapter 12

GCD and LCM

12.1 Divisors and multiples

12.1.1 Divisors and Greatest Common Divisors (GCD)

Divisors

The divisors d of a natural number n are the natural numbers such that $\frac{n}{d} \in \mathbb{N}$.

For example, for 6 the divisors are $1, 2, 3, 6$.

Divisors cannot be bigger than the number they are dividing.

Universal divisors

For any number $n \in \mathbb{N}^+$:

$\frac{n}{n} = 1$

$\frac{n}{1} = n$

Both 1 and n are divisors.

Common divisors

A common divisor is a number which is a divisor to two supplied numbers.

Greatest common divisor

The greatest common divisor of 2 numbers is as the name suggests.

So $GCD(18, 24) = 6$

12.1.2 Multiples and Lowest Common Multiples (LCM)

Multiples

The multiple of a number is it added to itself iteratively.

The multiples of 18 for example are:

$[18, 36, 54, 72, 90, ...]$

And for 24:

$[24, 48, 72, 96, 120, ...]$

Common multiples

Lowest common multiple

The lowest common multiple of 2 numbers is again as the name suggests.

So $LCM(18, 24) = 72$.

12.1.3 Coprimes

Also known as relatively prime.

Greatest common divisor is 1.

Chapter 13

Skolem arithmetic

13.1 Introduction

13.1.1 Multiplication

Just multiplication, no addition.

Chapter 14

Löwenheim-Skolem theorem

Part IV

Peano first-order etc

Chapter 15

Robinson arithmetic

Chapter 16

First-order peano arithmetic

16.1 Addition

16.1.1 Definition

Let's add another function: addition. Defined by:

$\forall a \in \mathbb{N}(a + 0 = a)$

$\forall ab \in \mathbb{N}(a + s(b) = s(a + b))$

That is, adding zero to a number doesn't change it, and $(a+b)+1 = a+(b+1)$.

16.1.2 Example

Let's use this to solve $1 + 2$:

$1 + 2 = 1 + s(1)$

$1 + s(1) = s(1 + 1)$

$s(1 + 1) = s(1 + s(0))$

$s(1 + s(0)) = s(s(1 + 0))$

$s(s(1 + 0)) = s(s(1))$

$s(s(1)) = s(2)$

$s(2) = 3$

$1 + 2 = 3$

All addition can be done iteratively like this.

16.1.3 Commutative property of addition

Addition is commutative:

$x + y = y + x$

16.1.4 Associative property of addition

Addition is associative:

$x + (y + z) = (x + y) + z$

16.2 Multiplication

16.2.1 Multiplication of natural numbers

16.2.2 Definition

Multiplication can be defined by:

$\forall a \in \mathbb{N}(a.0 = 0)$

$\forall ab \in \mathbb{N}(a.s(b) = a.b + a)$

16.2.3 Example

Let's calculate 2.2.

$2.2 = 2.s(1)$

$2.s(1) = 2.1 + 2$

$2.1 + 2 = 2.s(0) + 2$

$2.s(0) + 2 = 2.0 + 2 + 2$

$2.0 + 2 + 2 = 2 + 2$

$2 + 2 = 4$

16.2.4 Commutative property of multiplication

Multiplication is commutative:

$xy = yx$

16.2.5 Associative property of multiplication

Multiplication is associative:

$x(yz) = (xy)z$

16.2.6 Distributive property of multiplication

Multiplication is distributive over addition:

$a(b + c) = ab + ac$

$(a + b)c = ac + bc$

Chapter 17

The fundamental theorem of arithmetic

17.1 The Fundamental Theorem of Arithmetic

17.1.1 Euclidian division

Euclidian division is the theory for any pair of natural numbers, we can divide one by the other and have a remainder less than the divisor. Formally: $\forall a \in \mathbb{N}, \forall b \in \mathbb{N}^+, \exists q \in \mathbb{N}, \exists r \in \mathbb{N}[(a = bq + r) \wedge (0 \leq r < b)]$

Where $\mathbb{N}^+$ refers to natural numbers excluding 0.

That is, every natural number a is a multiple q of any other natural number b, plus another natural number r less than the other natural number b.

These are unique. For each jump in q, r falls by b. As the range of r is b there is only one solution.

$17 = 2.8 + 1$

$9 = 3.3 + 0$

17.1.2 Bezout's identity

For any two non-zero natural numbers a and b we can select natural numbers x and y such that

$ax + by = c$

The value of c is always a multiple of the greatest common denominator of a and b.

In addition, there exist x and y such that c is the greatest common denominator itself. This is the smallest positve value of c..

Let's take two numbers of the form $ax + by$:

$d = as + bt$

$n = ax + by$

Where $n > d$. And d is the smallest non-zero natural number form.

We know from Euclidian division above that for any numbers i and j there is the form $i = jq + r$.

So there are values for q and r for $n = dq + r$.

If r is always zero that means that all values of $ax + by$ are multiples of the smallest value.

$n = dq + r$ so $r = n - dq$.

