1 Elementary Set Theory

Notation:

$\{\}$ enclose a set.

$\{1, 2, 3\} = \{3, 2, 2, 1, 3\}$ because a set is not defined by order or multiplicity.

$\{0, 2, 4, \ldots\} = \{x|x \text{ is an even natural number}\}$ because two ways of writing a set are equivalent.

$\emptyset$ is the empty set.

$x \in A$ denotes x is an element of A.

$\mathbb{N} = \{0, 1, 2, \ldots\}$ are the natural numbers.

$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ are the integers.

$\mathbb{Q} = \{\frac{m}{n}|m, n \in \mathbb{Z} \text{ and } n \neq 0\}$ are the rational numbers.

$\mathbb{R}$ are the real numbers.

Axiom 1.1. *Axiom of Extensionality Let A, B be sets. If $(\forall x) x \in A$ iff $x \in B$ then $A = B$.*

Definition 1.1 (Subset)**.** *Let A, B be sets. Then A is a subset of B, written $A \subseteq B$ iff $(\forall x)$ if $x \in A$ then $x \in B$.*

Theorem 1.1. *If $A \subseteq B$ and $B \subseteq A$ then $A = B$.*

Proof. Let x be arbitrary.

Because $A \subseteq B$ if $x \in A$ then $x \in B$

Because $B \subseteq A$ if $x \in B$ then $x \in A$

Hence, $x \in A$ iff $x \in B$, thus $A = B$. □

Definition 1.2 (Union)**.** *Let A, B be sets. The Union $A \cup B$ of A and B is defined by $x \in A \cup B$ if $x \in A$ or $x \in B$.*

Theorem 1.2. $A \cup (B \cup C) = (A \cup B) \cup C$

Proof. Let x be arbitrary.

$x \in A \cup (B \cup C)$ iff $x \in A$ or $x \in B \cup C$

iff $x \in A$ or $(x \in B$ or $x \in C)$

iff $x \in A$ or $x \in B$ or $x \in C$

iff $(x \in A$ or $x \in B)$ or $x \in C$

iff $x \in A \cup B$ or $x \in C$

iff $x \in (A \cup B) \cup C$ □

Definition 1.3 (Intersection)**.** *Let A, B be sets. The intersection $A \cap B$ of A and B is defined by $a \in A \cap B$ iff $x \in A$ and $x \in B$*

Theorem 1.3. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

Proof. Let x be arbitrary. Then $x \in A \cap (B \cup C)$ iff $x \in A$ and $x \in B \cap C$

iff $x \in A$ and $(x \in B$ or $x \in C)$

iff $(x \in A$ and $x \in B)$ or $(x \in A$ and $x \in C)$

iff $x \in A \cap B$ or $x \in A \cap C$

iff $x \in (A \cap B) \cup (A \cap C)$ □

Definition 1.4 (Set Theoretic Difference)**.** *Let A, B be sets. The set theoretic difference $A \setminus B$ is defined by $x \in A \setminus B$ iff $x \in A$ and $x \notin B$.*

Theorem 1.4. $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$

Proof. Let x be arbitrary.
Then $x \in A \setminus (B \cup C)$ iff $x \in A$ and $x \notin B \cup C$
iff $x \in A$ and not ($x \in B$ or $x \in C$)
iff $x \in A$ and ($x \notin B$ and $x \not inC$)
iff $x \in A$ and $x \notin B$ and $x \not inC$
iff $x \in A$ and $x \notin B$ and $x \in A$ and $x \not inC$
iff $x \in (A \setminus B)$ and $x \in (A \setminus C)$
iff $x \in (A \setminus B) \cap (A \setminus C)$ □

Provisional definition of function: Let A, B be sets. Then f is a function from A to B written $f : A \to B$ if f assigns a unique element $b \in B$ to each $a \in A$.

But what is the meaning of "assign"?

Basic idea is to consider $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$. We shall identify f with its graph. To generalize this to arbitrary sets A and B we first need the concept of an ordered pair. IE, a mathematical object $\langle a, b\rangle$ satisfying

$\langle a, b\rangle = \langle c, d\rangle$ iff $a = c$ and $b = d$. In particular, $\langle 1, 2\rangle \neq \{1, 2\}$.

Definition 1.5 (Cartesian Product)**.** *If A, B are sets, then their Cartesian Product $A \times B = \{\langle a, b\rangle \,|a \in A, b \in B\}$*

Definition 1.6 (Function)**.** *f is a function from A to B iff $f \subseteq A \times B$ and for each $a \in A$, there exists a unique $b \in B$ such that $\langle a, b\rangle \in f$.*

In this case, the unique value b is called the value of f at a, and we write $f(a) = b$.

It only remains to define $\langle a, b\rangle$ in terms of set theory.

Definition 1.7 (Ordered Pair)**.** $\langle a, b\rangle = \{\{a\}, \{a, b\}\}$

Theorem 1.5. *$\langle a, b\rangle = \langle c, d\rangle$ iff $a = c$ and $b = d$.*

Proof. Clearly if $a = c$ and $b = d$ then $\langle a, b\rangle = \{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\} = \langle c, d\rangle$

1. Suppose $a = b$. Then $\{\{a\}, \{a, b\}\} = \{\{a\}, \{a, a\}\} = \{\{a\}, \{a\}\} = \{\{a\}\}$

   Since $\{\{a\}\} = \{\{c\}, \{c, d\}\}$ we must have $\{a\} = \{c\}$ and $\{a\} = \{c, d\}$. So $a = c = d$, in particular, $a = c$ and $b = d$.

2. Suppose $c = d$. Then similarly $a = b = c$ so $a = c$ and $b = d$.

3. Suppose $a \neq b$ and $c \neq d$.

   Since $\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$ we must have $\{a\} = \{c\}$ or $\{a\} = \{c, d\}$. The latter is clearly impossible, so $a = c$.

   Similarly, $\{a, b\} = \{c, d\}$ or $\{a, b\} = \{c\}$. The latter is clearly impossible, and as $a = c$, then $b = d$.

$\square$

NB (Note Bene) - It is almost never necessary in a mathematical proof to remember that a function is literally a set of ordered pairs.

Definition 1.8 (Injection)**.** *The function $f : A \to B$ is an injection iff* $(\forall a, a' \in A)$ *if $a \neq a'$ then $f(a) \neq f(a')$*

Definition 1.9 (Surjection)**.** *The function $f : A \to B$ is a surjection iff* $(\forall b \in B)(\exists a \in A)$ *such that $f(a) = b$*

Definition 1.10 (Composition)**.** *If $f : A \to B$ and $g : B \to C$ are functions, then their composition $g \circ f : A \to C$ is dined by* $(g \circ f)(x) = g(f(x))$

Theorem 1.6. *If $f : A \to B$ and $g : B \to C$ are surjections, then $g \circ f : A \to C$ is also a surjection.*

Proof. Let $c \in C$ be arbitrary.
Since g is surjective, $\exists b \in B$ such that $g(b) = c$.
Since f is surjective, $\exists a \in A$ such that $g(a) = b$.
Then, $(g \circ f)(a) = g(f(a)) = c$, hence $g \circ f$ is a surjection. $\square$

Definition 1.11 (Bijection)**.** *A function $f : A \to B$ is a bijection if f is an injection and a surjection.*

Theorem 1.7. *If $f : A \to B$ and $g : B \to C$ are bijections, then $g \circ f : A \to C$ is a bijection.*

Proof. Composition of surjections is a surjection, and compositions of injections are injections. $\square$

Definition 1.12 (Inverse Function)**.** *If $f : A \to B$ is a bijection, then its inverse, $f^{-1} : B \to A$ is defined by $f^{-1}(b)$ = the unique $a \in A$ such that $f(a) = b$.*

Remarks - If $f : A \to B$ is a bijection, it is easily checked that $f^{-1} : B \to A$ is a bijection.
In terms of ordered pairs, $f^{-1} = \{\langle b, a\rangle : \langle a, b\rangle \in f\}$

Definition 1.13 (Equinumerous)**.** *Two sets, A and B, are equinumerous, written $A \sim B$ iff there exists a bijection $f : A \to B$.*

Theorem 1.8 (Galileo)**.** *Let $\mathbb{E} = \{0, 2, 4, \ldots\}$ be the even natural numbers. Then, $\mathbb{N} \sim \mathbb{E}$*

Proof. We can define a bijection $f : \mathbb{N} \to \mathbb{E}$ by $f(n) = 2n$ $\square$

Remark 1.1. *If is often extremely difficult to explicitly define a bijection $f : \mathbb{N} \to A$. However, suppose that $f : \mathbb{N} \to A$ is a bijection. For each $n \in \mathbb{N}$ let a_n be $f(n)$. Then, $a_0, a_1, \ldots$ is a list of the elements of A such that every element occurs exactly once, and conversely, if such a list exists, then we can define a bijection $f : \mathbb{N} \to A$ by $f(n) = a_n$*

Theorem 1.9. $\mathbb{N} \sim \mathbb{Z}$

Proof. We can list the elements of $\mathbb{Z}$: $0, 1, -1, 2, -2, \dots$ $\square$

Theorem 1.10. $\mathbb{N} \sim \mathbb{Q}$

Proof. We proceed in two steps.

First, we prove that $\mathbb{N} \sim \mathbb{Q}^+ = \{q \in \mathbb{Q} : q > 0\}$ and consider the following infinite matrix

$$\begin{array}{ccc} \frac{1}{1} \rightarrow & \frac{2}{1} & \frac{3}{1} \rightarrow \\ \frac{2}{1} \swarrow & \frac{2}{2} \nearrow & \frac{3}{2} \swarrow \\ \downarrow \frac{1}{3} \nearrow & \frac{2}{3} \swarrow & \frac{3}{3} \end{array}$$

Proceed through the matrix along the indicated route adding rational numbers to your list if they have not already occurred.

Second, we declare that $\mathbb{N} \sim \mathbb{Q}$. In the first part, we showed that there exists a bijection $f : \mathbb{N} \to \mathbb{Q}^+$ hence we can list $\mathbb{Q}$ by $0, f(1), -f(1), \dots$. $\square$

Definition 1.14 (Power Set). *If A is any set, then its power set is $\mathscr{P}(A) = \{B : B \subseteq A\}$, so $\mathscr{P}(\{1, 2, \dots, n\})$is of size 2^n.*

Theorem 1.11 (Cantor). $\mathbb{N} \not\sim \mathscr{P}(\mathbb{N})$

Proof. This method of proof is called the diagonal argument.

We must show that there does not exist a bijection $f : \mathbb{N} \to \mathscr{P}(\mathbb{N})$.

Let $f : \mathbb{N} \to \mathscr{P}(\mathbb{N})$ be any function.

So, we shall prove that f is not a surjection. Hence, we must find a set $S \subseteq \mathbb{N}$ such that $\forall n \in \mathbb{N} \quad f(n) \neq S$.

We do this via a "time and motion study"

For each $n \in \mathbb{N}$ we must make the n^{th} decision. That is, if $n \in S$.

We perform the n^{th} task, that is, ensure $f(n) \neq S$.

We make the n^{th} decision so that it accomplishes the n^{th} task, ie, $n \in S$ iff $n \notin f(n)$.

Clearly, $f(n)$ and S will differ on whether they contain n, thus, $\forall n \in \mathbb{N} \quad f(n) \neq S$, and so f is not a surjection. $\square$

In general, unattributed Theorems are due to Cantor.

Theorem 1.12. *If A is any set, then $A \not\sim \mathscr{P}(A)$*

Proof. Suppose that $f : A \to \mathscr{P}(A)$ is any function. Consider the set $S = \{a \in A : a \notin f(a)\}$.

Then, $a \in S$ iff $a \notin f(a)$, so $f(a) = S$. Hence, f is not a surjection. $\square$

Definition 1.15 ($\preceq$). *Let A and B be sets.*

$A \preceq B$ iff there exists an injection $f : A \to B$.

$A \prec B$ iff $A \preceq B$ and $A \not\sim B$

Theorem 1.13. *For any set A, $A \prec \mathscr{P}(A)$*

Proof. We can define an injection $f : A \to \mathscr{P}(A)$ by $f(a) = \{a\}$.

Thus, $A \preceq \mathscr{P}(A)$

By Cantor's Theorem, $A \not\sim \mathscr{P}(A)$, thus $A \prec \mathscr{P}(A)$. $\square$

Corollary 1.14. $\mathbb{N} \prec \mathscr{P}(\mathbb{N}) \prec \mathscr{P}(\mathscr{P}(\mathbb{N})) \prec \dots$

Definition 1.16 (Countable)**.** *A set A is countable iff either A is finite or $A \sim \mathbb{N}$. Otherwise, A is uncountable.*

Theorem 1.15. *Let A, B, C be sets.*

1. $A \sim A$
2. $A \sim B \Rightarrow B \sim A$
3. $A \sim B$ *and* $B \sim C \Rightarrow A \sim C$

Proof.
1. Let $id_A : A \to A$ be the function defined by $id_A(a) = a$. Clearly, id_A is a bijection, so $A \sim A$
2. Suppose $A\ B$. Then there exists a bijection $f : A \to B$. Since $f^{-1} : B \to A$ is also a bijection, $B \sim A$
3. Suppose that $A \sim B$ and $B \sim C$. Then, there exist bijections $f : A \to B$ and $g : B \to C$. As f, g are bijections, $g \circ f : A \to C$ is also a bijection, so $A \sim C$

□

Theorem 1.16 (Cantor-Bernstein)**.** *If $A \preceq B$ and $B \preceq A$ then $A \sim B$.*

The proof will be delayed.

Theorem 1.17 (Zarmelo)**.** *If A, B are any sets, then either $A \preceq B$ or $B \preceq A$.*

This proof will be omitted, though the theorem is equivalent to the axiom of choice.

Axiom 1.2 (Axiom of Choice)**.** *Suppose $\mathfrak{F}$ is a set of nonempty sets. Then there exists a function f such that $f(A) \in A$ for each $A \in \mathfrak{F}$. We say that f is a choice function for $\mathfrak{F}$*

Theorem 1.18. $\mathbb{N} \sim \mathbb{Q}$

Proof. We can define an injection $f : \mathbb{N} \to \mathbb{Q}$ by $f(n) = n$. Hence, $\mathbb{N} \preceq \mathbb{Q}$

We next define $g : \mathbb{Q} \to \mathbb{N}$ as follows:

If $0 \neq q \in \mathbb{Q}$, we can uniquely express $q = \frac{\epsilon a}{b}$ where $\epsilon = \pm 1$ and $(a, b) = 1$, and $a, b > 0$.