$r = ax + by - (as + bt)q$

$r = a(x - sq) + b(y - tq)$

This is also of the form $ax + by$. Recall that r is the remainder for the division of d and n, and that $d = ax + by$ is the smallest positive value.

r cannot be above or equal to d due to the rules of euclidian division and so it must be 0.

As a result we know that all solutions to $ax + by$ are multiples of the smallest value.

As every possible $ax + by$ is a multiple of d, d must be a common divisor to both numbers. This is because $a.0 + b.1$ and $a.1 + b.0$ are also solutions, and d is their divisor.

So we know that the smallest positive solution is a common mutliple of both numbers.

We now need to show that that d is the largest common denominator. Consider a common denominator c.

$a = pc$

$b = qc$

And as before:

$d = ax + by$

So:

$d = pcx + qcy$

$d = c(px + qy)$

So $d \geq c$

17.1.3 Euclid's lemma

Statement

If a prime number p divides product $a.b$ then p must divide at least of one of a or b.

Proof

From Bezout's identity we know that:

$d = px + by$

Where p and b are natural numbers and d is their greatest common denominator.

Let's choose a prime number for p. There are no common divisors, other than one. As a result there are exist values for x and y such that:

$1 = px + by$

Now, we are trying to prove that if p divides $a.b$ then p must divide at least one of a and b, so let's multiply this by a.

$a = pax + aby$

We know that p divides pax, and p divides ab by definition. As a result p can divide a.

17.1.4 Fundamental Theorem of Arithmetic

Statement

Each natural number is a prime or unique product of primes.

Proof: existance of each number as a product of primes

If n is prime, no more is needed.

If n is not prime, then $n = ab$, $a, b \in \mathbb{N}$.

If a and b are prime, this is complete. Otherwise we can iterate to find:

$n = \prod_{i=1} p_i$

Proof: this product of primes is unique

Consider two different series of primes for the same number:

$s = \prod_{i=1}^{n} p_i = \prod_{i=1}^{m} q_i$

We need to show that $n = m$ and $p = q$.

We know that p_i divides s. We also know that through Euclid's lemma that if a prime number divides a non-prime number, then it must also divide one of its components. As a result p_i must divide one of q.

But as all of q are prime then p_i=q_j.

We can repeat this process to to show that $p = q$ and therefore $n = m$.

17.1.5 Existence of an infinite number of prime numbers

Existence of an infinite number of prime numbers

If there are a finite number of primes, we can call the set of primes P.

We identify a new natural number a by taking the product of existing primes and adding 1.

$a = 1 + \prod_{p \in P} p$

From the fundamental theorem of arithmetic we know all numbers are primes or the products of primes.

If a is not a prime then it can be divided by one of the existing primes to form number n:

$\frac{\prod^n p_i + 1}{p_j} = n$

$\frac{p_j \prod^n_{i \neq j} p_i + 1}{p_j} = n$

$\prod^n_{i \neq j} p_i + \frac{1}{p_j} = n$

As this is not a whole number, n must prime.

We can do this process for any finite number of primes, so there are an infinite number.

Chapter 18

Finite sequences of natural numbers

18.1 Sequences

18.1.1 Definition

A sequence is an ordered list of terms.

These are commonly maps from natural numbers to real (or complex) numbers.

We can use $a_i = f(i)$ to denote this.

If $f(i)$ is defined on all $i \in \mathbb{N}$ then the sequence is infinite. Otherwise it is finite.

If a sequence is defined on $n \in \mathbb{N}$ and $n \neq 0$ then the sequence must be defined on $n - 1$.

For example $a_0, a_1, a_2, ...$ is a sequence, but $a_1, a_2, ...$ is not.

18.1.2 Monotone sequence

A monotone sequence is one where each element is succeeded ordinally by the next entry.

For example:

$< 1, 2, 3, 6, 7 >$ is monotone

$< 1, 2, 3, 3, 4 >$ is not monotone

An increasing sequence is one where:

$\forall m \in \mathbb{N} \forall n \in \mathbb{N}[m > n \leftrightarrow a_m \geq a_n]$

A strictly increasing sequence is one where:

$\forall m \in \mathbb{N} \forall n \in \mathbb{N}[m > n \leftrightarrow a_m > a_n]$

A decreasing sequence is one where:

$\forall m \in \mathbb{N} \forall n \in \mathbb{N}[m > n \leftrightarrow a_m \leq a_n]$

A strictly decreasing sequence is one where:

$\forall m \in \mathbb{N} \forall n \in \mathbb{N}[m > n \leftrightarrow a_m < a_n]$

All strictly decreasing sequences are decreasing, and all strictly increasing sequences are increasing.

A monotone sequence is one which is either increasing or decreasing.

18.1.3 Subsequences

A subsequence of a sequence is the original sequence with some elements of the original removed, not changing the order.

For example:

$< 1, 3, 5 >$ is a subsequence of $< 2, 1, 3, 4, 7, 5 >$

18.2 Series

18.2.1 Definition

A series is the summation of a sequence. For a series a_n there is a corresponding series:

$s_n = \sum_{i=0}^{n} a_n$

Where:

$\sum_{i=0}^{n} a_i = a_0 + a_1 + a_2 + ... + a_n$

18.2.2 Multiplication of summations

If all members of a sequence are multiplied by a constant, so is each member of the series.