So, $g(q) = 2^{\epsilon+1} 3^a 5^b$. We also define $g(0) = 0$.

Clearly, g is an injection, so $\mathbb{Q} \preceq \mathbb{N}$

Thus, by the Cantor-Bernstein Theorem, $\mathbb{N} \sim \mathbb{Q}$ □

Lemma 1.19. $(0, 1) \sim \mathbb{R}$

Proof. From elementary claculus, we can define a bijection $f : (0, 1) \to \mathbb{R}$ by $f(x) = \tan(\pi x - \frac{\pi}{2})$ □

Theorem 1.20. $\mathbb{R} \sim \mathscr{P}(\mathbb{N})$

Proof. By the lemma, it is eanough to show that $(0,1) \sim \mathscr{P}(\mathbb{N})$.

We make use of the fact that each $r \in (0,1)$ has a unique decimal expansion $r = 0.r_1r_2\ldots$ such that $0 \leq r_n < 9$ and the expansion doesn't end in an infinite string of nines. (this is to avoid two expansions such as $0.500\ldots = 0.4999\ldots$)

First we define a function $f : (0,1) \to \mathscr{P}(\mathbb{N})$ as follows. Suppose that $r = 0.r_0r_1r_2\ldots$. Let $p_0, p_1, \ldots$ be the primes in increasing order. Then $f(r) = \{p_0^{r_0+1}, p_1^{r_1+1}, \ldots\}$. Clearly, f is an injection, hence $(0,1) \preceq \mathscr{P}(\mathbb{N})$

Next, we define a function $g : \mathscr{P}(\mathbb{N}) \to (0,1)$ as followes: If $S \subset \mathbb{N}$ then $g(S) = 0.S_0S_1S_2\ldots$ where $S_n = 7$ if $n \in S$ and $S_n = 5$ if $n \notin S$ (note, 7 and 5 are arbitrarily chosen), hence $\mathscr{P}(\mathbb{N}) \preceq (0,1)$

By the Cantor-Bernstein Theorem, $(0,1) \sim \mathscr{P}(\mathbb{N})$, hence $\mathbb{R} \sim \mathscr{P}(\mathbb{N})$ $\square$

Theorem 1.21. *If $S \subseteq \mathbb{N}$ then either S is finite or $S \sim \mathbb{N}$. That is, $\mathbb{N}$ has the least infinite size.*

Proof. Suppose $S \subset \mathbb{N}$ is infinite. Let $S_0, S_1, S_2, \ldots$ be the increasing enumeration of S. This list witnesses that $\mathbb{N} \sim S$ $\square$

Hypothesis 1.1 (Continuum Hypothesis). *If $X \subseteq \mathbb{R}$, then either X is countable or $X \sim \mathbb{R}$*

Theorem 1.22 (Gödel and Cohen). *If the axioms of set theory are consistent, then it is impossible to prove or disprove the Continuum Hypothesis from these axioms.*

Definition 1.17 (Set of Finite Subsets). $\mathrm{Fin}(\mathbb{N})$ *is the set of finite subsets of* $\mathbb{N}$.

Clearly, $\mathbb{N} \preceq \mathrm{Fin}(\mathbb{N}) \preceq \mathscr{P}(\mathbb{N})$

Theorem 1.23. $\mathbb{N} \sim \mathrm{Fin}(\mathbb{N})$

Proof. We can define an injection $f : \mathbb{N} \to \mathrm{Fin}(\mathbb{N})$ by $f(n) = \{n\}$.

Next, we can define $g : \mathrm{Fin}(\mathbb{N}) \to \mathbb{N}$ as follows.

Suppose that $S = \{s_0, s_1, \ldots, s_n\} \neq \emptyset$, where $s_0 < s_1 < \ldots < s_n$. Then $g(S) = p_0^{s_0+1} \ldots p_n^{s_n+1}$, with $p_0, \ldots, p_n$ being the primes in increasing order, and also $g(\emptyset) = 0$. Clearly, g is an injection, so $\mathrm{Fin}(\mathbb{N}) \preceq \mathbb{N}$

By Cantor-Bernstein, $\mathrm{Fin}(\mathbb{N}) \sim \mathbb{N}$ $\square$

Definition 1.18 (The set of functions between sets). *If A, B are sets, then* ${}^{A}{}_{B} = \{f | f : A \to B\}$

Theorem 1.24. ${}^{\mathbb{N}}{}_{\mathbb{N}} \sim \mathscr{P}(\mathbb{N})$

Proof. We first define a function $g : \mathscr{P}(\mathbb{N}) \to {}^{\mathbb{N}}{}_{\mathbb{N}}$ as follows:

For each subset of $\mathbb{N}$, the characteristic function is $\chi(x) : \mathbb{N} \to \{0,1\}$ defined by $\chi_S(n) = 1$ if $n \in S$ and $\chi_S(n) = 0$ if $n \notin S$. The set $g(S) = \chi_S \in {}^{\mathbb{N}}{}_{\mathbb{N}}$.

Clearly, g is an injection, and so $\mathscr{P}(\mathbb{N}) \preceq {}^{\mathbb{N}}{}_{\mathbb{N}}$

Next we define $\pi : {}^{\mathbb{N}}\mathbb{N} \to \mathscr{P}(\mathbb{N})$ by $\pi(f) = \{p_0^{f(0)+1}, \ldots, p_n^{f(n)+1}, \ldots\}$, where $p_0, p_1, \ldots$ are the primes in increasing order.

Clearly, π is an injection.

Hence, ${}^{\mathbb{N}}\mathbb{N} \preceq \mathscr{P}(\mathbb{N})$.

So, by Cantor-Bernstein, ${}^{\mathbb{N}}\mathbb{N} \sim \mathscr{P}(\mathbb{N})$ □

And now, a heuristic principle. If S is an infinite set, then, in general, if each $s \in S$ is determined by finitely many pieces of data, then S is countable, and if each $s \in S$ is determined by infinitely many independent pieces of data, then S is countable.

Definition 1.19 (EC($\mathbb{N}$))**.** EC($\mathbb{N}$) *is the set of eventually constant functions* $f : \mathbb{N} \to \mathbb{N}$*, ie, functions* f *such that there exist* $a, b \in \mathbb{N}$ *such that* $f(n) = b \quad \forall n \geq a$

Theorem 1.25. $\mathbb{N} \sim \mathrm{EC}(\mathbb{N})$

Proof. First, we define a mat $f : \mathbb{N} \to \mathrm{EC}(\mathbb{N})$ by $f(n) = c_n$, where $c_n(t) = n \quad \forall t \in \mathbb{N}$.

Clearly, f is an injection, so $\mathbb{N} \preceq \mathrm{EC}(\mathbb{N})$.

Next, we define a map $\pi : \mathrm{EC}(\mathbb{N}) \to \mathbb{N}$ by $\pi(g) = p_0^{f(0)+1} \ldots p_a^{f(a)+1}$, where a is the least integer such that $f(t) = f(a) \quad \forall t \geq a$. Clearly, π is an injection, so $\mathrm{EC}(\mathbb{N}) \preceq \mathbb{N}$

Thus, by Cantor-Bernstein, $\mathbb{N} \sim \mathrm{EC}(\mathbb{N})$ □

We are almost ready to prove the Cantor-Bernstein Theorem. First, we will require a definition and a lemma.

Definition 1.20 (Image of Z)**.** *If* $f : X \to Y$ *and* $Z \subseteq X$*, then* $f[Z] = \{f(z) : z \in Z\}$ *is the image of* Z*.*

Lemma 1.26. *If* $f : A \to B$ *is an injection and* $C \subseteq A$*, then* $f[A \setminus C] = f[A] \setminus f[C]$

Proof. First suppose $x \in f[A \setminus C]$. Then, $\exists a \in A \setminus C$ such that $f(a) = x$. Hence, $x \in f[A]$.

Suppose $x \in f[C]$. Then, $\exists c \in C$ such that $f(c) = x$. As $a \neq c$, this contradicts f being an injection, thus $x \in f[A] \setminus f[C]$

Conversely, suppose $x \in f[A] \setminus f[C]$. Then $\exists a \in A$ such that $f(a) = x$.

Since $x \notin f[C]$, $a \notin C$, so $a \in A \setminus C$, therefore, $x \in f[A \setminus C]$ □

And now, the proof of the Cantor-Bernstein Theorem.

Proof. Since $A \preceq B$ and $B \preceq A$, there exist injection $f : A \to B$ and $g : B \to A$.

Let $C = g[B] = \{g(b) : b \in B\}$.

Claim 1 - $B \sim C$.

The map $b \mapsto g(b)$ is a bijection from B to C, so the claim is proved.

Thus, it is enough to show $A \sim C$, because then $A \sim C$ and $C \sim B$, so $A \sim B$

Let $h = g \circ f : A \to A$, then h is an injection.

Define by induction on $n \geq 0$ $A_0 = A4$, $A_{n+1} = h[A_n]$ and $C_0 = C$, $C_{n+1} = h[C_n]$.

Define a function $k : A \to C$ by $k(x) = h(x)$ if $x \in A_n \setminus C_n$ for some n and $k(x) = x$ otherwise.

Claim 2 - k is an injection.

Suppose that $x \neq x'$ are distinct elements of A.

There are three cases:

1. Suppose $x \in A_n \setminus C_n$, $x' \in A_m \setminus C_m$ for some n, m. Since h is an injection, $k(x) = h(x) \neq h(x') = k(x')$

2. Suppose $x, x' \notin A_n \setminus C_n \quad \forall n$. Then $k(x) = x \neq x' = k(x')$

3. Without loss of generality, suppose $x \in A_n \setminus C_n$ for some n and $x' \notin A_n \setminus C_n \quad \forall n$. Then, $k(x) = h(x) \in h[A_n \setminus C_n] = h[A_n] \setminus h[C_n] = A_{n+1} \setminus C_{n+1}$. Hence, $k(x) = h(x) \neq x' = k(x')$

Claim 3 - k is a surjection.

Let $c \in C$ be arbitrary. There are two cases.

1. Suppose $c \notin A_n \setminus C_n \quad \forall n$, then $k(c) = c$

2. Suppose $c \in A_n \setminus C_n$ for some n. Since $c \in C = C_0$, $\exists m$ such that $n = m+1$, since $h[A_m \setminus C_m] = h[A_m] \setminus h[C_m] = A_n \setminus C_n$. So, $\exists a \in A_m \setminus C_m$ such that $k(a) = h(a) = c$.

Therefore, k is a bijection, so $A \sim C$ $\square$

Theorem 1.27. $\mathbb{R} \sim \mathbb{R} \times \mathbb{R}$

Proof. Since $\mathbb{R} \sim (0,1)$, it is enough to prove that $(0,1) \sim (0,1) \times (0,1)$

We can define an injection $f : (0,1) \to (0,1) \times (0,1)$ such that $f(r) = \langle \frac{1}{2}, r \rangle$.

Next we define an injection $g : (0,1) \times (0,1) \to (0,1)$ as follows.

If $r = 0.r_0 r_1 \ldots r_n \ldots$ and $s = 0.s_0 s_1 \ldots s_n \ldots$, then,

$g(\langle r, s \rangle) = 0.r_0 s_0 r_1 s_1 \ldots r_n s_n \ldots$.

By the Cantor-Bernstein Theorem, $(0,1) \sim (0,1) \times (0,1)$ $\square$

Definition 1.21 (Sym($\mathbb{N}$))**.** $\text{Sym}(\mathbb{N}) = \{f \in {}^{\mathbb{N}}\mathbb{N} : f \textit{ is a bijection } \}$

Theorem 1.28. $\text{Sym}(\mathbb{N}) \sim \mathscr{P}(\mathbb{N})$

Proof. Since $\text{Sym}(\mathbb{N}) \subseteq {}^{\mathbb{N}}\mathbb{N} \sim \mathscr{P}(\mathbb{N})$, we have $\text{Sym}(\mathbb{N}) \preceq \mathscr{P}(\mathbb{N})$.

Next, we define a function $f : \mathscr{P}(\mathbb{N}) \to \text{Sym}(\mathbb{N})$ by $S \to f_S$ where $f_S(2n) = 2n+1$ and $f_S(2n+1) = 2n$ if $n \in S$ and $f_S(2n) = 2n$ and $f_S(2n+1) = 2n+1$ otherwise.

This is an injection, and so $\mathscr{P}(\mathbb{N}) \preceq \text{Sym}(\mathbb{N})$, so, by Cantor-Bernstein, $\mathscr{P}(\mathbb{N}) \sim \text{Sym}(\mathbb{N})$ $\square$

Definition 1.22 (Finite Sequence)**.** *Let A be a set. Then a finite sequence of elements of A is an inject $\langle a_0, a_1, \ldots, a_n \rangle$, with $a_i \in A$ and $n \geq 0$.*

$\langle a_0, a_1, \ldots a_n \rangle = \langle b_0, b_1, \ldots b_m \rangle$ *if and only if* $n = m$ *and* $\forall i \quad a_i = b_i$

Definition 1.23 (Finite Sequence)**.** $\langle a_0, \ldots a_n \rangle = f : \{0, \ldots, n\} \to A : f(i) = a_i$

Definition 1.24 (Finseq(A))**.** Finseq(A) *is the set of finite sequences of elemetns of A.*

Theorem 1.29. *If A is a nonempty countable set, then* $\mathbb{N} \sim \text{Finseq}(A)$

Proof. Fix some $a \in A$. Then, we can define an injection $f : \mathbb{N} \to \text{Finseq}(A)$: $n \mapsto \overbrace{\langle a, \ldots, a \rangle}^{n}$

So, $\mathbb{N} \sim \text{Finseq}(A)$

Next, we define an injection $g : \text{Finseq}(A) \to \mathbb{N}$ as follows:

Since A is countable, there exists an injection $e : A \to \mathbb{N}$. We define $\langle a_0, \ldots, a_n \rangle \mapsto 2^{e(a_0)+1} \ldots p_n^{e(a_n)+1}$, where p_i is the i^{th} prime.

Thus, $\text{Finseq}(A) \preceq \mathbb{N}$, and so, by the Cantor-Bernstein Theorem, $\mathbb{N} \sim \text{Finseq}(A)$ ☐

And now, we move on to Cardinal Arithmetic.