We can take constants out of the series:

$s_n = \sum_{i=0}^{n} a_i$

$s_n = \sum_{i=0}^{n} cb_i$

$s_n = a \sum_{i=0}^{n} b_i$

18.2.3 Summation of constants

If all elements of a sequence are the same, then the series is a multiple of that constant.

$s_n = \sum_{i=0}^{n} a_i$

$s_n = \sum_{i=0}^{n} c$

$s_n = nc$

18.2.4 Addition of summations

Consider a sequence $a_i = b_i + c_i$.

$s_n = \sum_{i=0}^{n} a_i$

$s_n = \sum_{i=0}^{n} (b_i + c_i)$

We can then split this out.

$s_n = \sum_{i=0}^{n} b_i + \sum_{i=0}^{n} c_i$

18.2.5 Summation from a different start point

$\sum_{i=0}^{n} a_i = a_0 + \sum_{i=1}^{n} a_i$

18.2.6 Multiple summations

$\sum_{i=0}^{n} \sum_{j=0}^{m} a_i = n \sum_{j=0}^{m} a_i$

$\sum_{i=0}^{n} \sum_{j=0}^{m} a_i b_j = \sum_{i=0}^{n} a_i \sum_{j=0}^{m} b_i$

18.3 Products

18.3.1 Definition

A product is a repeated multiplication of a sequence.

$p_n = \prod_{i=0}^{n} s_i$

18.3.2 Multiplication of products

We can take constants out of the product.

$p_n = \prod_{i=0}^{n} c a_i$

$p_n = a^n \sum_{i=0}^{n} a_i$

18.3.3 Products of constants

If $a_i = c$ then the summation is then of the form:

$p_n = \prod_{i=0}^n c$

$p_n = c^n \prod_{i=j}^n 1$

$p_n = c^n$

18.3.4 Combining products

If a sequence is the product of to other sequences then the product of the sequence is equal to the product of the two individual sequences.

$p_n = \prod_{i=0}^n a_i$

$p_n = \prod_{i=0}^n b_i c_i$

$p_n = \prod_{i=0}^n b_i \prod_{i=0}^n c_i$

18.3.5 Factorials

A factorial is a a product across natural numbers. That is:

$n! := \prod_{i=0}^n i$

18.4 Summation of natural numbers

18.4.1 Goal

Let's prove that:

$\sum_{i=0}^n i = \frac{n(n+1)}{2}$

18.4.2 Proof by induction

We use the inference rules Modus Ponens, which says that if X is true, and $X \to Y$ is true, then Y is true.

18.4.3 True for $n = 0$

We know this is true for $n = 0$:

$0 = \frac{0(0+1)}{2}$

$0 = 0$

18.4.4 If it's true for n, it's true for $n + 1$

We can also prove that if it true for n, it is true for $n + 1$.

$\sum_{i=0}^{n+1} i = \frac{(n+1)(n+2)}{2}$

$(n+1) + \sum_{i=0}^{n} i = \frac{n^2+3n+2}{2}$

If it is true for n, then:

$(n+1) + \frac{n(n+1)}{2} = \frac{n^2+3n+2}{2}$

$\frac{n^2+3n+2}{2} = \frac{n^2+3n+2}{2}$

$1 = 1$

18.4.5 Result

So we know that it is true for $n = 0$, and if it is true for n, then it is true for $n + 1$. As a result it is true for all natural numbers.

18.5 Bounded sequences

18.5.1 Bounded sequences

A function $f(x)$ on set X is bounded if:

$\exists M \in \mathbb{R}[\forall x \in X f(x) \leq M]$

A bounded sequence is a special case of a bounded function where:

$X = \mathbb{N}$

That is, a sequence is bounded by M iff:

$\forall n \in \mathbb{R}|f(a_n)| \leq M$

Chapter 19

Powers, exponents and logarithms of natural numbers

19.1 Powers

19.1.1 Recap

Previously we defined addition and multiplication in terms of successive use of the sucessor function. That is, the definition of addition was:

$\forall a \in \mathbb{N}(a + 0 = a)$

$\forall ab \in \mathbb{N}(a + s(b) = s(a + b))$

And similarly for multiplication:

$\forall a \in \mathbb{N}(a.0 = 0)$

$\forall ab \in \mathbb{N}(a.s(b) = a.b + a)$

Additional functions could also be defined, following the same pattern:

$\forall a \in \mathbb{N}(a \oplus_n 0 = c)$

$\forall ab \in \mathbb{N}(a \oplus_n s(b) = (a \oplus_n b) \oplus_{n-1} a)$

19.1.2 Powers

Powers can also be defined:

$\forall a \in \mathbb{N} a^0 = 1$

$\forall ab \in \mathbb{N} a^{s(b)} = a^b.a$

Note that by convention:

$a^{b^c} := a^{(b^c)}$

This reflects results from logarithms shown below.

$(a^b)^c = n^{c.log_n(a^b)} = n^{b.c.log_n a} = a^{b.c}$

And so there isn't need to write $a^b)^c$ and so a^{b^c} can be used to refer to $a^{(b^c)}$ unambiguously.

Note that this means that powers are non-associative.

19.1.3 Example

So 2^2 can be calculated like:

$2^2 = 2^{s(1)}$

$2^{s(1)} = 2.2^1$

$2.2^1 = 2.2.2^0$

$2.2.2^0 = 2.2.1$

$2.2.1 = 4$

Unlike addition and multiplication, exponention is not commutative. That is

$a^b \neq b^a$

19.1.4 Exponential rules

$a^b a^c = a^{b+c}$

$(a^b)^c = a^{bc}$

$(ab)^c = a^c b^c$

19.1.5 Binomial expansion

How can we expand

$(a+b)^n, n \in \mathbb{N}$

We know that:

$(a+b)^n = (a+b)(a+b)^{n-1}$

$(a+b)^n = a(a+b)^{n-1} + b(a+b)^{n-1}$

Each time this is done, the terms split, and each terms is multiplied by either a or b. That means at the end there are n total multiplications.

This can be shown as:

$(a+b)^n = \sum_{i=1}^{n} a^i b^{n-i} c_i$

So we want to identify c_i.

Each term can be shown as a series of n as and bs. For example:

- $aaba$
- $baaa$

For any of these, there are $n!$ ways or arranging the sequence, but this includes duplicates. If we were given n unique terms to multiply there would indeed by $n!$ different ways this could have arisen, but we can swap as and bs, as they were only generated once. So let's count duplicates.

There are duplicates in the as. If there are i as, then there are $i!$ ways of rearranging this. Similarly, if there are $n-i$ bs, then there are $(n-i)!$ ways or arranging this.

As a result the number of actual observed instances, c_i, is:

$c_i = \frac{n!}{i!(n-i)!}$

And so:

$(a+b)^n = \sum_{i=0}^{n} a^i b^{n-i} \frac{n!}{i!(n-i)!}$

We can also write this last term as:

$\binom{n}{i}$

19.1.6 Difference of two squares

$(a+b)(a-b) = a^2 - ab + ab - b^2$

$(a+b)(a-b) = a^2 - b^2$

19.2 Logarithms

19.2.1 Definition

If:

$c = a^b$

Then

$log_a c = b$

Product rule:

$a = c^{log_c a}$

$b = c^{log_c b}$

So:

$ab = c^{log_c ab}$

But also:

$ab = c^{log_c a} c^{log_c b}$

$ab = c^{log_c a + log_c b}$

So:

$log_c a + log_c b = log_c ab$

19.2.2 Power rule

$a = b^{log_b a}$

So:

$a^c = b^{log_b a^c}$

And separately:

$a^c = (b^{log_b a})^c$

$a^c = (b^{c log_b a})$

So:

$c log_b a = log_b a^c$

Chapter 20

Gödel numbering

20.1 Introduction

20.1.1 Gödel numbering

Gödel numbering assigns a unique number to each formula.

To contruct this we first assign a natural number to each symbol.

This gives us a sequence:

$\{x_1, x_2, x_3, ..., x_n\}$

We can assign a unique number to this by using the first n prime numbers.

$2^{x_1}3^{x_2}5^{x_3}...$

This number can then be prime factored to recover the sequence, and therefore the formula.

Chapter 21

The Gödel incompleteness theorems

21.0.1 Introduction

Part V

Second-order arithmetic of natural numbers

Chapter 22

Second-order logic

Chapter 23

Second-order peano arithmetic

Part VI

General Set Theory (GST)

Chapter 24

Axiom schema of specification and cardinal numbers

24.1 Defining sets

24.1.1 Axiom schema of specification

The axiom schema of unrestricted comprehension

We want to formalise the relationship between the preterite and the set. An obvious way of doing this is to add an axiom for each preterite in our structure that:

$\forall x \exists s[P(x) \leftrightarrow (x \in s)]$

This is known as ”unrestricted comprehension” and there are problems with this approach.

Consider a predicate for all terms which are not members of themselves. That is:

$\neg(x \in x)$

This implies the following is true:

$\forall x \exists s[\neg(x \in x) \leftrightarrow (x \in s)]$

As this is true for all x, it is true for $x = s$. So:

$\exists s[\neg(s \in s) \leftrightarrow (s \in s)]$

This statement is false. As we have inferred a false formula, the axiom of unrestricted comprehension does not work. This result is known as Russel's Paradox.

This is an axiom schema rather than an axiom. That is, there is a new axiom for each preterite.

Axiom schema of specification

To resolve Russel's paradox, we amend the axiom schema to:

$\forall x \forall a \exists s[(P(x) \land x \in a) \leftrightarrow (x \in s)]$

That is, for every set a, we can define a subset s for each predicate.

This resolves Russel's Paradox. Let's take the same steps on the above formula as in unrestricted comprehension;

$\forall x \forall a \exists s[(\neg(x \in x) \land x \in a) \leftrightarrow (x \in s)]$

$\exists s[(\neg(s \in s) \land s \in s) \leftrightarrow (s \in s)]$

So long as the subsets s are not members of themselves, this holds.

24.1.2 Implications of axiom schema of specification

All finite subsets exist

Finite subsets. Don't know about infinite subsets

If we can define a subset, by the axiom of specification it exists.