Definition 1.25 (Cardinality)**.** *To each set A we associate an object, its cardinality, denoted* $\text{card}(A)$ *or* $|A|$ *such that* $|A| = |B|$ *iff* $A \sim B$

Examples

1. If A is a finite set, then $|A|$ is its usual size.
2. $|\mathbb{N}| = \aleph_0$
3. The infinite cardinals begin $\aleph_0, \aleph_1, \ldots, \aleph_\omega, \aleph_{\omega+1}, \ldots$

Definition 1.26 (Cardinal Addition)**.** *Let κ, λ be cardinal numbers, then* $\kappa + \lambda = \text{card}(A \cup B)$ *where* $\text{card}(A) = \kappa$, $\text{card}(B) = \lambda$ *and* $A \cap B = \emptyset$

Theorem 1.30. *If $A \sim A'$ and $B \sim B'$ and $A \cap B = A' \cap B' = \emptyset$, then $A \cup B \sim A' \cup B'$*

Proof. Since $A \sim A'$ and $B \sim B'$, there exist bijections $f : A \to A'$ and $g : B \to B'$, then we can define a bijection $h : A \cup B \to A' \cup B'$ by $h(x) = f(x)$ if $x \in A$ and $h(x) = g(x)$ if $x \in B$. ☐

Theorem 1.31. $\aleph_0 + \aleph_0 = \aleph_0$

Proof. Let $\mathbb{E}$ be the even natural numbers and $\mathbb{O}$ be the odd natural numbers. So $\aleph_0 + \aleph_0 = \text{card}(\mathbb{E} \cup \mathbb{O}) = \text{card}\, \mathbb{N} = \aleph_0$ ☐

In fact, if κ, λ are cardinal numbers, at least one of which is infinite, then $\kappa + \lambda = \max\{\kappa, \lambda\}$

And it is clearly impossible to sensibly define an operation of cardinal subtraction.

Definition 1.27 (Cardinal Multiplication)**.** *Let λ, κ be cardinals. Then $\lambda\kappa = \mathrm{card}(A \times B)$ when $|A| = \kappa$ and $|B| = \lambda$.*

We have already checked that this is well defined.

Theorem 1.32. $\aleph_0 \times \aleph_0 = \aleph_0$

Proof. Since $\mathbb{N} \sim \mathbb{N} \times \mathbb{N}$, we have $\aleph_0 \times \aleph_0 = \mathrm{card}(\mathbb{N} \times \mathbb{N}) = \mathrm{card}(\mathbb{N}) = \aleph_0$ □

In fact, if κ, λ are cardinals, at least one of which is infinite, and neither is zero, then $\kappa\lambda = \max\{\kappa, \lambda\}$

Definition 1.28 (Cardinal Exponentiation)**.** *If κ, λ are cardinal numbers, then $\kappa^\lambda = \mathrm{card}({}^{A}{}_{B})$ where $|A| = \lambda$ and $|B| = \kappa$.*

Theorem 1.33. $|\mathbb{R}| = 2^{\aleph_0}$

Proof. We know $\mathbb{R} \sim \mathscr{P}(\mathbb{N}) \sim {}^{\mathbb{N}}{}_{\{0,1\}}$, hence $2^{\aleph_0} = \mathrm{card}({}^{\mathbb{N}}{}_{\{0,1\}} = |\mathbb{R}|$ □

In fact, if κ is any cardinal number, then $\kappa < 2^\kappa$.

This just restates that $A \preceq \mathscr{P}(A)$

2 Relations

Definition 2.1 (Binary Relation)**.** *A binary relation on a set A is a subset $R \subseteq A \times A$. We usually write aRb instead of $\langle a, b\rangle \in R$*

Example 2.1.

1. *The order relation on $\mathbb{N}$ is $<= \{\langle n, m\rangle : n, m \in \mathbb{N}, n < m\}$*
2. *divisibility relation on $\mathbb{N}^+$ is $D = \{\langle n, m\rangle : n, m \in \mathbb{N}^+, m$ divides $n\}$*

Observation: Thus $\mathscr{P}(\mathbb{N} \times \mathbb{N})$ is the set of binary relations on $\mathbb{N}$. Since $\mathbb{N} \times \mathbb{N} \sim \mathbb{N}$, it follows that $\mathscr{P}(\mathbb{N} \times \mathbb{N}) \sim \mathscr{P}(\mathbb{N})$, in particular, $\mathscr{P}(\mathbb{N} \times \mathbb{N})$ is uncountable.

Let R be a binary relation on A.

Definition 2.2 (Reflexive Property)**.** *R is reflexive if $(\forall a \in A)aRa$*

Definition 2.3 (Symmetric Property)**.** *R is symmetric if $(\forall a, b \in A)aRb \Rightarrow bRa$*

Definition 2.4 (Transitive Property)**.** *R is transitive if $(\forall a, b, c \in A)aRb \wedge bRc \Rightarrow aRc$*

Definition 2.5 (Equivalence Relation)**.** *R is an equivalence relation iff R is reflexive, symmetric and transitive.*

Example: Consider the relation R defined on $\mathbb{Z}$ by aRb iff $3|a-b$

Theorem 2.1. *R is an equivalence relation on Z.*

Proof. Let $a \in \mathbb{Z}$, then $3|a-a=0$. Hence, aRa, thus R is reflexive.

Let $a, b \in \mathbb{Z}$. Suppose aRb, so $3|a-b$, so $3|b-a=-(a-b)$, so bRa, thus, R is symmetric.

Let $a, b, c \in \mathbb{Z}$. Suppose aRb and bRc, so $3|a-b$ and $3|b-c$, so, $3|(a-b)+(b-c)=a-c$, so aRc, and so R is transitive. □

Definition 2.6 (Equivalence Class)**.** *Let R be an equivalence relation on A. For each $x \in A$, the corresponding equivalence class is $[x]=\{y \in A : xRy\}$*

Example continued:
The equivalence classes of R above are:
$[0]=\{\ldots,-6,-3,0,3,6,\ldots\}$
$[1]=\{\ldots,-5,-2,1,4,7,\ldots\}$
$[2]=\{\ldots,-4,-1,2,5,8,\ldots\}$

Definition 2.7 (Partition)**.** *Let A be a nonempty set. Then, a partition of A is a collection $\{B_i : i \in I\}$ such that*

1. $(\forall i \in I) B_i \neq \emptyset$
2. $(\forall i, j \in I)$ *if* $i \neq j$ *then* $B_i \cap B_j = \emptyset$
3. $(\forall a \in A)(\exists i \in I)$ *such that* $a \in B_i$*. That is,* $A = \cup_{i \in I} B_i$

Theorem 2.2. *Let R be an equivalence relation on A.*

Then, $(\forall a \in A) a \in [a]$ and If $a, b \in A$ and $[a] \cap [b] \neq \emptyset$, then $[a]=[b]$. Hence, the set of equivalence classes $\{[a] : a \in A\}$ forms a partition of A.

Theorem 2.3. *Let $\{B_i : i \in I\}$ be a partition of A. Define the binary relation E on A by aEb iff $(\exists i \in I)$ such that $a, b \in B_i$. Then, E is an equivalence relation and the $E-$equivalence classes are precisely $\{B_i : i \in I\}$*

Example: How many equivalence classes are there on $\{1,2,3\}$?
Answer: There are exactly five equivalence relation, corresponding to
$\{\{1,2,3\}\}, \{\{1\},\{2,3\}\}, \{\{2\},\{1,3\}\}, \{\{3\},\{1,2\}\}, \{\{1\},\{2\},\{3\}\}$

Definition 2.8 (Irreflexive Property)**.** *R is irreflexive iff $(\forall a)\ \langle a, a\rangle \notin R$*

Definition 2.9 (Trichotomy Property)**.** *R satisfies the Trichotomy Property if $(\forall a, b \in A)$ exactly one of the following holds, $aRb, a=b, bRa$.*

Definition 2.10 (Linear Order)**.** *$\langle A, R\rangle$ is a linear order if R is irreflexive, transitive, and satisfies the trichotomy property.*

Definition 2.11 (Partial Order)**.** *Let R be a binary relation on A, then $\langle A, R\rangle$ is a partial order if R is irreflexive and transitive.*

Definition 2.12 (Isomorphism)**.** *Let $\langle A, <\rangle$ and $\langle B, \prec\rangle$ be partial orders. A map $f : A \to B$ is an isomorphism if the following conditions are satisfied:*

1. *f is a bijection*
2. *$(\forall a, b \in A) a < b$ iff $f(a) \prec f(b)$*

In this case, we say that $\langle A, <\rangle$ an $\langle B, \prec\rangle$ are isomorphic, and write $\langle A, <\rangle \cong \langle B, \prec\rangle$

Theorem 2.4. $\langle \mathbb{Z}, <\rangle \cong \langle \mathbb{Z}, >\rangle$

Proof. Define $f : \mathbb{Z} \to \mathbb{Z}$ by $f(z) = -z$, then $a < b$ iff $-a > -b$ iff $f(a) > f(b)$. Thus, f is an isomorphism □

Notation - Let D be the strict divisibility relation on $\mathbb{N}^+$. that is, $aDb \Leftrightarrow a < b \& a|b$

Theorem 2.5. $\langle \mathbb{N}^+, D\rangle \ncong \langle \mathscr{P}(\mathbb{N}), \subset\rangle$

Proof. $\mathbb{N}^+ \not\sim \mathscr{P}(\mathbb{N})$, so no bijection exists. □

Theorem 2.6. $\langle \mathbb{R} \setminus \{0\}, <\rangle \ncong \langle \mathbb{R}, <\rangle$

Proof. Suppose $f : \mathbb{R} \setminus \{0\} \to \mathbb{R}$ is an isomorphism.
For each $n \geq 1$ let $r_n = f(\frac{1}{n})$
Then, $r_1 > r_2 > \dots r_k > \dots f(-1)$
Let s be the greatest lower bound of $\{r_n : n \geq 1\}$.
$\exists t \in \mathbb{R} \setminus \{0\}$ such that $f(t) = s$
Clearly, $t < 0$, thus $\frac{t}{2} > t$
$f(\frac{t}{2}) > s$, hence $\exists n \geq 1$ such that $r_n < f(\frac{t}{2})$.
But then $\frac{t}{2} < \frac{1}{n}$ and $f(\frac{1}{n}) < f(\frac{t}{2})$, so a contradiction. □

Definition 2.13. *For each prime p, let $\mathbb{Z}[1/p] = \{\frac{a}{p^n} : a \in \mathbb{Z}, n \geq 0\}$*

Definition 2.14 (Dense Linear Order without Endpoints)**.** *A linear order $\langle D, <\rangle$ is a dense linear order without endpoints, or DLO, if the following hold:*

1. *if $a, b \in D$ and $a < b$ then $\exists c \in D$ such that $a < c < b$*
2. *if $a \in D$ then $\exists b \in D$ such that $a < b$*
3. *if $a \in D$ then $\exists c \in D$ such that $c < a$*

Theorem 2.7. *For each prime p, $\langle \mathbb{Z}[1/p], <\rangle$ is a DLO.*

Proof. Clearly $\langle \mathbb{Z}[1/p], <\rangle$ is a linear order without endpoints.
Let $a, b \in \mathbb{Z}[1/p]$ with $a < b$. Then, we can express $a = \frac{c}{p^n}$ and $b = \frac{d}{p^m}$. Adjusting c or d if necessary, we can suppose $a = \frac{c}{p^n}$ and $b = \frac{d}{p^n}$.
So then $a = \frac{c}{p^n} < \frac{c+1}{p^n} \leq \frac{d}{p^n} = b$
So, let $r = \frac{c}{p^n} + \frac{1}{p^{n+1}} = \frac{cp+1}{p^{n+1}} \in \mathbb{Z}[1/p]$
Then, $a < r < b$ □

Theorem 2.8. *If $\langle A, <\rangle$ and $\langle B, \prec\rangle$ are countable DLOs, then $\langle A, <\rangle \cong \langle B, \prec\rangle$*

Proof. This is called the Back and Forth Argument.

Let $A = \{a_n : n \in \mathbb{N}\}$ and $B = \{b_n : n \in \mathbb{N}\}$

First define $A_0 = \{a_0\}$ and $B_0 = \{b_0\}$ and $f_0 = \{\langle a_0, b_0\rangle$

Suppose inductively that we have constructed A_n, B_n, f_n such that A_n is a finite subset of A such that $a_0, \ldots, a_n \in A_n$, B_n is similarly related to B, and $f_n : A_n \to B_n$ is an order preserving bijection.

We construct $A_{n+1}, B_{n+1}, f_{n+1}$ in two steps.

1. If $a_{n+1} \in A_n$, then $A'_n = A_n$, $B'_n = B_n$ and $f'_n = f_n$.

   If $a_{n+1} \notin A_n$, then say $c_0 < c_1 < \ldots, a_{n+1} < \ldots < c_m$ where $A_n = \{c_0, \ldots, c_m\}$

   $\exists d \in B$ such that $f(c_0) < \ldots < d < \ldots < f(c_m)$, so we define $A'_n = A_n \cup \{a_{n+1}\}$, $B'_n = B_n \cup \{d\}$ and $f'_n = f_n \cup \{\langle a_{n+1}, d\rangle$

2. If $b_{n+1} \in B'_n$, then $A_{n+1} = A'_n$, $B_{n+1} = B'_n$ and $f_{n+1} = f'_n$

   Else, $d_0 < \ldots < b_{n+1} < \ldots < d_\ell$, where $B'_n = \{d_0, \ldots, d_\ell\}$.

   Then, $\exists e \in A$ such that $(f'_n)^{-1}(d_0) < \ldots < e < \ldots < (f'_n)^{-1}(d_\ell)$

   And so, we define $A_{n+1} = A'_n \cup \{e\}$, $B_{n+1} = B'_n \cup \{b_{n+1}\}$ and $f_{n+1} = f'_n \cup \{\langle e, b_{n+a}\rangle\}$

   Finally, let $f = \cup_n f_n$, then f is an order preserving bijection between A and B.