For example if set $\{a, b, c\}$ exists, we can define a preterite to select any subset of this.

For example we can use define a $P(x)$ as $x = a \lor x = b$ to extract the subset $\{a, b\}$.

If a subset is infinitely large,

Intersections of finite sets exist

Can prove exists from this axiom

If any set exists, the empty set exists

$\forall x \forall a \exists s[(P(x) \land x \in a) \leftrightarrow (x \in s)]$

24.1.3 Set-builder notation

Notation

We can use short-hand to describe sets.

$\{x \in S : P(x)\}$

This defines a set by a restriction. For example we will later be able to define natural numbers above 5 as:

$\{x \in \mathbb{N} : x > 5\}$

Class builder notation

Emuneration can be done through set builder notation too

Can define sets formally! defintion doesn't just affect sets

$\forall x(x \in C \leftrightarrow P(x))$

NB: We're not saying C exists

Can then use examples of equiv class

$\forall x(x \in C \leftrightarrow x = x)$

24.1.4 Empty set

We can use this to define the empty set - the set with no members.

$\varnothing = \{\}$

Using the above definition this is the same as writing:

$\forall x \neg (x \in \varnothing)$

24.1.5 Defining sets by enumeration

We can describe a set by the elements it contains.

$s = \{a, b, c\}$

This is a shorthand way of writing:

$\forall x(x \in s \leftrightarrow (x = a \vee x = b \vee x = c))$

24.1.6 Finite and infinite sets

Finite sets

A set is finite is there is a proper subset without a bijection.

Proper subset: $A \subset B$

For example for set $\{a, b, c\}$ There is no subset with a bijection.

Infinite sets

For the natural numbers, all natural numbers except 0 is a proper subset, and there is a bijection.

24.1.7 Cardinality

Cardinality of finite sets

The cardinality of a set s is shown as $|s|$. It is the number of elements in the set. We define it formally below.

Injectives, surjectives and bijectives

Consider 2 sets. If there is an injective from a to b then for every element in a there is a unique element in b.

If this injective exists then we say $|a| \leq |b|$.

Similarly, if there is a surjective, that is for every element in b there is a unique element in a, then $|a| \geq |b|$.

Therefore, if there is a bijection, $|a| = |b|$, and if there is only an injective or a surjective then $|a| < |b|$ or $|a| > |b|$ respectively.

Cardinality as a function

Every set has a cardinality. As a result cardinality cannot be a well-defined function, for the same reason there is no set of all sets.

Cardinality functions can be defined on subsets.

24.2 Introduction to sets

24.2.1 Membership relation

Say we have a preterite $P(x)$ which is true for some values of x. Sets allow us to explore the properties of these values.

We may want to talk about a collection of terms for which $P(x)$ is true, which we call a set.

To do this we need to introduce new axioms, however first we can add (conservative) definitions to help us do this.

We introduce a new relation: membership. If element x is in set s then the following relation is true, otherwise it is false:

$x \in s$

Sets are also terms. In first-order logic they will be included in quantifiers. Indeed, in set theory, we aim to treat everything as sets.

If a term is not a member of another term, we can write this using the non-member relation as follows:

$\forall x \forall s[\neg (x \in s) \leftrightarrow x \notin s]$

Chapter 25

Set algebra

25.1 Set algebra

25.1.1 Set union and intersection

We discuss functions. Just because we can write a function of sets which exist, does not mean the results of the functions exist. For that we need axioms discussed later.

Union function

We define a function on two sets, $a \vee b$, such that the result contains all elements from either sets.

$\forall a \forall x \forall y[a \in (x \vee y) \leftrightarrow (a \in x \vee a \in y)]$

This is commutative: $a \vee b = b \vee a$

This is associative: $(a \vee b) \vee c = a \vee (b \vee c)$

Intersection function

We define a function, $a \wedge b$, on two sets, such that the result contains all elements which are in both.

$\forall a \forall x \forall y[a \in (x \wedge y) \leftrightarrow (a \in x \wedge a \in y)]$

This is commutative: $a \wedge b = b \wedge a$

This is associative: $(a \wedge b) \wedge c = a \vee (b \wedge c)$

Distribution of union and intersection

Union is distributive over intersection: $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$

Intersection is distributive over union: $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$

25.1.2 Complements and disjoint sets

Disjoint sets

Sets are disjoint is there is no overlap in their elements. Two sets are s_i and s_j are mutually exclusive if:

$s_i \wedge s_j = \emptyset$

A collection of events s are all mutually exclusive if all pairs are mutually exclusive. That is:

$\forall s_i \in s \forall s_j \in s[s_i \wedge s_j \neq \emptyset \rightarrow s_i = s_j]$

Complement function

x^C is the completement. It is defined such that:

$\forall x[x \wedge x^C = \varnothing]$

For a set b, the complement with respect to a is all elements in a which are not in b.

$\forall x \in a \forall y \in b[x \in (a \setminus b) \wedge y \in (a \setminus b)]$

$b \wedge (a \setminus b) = \varnothing$

That is, b and $a \setminus b$ are disjoint.