□

Corollary 2.9. *1.* $\langle \mathbb{Q}, <\rangle \cong \langle \mathbb{Q} \setminus \{0\}, <\rangle$

2. $\langle \mathbb{Z}[1/2], <\rangle \cong \langle \mathbb{Z}[1/3], <\rangle$

3. If $\langle D, <\rangle$ is a countable DLO, then $\langle D, <\rangle \cong \langle \mathbb{Q}, <\rangle$

Definition 2.15 (S extends R)**.** *Suppose R and S are binary relations on the set A. We say S extends R if $R \subseteq S$*

Theorem 2.10. *If $\langle A, \prec\rangle$ is a partial order, then there exists a binary relation $<$ extending $\prec$ such that $\langle A, <\rangle$ is a linear order.*

3 Propositional Logic

Definition 3.1 (Formal Language)**.** *We define our formal alphabet as the following symbols*

1. *The sentence connectives* $\vee, \wedge, \neg, \Rightarrow, \Leftrightarrow$

2. *The punctuation symbols* (,)

3. *The sentence symbols* $A_0, A_1, \ldots, A_n, \ldots$ *for* $n \geq 0$

Definition 3.2 (Expression)**.** *An expression is a finite sequence of symbols from the alphabet.*

Definition 3.3 (Well Formed Formulas)**.** *The set of well-formed formulas, or wffs, is defined recursively as follows*

1. *Every sentence symbol* A_n *is a wff.*
2. *If* α, β *are wffs, then* $(\alpha \wedge \beta), (\alpha \vee \beta), (\not\alpha), (\alpha \Rightarrow \beta), (\alpha \Leftrightarrow \beta)$
3. *No expression is a wff unless compelled to be so by finitely many applications of 1 and 2.*

Remark 3.1. *From now on, we will omit 3 in recursive definitions. Clearly, the set of wffs is countable, and since the definition of a wff is recursive, many of the basic properties of wffs are proved by induction.*

Example 3.1. $(A_1 \Rightarrow A_2)$ *is a wff, but* $(A_1 \Rightarrow A_2))$ *is not.*

Theorem 3.1. *If* α *is a wff, then* α *has the same number of left and right parentheses.*

Proof. We argue by induction on the length of the wff α.
If $n = 1$, then α is a sentence symbol, say, A_s. So the result holds.
Suppose $n > 1$ and the result holds for all wffs of length less than n.
Then there exist wffs β, γ such that α has one of the following forms:
$(\beta \wedge \gamma), (\beta \vee \gamma), (\neg\beta), (\beta \Rightarrow \gamma), (\beta \Leftrightarrow \gamma)$
By induction, the result holds for β and γ, hence, the result also holds for α. $\square$

Definition 3.4. $\mathscr{L}$ *is the set of sentence symbols*
$\overline{\mathscr{L}}$ *is the set of wffs.*
$\{T, F\}$ *is the set of truth values.*

Definition 3.5 (Truth Assignment)**.** *A truth assignment is a function* $\nu : \mathscr{L} \to \{T, F\}$

Definition 3.6 (Extension of ν)**.** *Let* ν *be a truth assignment. Then we define the extension* $\overline{\nu} : \overline{\mathscr{L}} \to \{T, F\}$ *recursively as follows*

1. *If* $A_n \in \mathscr{L}$*, then* $\overline{\nu}(A_n) = \nu(A_n)$
2. $\overline{\nu}\left((A_n)\right) = T$ *of* $\overline{\nu}(\alpha) = F$
   $\overline{\nu}\left((A_n)\right) = F$ *of* $\overline{\nu}(\alpha) = T$
3. $\overline{\nu}((\alpha \wedge \beta)) = T$ *if* $\overline{\nu}(\alpha) = T$ *and* $\overline{\nu}(\beta) = T$
   $\overline{\nu}((\alpha \wedge \beta)) = F$ *else.*

4. $\overline{\nu}((\alpha \vee \beta)) = F$ *if* $\overline{\nu}(\alpha) = \overline{\nu}(\beta) = F$
   $\overline{\nu}((\alpha \vee \beta)) = T$ *else.*

5. $\overline{\nu}((\alpha \Rightarrow \beta)) = F$ *if* $\overline{\nu}(\alpha) = T$ *and* $\overline{\nu}(\beta) = F$
   $\overline{\nu}((\alpha \Rightarrow \beta)) = T$ *else.*

6. $\overline{\nu}((\alpha \Leftrightarrow \beta)) = T$ *if* $\overline{\nu}(\alpha) = \overline{v}(\beta)$
   $\overline{\nu}((\alpha \Leftrightarrow \beta)) = F$ *else.*

Definition 3.7 (Proper Initial Segment). *If $\langle a_0, \ldots, a_n \rangle$ is a finite sequence, then a proper initial segment has the form $\langle a_0, \ldots, a_s \rangle$ where $0 \leq s < n$*

Lemma 3.2. *Any proper initial segment of a wff has more left than right parentheses. Thus, no proper initial segment of a wff is a wff.*

Proof. We argue by induction on the length $n \geq 1$ of the wff α.

First, suppose $n = 1$, then α is a sentence symbol, say, A_s. As A_s has no proper initial segments, the result holds vacuously.

Suppose $n > 1$, and the result holds for all wffs of length less than n.

Then, α has the form $(\beta \wedge \gamma), (\beta \vee \gamma), (\neg\gamma), (\beta \Rightarrow \gamma), (\beta \Leftrightarrow \gamma)$ for some shorter wffs β and γ.

Since all the cases are similar, we just consider the case when α is $(\beta \wedge \gamma)$.

The proper initial segments are $($,$(\beta_0$ where β_0 is a not necessarily proper initial segment of β, $(\beta\wedge$, $(\beta \wedge \gamma_0$ where γ_0 is a not necessarily proper initial segment of γ.

So, using the inductive hypothesis and the previous theorem, we see that the result also holds for α. □

Theorem 3.3 (Unique Readability Theorem). *If α is a wff of length greater than one, then there exists exactly one way of expressing α in the form $(\neg\beta), (\beta \vee \gamma), (\beta \wedge \gamma), (\beta \Rightarrow \gamma), (\beta \Leftrightarrow \gamma)$ for shorter wffs β, γ.*

Proof. Suppose α is both $(\beta \wedge \gamma)$ and $(\theta \wedge \psi)$.

Then, $(\beta \wedge \gamma) = (\theta \wedge \psi)$, and so deleting the first parenthesis, $\beta \wedge \gamma) = \theta \wedge \psi)$.

Suppose $\beta \neq \theta$, then without loss of generality, β is a proper initial segment of θ.

By the lemma, β is not a wff. This is a contradiction, so $\beta = \theta$.

Hence, deleting β, θ, we have $\wedge\gamma) = \wedge\psi)$. So $\gamma = \psi$

The other cases are similar. □

From now on, we will use common sense in writing proofs, and may omit parentheses when there is no ambiguity. These are not wffs, however, just representations of them.

Definition 3.8 (Satisfiable). *Let $\nu : \mathscr{L} \to \{T, F\}$ be a truth assignment.*

1. *If φ is a wff, then ν satisfies φ if $\overline{\nu}(\varphi) = T$.*

2. *If Σ is a set of wffs, then ν satisfies Σ if $\overline{\nu}(\sigma) = T$ for all $\sigma \in \Sigma$*

3. Σ is satisfiable if there exists a truth assignment ν which satisfies Σ.