Existence of the complement

For two sets a and b we can write $(a \setminus b)$. This is the set of elements of a which are not in b.

Consider the axiom of specification:

$\forall x \forall a \exists s[(P(x) \wedge x \in a) \leftrightarrow (x \in s)]$

We can also write

$\forall x \forall a \forall b \exists s[(x \notin b \wedge x \in a) \leftrightarrow (x \in s)]$

Which provides the complement, s.

25.1.3 Boolean algebra

Boolean algebra in propositional logic

We previously discussed properties of normal form, and the results from these properties.

If another structure shares these properties then they will also share the results.

Sets satisfy the definitions of a boolean algebra

If a mathematical structure has the following properties, it shares the results from normal form, and is a boolean algebra.

- Both binary operators are commutitive - $A \wedge B = B \wedge A$ and $A \vee B = B \vee A$
- Both binary operators are associative - $(A \wedge B) \wedge C = A \wedge (B \wedge C)$ and $(A \vee B) \vee C = A \vee (B \vee C)$
- Completements - $A \wedge \neg A = \emptyset$ and $A \vee \neg A = U$
- Absorption - $A \wedge (A \vee B) = A$ and $A \vee (A \wedge B) = A$
- Identity - $A \wedge U = A$ and $A \vee \emptyset = A$
- Distributivity - $A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C)$ and $A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C)$

These hold for sets, and so boolean algebra holds for sets.

25.1.4 Algebra on a set

Standard algebra

An algebra, Σ, on set s is a set of subsets of s such that:

- Closed under intersection: If a and b are in Σ then $a \wedge b$ must also be in Σ
- $\forall ab[(a \in \Sigma \wedge b \in \Sigma) \rightarrow (a \wedge b \in \Sigma)]$
- Closed under union: If a and b are in Σ then $a \vee b$ must also be in Σ.
- $\forall ab[(a \in \Sigma \wedge b \in \Sigma) \rightarrow (a \vee b \in \Sigma)]$

If both of these are true, then the following is also true:

- Closed under complement: If a is in Σ then $s \backslash a$ must also be in Σ

We also require that the null set (and therefore the original set, null's complement) is part of the algebra.

Chapter 26

The axiom of extensionality

26.1 Introduction

26.1.1 Axiom of extensionality

If two sets contain the same elements, they are equal.

$\forall x \forall y [\forall z (z \in x \leftrightarrow z \in y) \rightarrow x = y]$

This is an axiom, not a definition, because equality was defined as part of first-order logic.

Note that this is not bidirectional. $x = y$ does not imply that x and y contain the same elements. This is appropriate as $\frac{1}{2} = \frac{2}{4}$ for example, even though they are written differently as sets.

Reflexivity of equality

The reflexive property is:

$\forall x (x = x)$

We can replace the instance of y with x:

$\forall x [\forall z (z \in x \leftrightarrow z \in x) \rightarrow x = x]$

We can show that the following is true:

$\forall z (z \in x \leftrightarrow z \in x)$

Therefore:

$\forall x [T \rightarrow x = x]$

$x = x$

Symmetry of equality

The symmetry property is:

$\forall x \forall y[(x = y) \leftrightarrow (y = x)]$

We know that the following are true:

$\forall x \forall y[\forall z(z \in x \leftrightarrow z \in y) \rightarrow x = y]$

$\forall x \forall y[\forall z(z \in x \leftrightarrow z \in y) \rightarrow y = x]$

So:

$\forall x \forall y[\forall z(z \in x \leftrightarrow z \in y) \rightarrow (x = y \wedge y = x)]$

Transitivity of equality

The transitive property is:

$\forall x \forall y \forall z[(x = y \wedge y = z) \rightarrow x = z]$

Substitution for functions

The substitutive property for functions is:

$\forall x \forall y[(x = y) \rightarrow (f(x) = f(y))]$

Substitution for formulae

The substitutive property for formulae is:

$\forall x \forall y[((x = y) \wedge P(x)) \rightarrow P(y)]$

Doesn't this require iterating over predicates? Is this possible in first order logic??

Result 1: The empty set is unique

We can now show the empty set is unique.

Result 2: Every element of a set exists

If an element did not exist, the set containing it would be equal to a set which did not contain that element.

Result 3: Sets are unique

26.1.2 Equivalence classes

We have already ready defined the relationship equality, between terms.

$a = b$.

Sometimes we may wish to talk about a collection of terms which are all equal to each other. This is an equivalence class.

Though we have not yet defined them, integers are example of this. For example -1 can be written as $0-1$, $1-2$ and so on.

$\forall y \forall x x = y \rightarrow x \in z$

For all sets, we can call the class of all sets equal to the set an equivalence class.

This does not necessarily exist.

Chapter 27

Axiom of adjunction

27.0.1 Introduction

Chapter 28

Algebra of cardinality

28.1 Other

28.1.1 Cardinality

Cardinality of cartesian product

What about the cardinality of Cartesian products? So if we have sets:

$\{1,2,3\}$

$\{a,b\}$

We can have the Cartesian product set:

$\{(1,a),(2,a),(3,a),(1,b),(2,b),(3,b)\}$

We can see that:

$|A.B|=|A|.|B|$

Cardinality of union and intersection

$|A\lor B|=|A|+|B|-|A\land B|$

Cardinality of powerset

$|P(s)|=2^{|s|}$

Cardinality of complement

$|a\setminus b|=|a|-|a\land b|$

Cardinality of even/odd natural numbers

What about the cardinality of even numbers? Well, we can define a bijective function between each:

$f(n) = 2n$

Similarly for odd numbers:

$f(n) = 2n + 1$

So these both have cardinality $\aleph_0$.

Chapter 29

Orderings on sets and ordinal numbers

29.1 Introduction

29.1.1 Introduction

Part VII

Zermelo-Fraenkel set theory (ZF)

Chapter 30

Zermelo–Fraenkel set theory

30.1 Natural numbers

30.1.1 Axiom of infinity

The axiom of infinity states that:

$\exists I(\varnothing \in I \land \forall x \in I((x \lor \{x\}) \in I))$

There exists a set, called the infinite set. This contains the empty set, and for all elements in I the set also contains the successor to it.

Sequential function

Let's define the sequential function:

$s(n) := \{n \lor \{n\}\}$

We can now rewrite the axiom of infinity as:

$\exists \mathbb{N}(\varnothing \in \mathbb{N} \land \forall x \in \mathbb{N}(s(x) \in \mathbb{N}))$

Zero

This set contains the null set: $\varnothing \in \mathbb{N}$.

Zero is defined as the empty set.

$0 := \{\}$

Natural numbers

For all elements in the infinite set, there also exists another element in the infinite set: $\forall x \in \mathbb{N}((x \vee \{x\}) \in \mathbb{N})$.

We then define all sequential numbers as the set of all preceding numbers. So:

$1 := \{0\} = \{\{\}\}$

$2 := \{0, 1\} = \{\{\}, \{\{\}\}\}$

$3 := \{0, 1, 2\} = \{\{\}, \{\{\}\}, \{\{\}, \{\{\}\}\}\}$

Existence of natural numbers

Does each natural number exist? We know the infinite set exists, and we also know the axiom schema of specification:

Point is: For each set, all finite subsets exist. PROVE ELSEWHERE

From infinite set to natural set

We don't know I is limited to natural numbers. Could contain urelements etc.

More

Infinite set axiom written using N. should be I

I could be superset of N, for example set of all natural numbers, and also the set containing the set containing 2.

Can extract N using axiom of specification

We need a way to define the set of natural numbers:

$\forall n(n \in \mathbb{N} \leftrightarrow ([n = \emptyset \vee \exists k(n = k \vee \{k\})]\wedge))$

If we can can define N, we can show it exists from specicication

$\forall x \exists s[P(x) \leftrightarrow (x \in s)]$

$\forall n \exists s[n \in N \leftrightarrow (n \in s)]$

30.1.2 Cardinality of the natural numbers

Consider the infinite set, that is the set of all natural numbers which is defined in ZFC. Clearly there isn't a natural number cardinality of this – we instead write $\aleph_0$.

We call sets with this cardinality, countably infinite.

So:

$|\mathbb{N}| = \aleph_0$

Cardinality of natural numbers

We define:

$|\emptyset| = 0$

That, the empty set has a cardinality of 0.

As we define 0 as the empty set, $|0| = 0$.

What is 1? using the definition above we know $|1| > |0|$, so let's say $|1| = 1$, and more generally:

$\forall n \in \mathbb{N} |n| = n$

30.1.3 Ordering

Ordering of the natural numbers

For natural numbers we can say that number n preceeds number $s(n)$. That is:

$n \leq s(n)$

Similarly:

$s(n) \leq s(s(n))$

From the transitive property we know that:

$n \leq s(s(n))$

We can continue this to get:

$n \leq s(s(...s(n)..))$

What can we say about an arbitary comparison?

$a \leq b$

We know that either:

- $a = b$
- $b = s(s(...s(a)...))$
- $a = s(s(...s(b)...))$

In the first case the relation holds.

In the second case the relation holds.

In the third case the relation does not hold, but antisymmetry holds.

As this is is then defined on any pair, the order on natural numbers is total.

As there is a minimum, 0, the relation is also well-ordered.

However if this does not hold then the following instead holds:

30.2 Subsets and powersets

30.2.1 Subset relation

Subset

If all terms which are members of term x are also members of term y, then x is a subset of y.

$\forall x \forall y[(\forall z(z \in x \rightarrow z \in y)) \leftrightarrow (x \subseteq y)]$

Proper subset

If two sets are equal, then each is a subset of the other. A proper subset is one which is a subset, and not equal to the other set.

$\forall x \forall y[((\forall z(z \in x \rightarrow z \in y))) \wedge (x \neq y) \leftrightarrow (x \subset y)]$

30.2.2 Powerset function

The power set of s, $P(s)$, contains all subsets of s.

$\forall x x \subseteq s \leftrightarrow x \in P(x)$

Do all subsets exist?? show elsewhere.

30.2.3 Cantors theorem

The cardinality of the powerset is strictly greater than the cardinality of the underlying set.

That is, $|P(s)| < |s|$.

This applies to finite sets and infinite sets. In particular, this means that the powerset of the natural numbers is bigger than the natural numbers.

Proof

If one set is at least as big as another, then then is a surjection from that set to the other.

That is, if we can prove that there is no surjection from a set to its powerset, then we have proved the theorem.

We consider $f(s)$. If there is a surjection, then for every subset of s there should be a mapping from s to that subset.

We take set s and have the powerset of this, $P(s)$.

Consider the set:

$A = \{x \in s | x \notin f(x)\}$

That is, the set of all elements of s which do not map to the surjection.

30.3 Tuples

30.3.1 Tuples

We can get a list of sets in an order. A 2-tuple is an ordered pair:

(a, b)

We can write an ordered pair of a and b as:

$\{\{a\}, \{a, b\}\}$

Ordred pair definition, and tuple

$(a, b) = (c, d) \leftrightarrow (a = c \land b = d)$

This is the characteristic property.

30.3.2 Axiom of pairing

For any pair of sets, x and y there is another set z which containing only x and y.

$\forall x \forall y \exists z \forall a[a \in z \leftrightarrow a = x \lor a = y]$

For each set, there exists a set containing only that set

Take the axiom, but replace all instance of y with x.

$\forall x \exists z \forall a[a \in z \leftrightarrow a = x \lor a = x]$

$\forall x \exists z \forall a[a \in z \leftrightarrow a = x]$

For any finite number of sets, there is a set containing only those sets

For any finite number of sets, there is a set containing the intersection of those sets

30.3.3 Cartesian product

The cartesian product takes two sets, and creates a set containing all ordered pairs of a and b.

$a \times b$

30.3.4 Direct sums

30.4 Functions

30.4.1 Constructing functions

Use of ordered pairs

We can define this as a set of ordered pairs.

$\{\{a\}, \{a, b\}\}$

30.4.2 Domains and ranges

Domain

All values on which the function can be called

$\forall x(f(x) = y) \rightarrow P(y))$

Image

$\forall x((\exists y f(x) = y) \rightarrow P(y))$

Outputs of a function.

AKA: Range

The image of x is $f(x)$.

Preimage

The preimage of y is all x where $f(x) = y$.

Codomain

Sometimes the image is a subset of another set. For example a function may map onto natural numbers above 0. Natural numbers above 0 would be the image, and the natural numbers would be the codomain.

Example

$f(n) = s(n)$

Domain is: $\mathbb{N}$

Codomain is also: $\mathbb{N}$

Image is $\mathbb{N} \wedge n \neq 0$

Describing functions

If function f maps from set X to set Y we can write this as:

$f : X \to Y$

30.4.3 Axiom of regularity

The axiom of regularity states that:

$\forall x[x \neq \varnothing \to \exists y \in x(y \land x) = \varnothing]$

That is, for all non-empty sets, there is an element of the set which is disjoint from the set itself.

This means that no set can be a member of itself.

Chapter 31

Axiom of union

31.1 Axiom of union

31.1.1 Axiom of union

Motivation

While we have described various sets, we have not said that they exist. That is, if A and B both exist, then currently we cannot ensure $A \wedge B$ exists, just that it can be described.

The axiom of union enables us to ensure all sets from unions and intersections exist.

Axiom of union

$\forall a \exists b \forall c[c \in b \leftrightarrow \exists d(c \in d \wedge d \in a)]$

That is, for every set a, there exists a set b where all the elements in b are the elements of the elements in a.

Here, b is the union of the sets in a.

Part VIII

Computable functions

Chapter 32

The halting problem

Chapter 33

Effective procedures

Chapter 34

Proof theory

Chapter 35

Model theory

Chapter 36

The Entscheidungsproblem

Chapter 37

Kleene's s-m-n Theorem

37.0.1 Introduction

Chapter 38

Primative recursive functions

38.1 Introduction

38.1.1 Introduction

Functions which can be computed where all loops are of known length in advance. Eg for loops.

Chapter 39

Computable functions

Chapter 40

General recursive functions

Chapter 41

The Ackermann function

41.1 Introduction

41.1.1 Introduction

Not primative recursive.

$A(0, n) = n + 1$

$A(m + 1, 0) = A(m, 1)$

$A(m + 1, n + 1) = A(m, A(m + 1, n))$

Part IX

Lambda calculus and combinatory logic

Chapter 42

The Lambda calculus

42.1 Introduction

42.1.1 Lambda calculus reduction strategy for rewriting

42.1.2 Logic using the Lambda calculus

lambda negation. lambda true false.

42.1.3 Representing natural number arithmetic using the lambda calculus

lambda numerals. lambda addition.

42.1.4 Branching using the lambda calculus

if else.

42.1.5 Partial functions and currying

partial functions (take a function and fix some parameters, creates function with lower dimensions. Has uses). currying.

42.1.6 The Y combinator

42.1.7 Simply typed Lambda calculus

Chapter 43

Church encoding and Church numerals

43.1 Introduction

43.1.1 Church numerals

Chapter 44

Combinatory logic

44.1 Introduction

44.1.1 Introduction

The combinatory logic is related to the Lambda calculus, but there are no free variables.