Definition 3.9 (Tautological Implication)**.** *Let Σ be a set of wffs and φ be a wff. Then Σ tautologically implies φ, written $\Sigma \models \varphi$ iff every truth assignment which satisfies Σ also satisfies φ.*

Definition 3.10 (Tautology)**.** *φ is a tautology iff $\emptyset \models \varphi$, ie, every truth assignment satisfies φ.*

Definition 3.11 (Tautological Equivalence)**.** *The wffs φ, ψ are tautologically equivalent iff $\{\varphi\} \models \psi$ and $\{\psi\} \models \varphi$*

Definition 3.12 (Finitely Satisfiable)**.** *Σ is finitely satisfiable if every finite subset Σ_0 is satisfiable.*

Theorem 3.4 (The Compactness Theorem)**.** *If Σ is finitely satisfiable, then Σ is satisfiable.*

Before proving the Compactness Theorem, we will make a number of applications.

Theorem 3.5. *Suppose Σ is an infinite set of wffs and $\Sigma \models \varphi$. Then, there exists a finite subset Σ_0 such that $\Sigma_0 \models \varphi$.*

Proof. Suppose not.

Then, for every finite subset $\Sigma_0 \subset \Sigma$, we have $\Sigma_0 \not\models \varphi$, and so $\Sigma_0 \cup \{(\neg\varphi)\}$ is satisfiable.

Thus, $\Sigma \cup \{(\neg\varphi)\}$ is finitely satisfiable.

By compactness, $\Sigma \cup \{(\neg\varphi)\}$ is satisfiable, but this contradicts $\Sigma \models \varphi$. □

Definition 3.13 (Graph)**.** *Let E be a binary relation on a set V. Then, $\Gamma = \langle V, R\rangle$ is a graph iff E is symmetric and irreflexive.*

Definition 3.14 (k-colorable)**.** *Let $k \geq 1$. Then, the graph $\Gamma = \langle V, R\rangle$ is k-colorable if there exists a function*

$$\chi : V \to \{1, 2, \ldots, k\}$$

such that if aEb then $\chi(a) \neq \chi(b)$

Theorem 3.6 (Erdös)**.** *Let $\Gamma = \langle V, R\rangle$ be a countably infinite graph, and $k \geq 1$. Then, Γ is k-colorable iff every finite subgraph Γ_0 of Γ is k-colorable.*

Proof. Suppose that $\chi : V \to \{1, 2, \ldots, k\}$ is a one coloring of Γ.

Let $\Gamma_0 = \langle V_0, E_0\rangle$ be a finite subgraph.

Then, let $\chi_0 = \chi \restriction V_0$ be the restriction of χ to V_0.

Then, χ_0 is a k-coloring of Γ_0.

First, we must choose a suitable propositional language. We need a sentence symbol for each decision we must make.

In this case, we take sentence symbols $C_{v,i}$ $v \in V$ and $1 \leq i \leq k$

Next, we write down the set of wffs Σ which imposes suitable constraints on truth assignments. In this case, Σ consists of the wffs

1. $(\neg(C_{v,i} \wedge C_{v,j}))$ for $v \in V$ and $1 \leq i \neq j \leq k$
2. $(C_{v,1} \vee \ldots \vee C_{v,k})$ for $v \in V$
3. $(\neg(C_{v,i} \wedge C_{w,i}))$ for all $v, w \in V$ with vEw and $1 \leq i \leq k$.

We check that Σ is indeed a suitable collection of wffs.

So, by 1 and 2, for each $v \in V$ there exists a unique $1 \leq i \leq k$ such that $v(C_{v,i}) = T$, hence, χ is a function.

Suppose vEw. By 3, they cannot be assigned the same color. That is, we cannot have $v(C_{v,i}) = T = v(C_{w,i})$ for any $1 \leq i \leq k$.

So now we check that Σ is satisfiable.

Let $\Sigma_0 \subset \Sigma$ be any finite subset.

Let $\Gamma_0 = \langle V_0, E_0 \rangle$ be the finite subgraph consisting of the vertices which were mentioned in Σ_0.

By assumption, Γ_0 is k-colorable.

Let $\chi : V_0 \to \{1, \ldots, k\}$ be a k-coloring of Γ_0.

Then, let ν_0 be a truth assignment such that for all $v \in V_0$, and $1 \leq i \leq k$, $\nu_0(C_{v,i}) = T$ iff $\chi_0(v) = i$.

Then clearly, ν_0 satisfies Σ_0.

Thus, Σ is finitely satisfiable.

By compactness, Σ is satisfiable. Thus, Γ is k-colorable. □

Theorem 3.7. *Let $\langle A, \prec \rangle$ be a countably infinite partial ordering. Then, there exists a linear ordering $\langle A, < \rangle$ such that $<$ extends $\prec$.*

Proof. We work with the propositional language consisting of the sentence symbols $L_{a,b}$ where $a \neq b \in A$.

Let Σ be the set of wffs of the form

1. $(L_{a,b} \wedge L_{b,c}) \Rightarrow L_{a,c}$ for $a, b, c \in A$ distinct.
2. $\neg(L_{a,b} \wedge L_{b,a})$ for $a \neq b \in A$.
3. $(L_{a,b} \vee L_{b,a})$ for $a \neq b \in A$.
4. $L_{a,b}$ for $a \prec b$

Clearly, $<$ is irreflexive, and 2 and 3 show that $<$ has the trichotomy property. By 1, $<$ is transitive, and by 4, $< \supset \prec$.

Thus, it is enough to show that Σ is satisfiable.

By the compactness theorem, it is enough to show that Σ is finitely satisfiable.

Let $\Sigma_0 \subset \Sigma$ be any finite subset.

Let A_0 be the finite subset of A which is actually mentioned in Σ_0.

Let $\prec_0$ be the restriction of $\prec$ to A_0.

By the homework, there exists a linear ordering $<_0$ of A_0 which extends $\prec_0$.

Let ν_0 be a truth assignment such that for all $a \neq b \in A_0$, $\nu_0(L_{a,b}) = T$ iff $a <_0 b$.

So ν_0 satisfies Σ_0. hence, Σ is finitely satisfiable. □

Theorem 3.8 (clearly false). *If $\langle A, < \rangle$ is a countable infinite linear order then A has a least element.*

What goes wrong with an attempted proof by compactness? It turns out to be impossible to translate this into a set of wffs.

Definition 3.15 (Distinct Representatives). *Suppose that S is a set.*

Suppose $\langle S_i : i \in I \rangle$ is an indexed collection of not necessarily distinct subsets of S.

A system of distinct representatives is a choice of elements $x_i \in S_i$ such that if $i \neq j$ then $x_i \neq x_j$.

Theorem 3.9 (Hall's Matching Theorem 1935). *Let S be any set and $n \in \mathbb{N}^+$. Let $\langle s_1, \ldots, s_n \rangle$ be an indexed collection of subsets of S.*

Then, the necessary and sufficient condition for the existence of a system of distinct representatives is

For any $1 \leq k \leq n$ and choice of k distinct indices $i_1, \ldots, i_k$, then we have $|S_{i_1} \cup \ldots \cup S_{i_k}| \geq k$

Theorem 3.10 (clearly false attempt at an infinite Hall's theorem). *As above, but cross out all reference to n.*

Counterexample is $S = \mathbb{N}$.

Theorem 3.11 (Infinite Version of Hall's Matching Theorem). *Let S be any set.*

Let $\langle S_{:} i \in \mathbb{N}^+ \rangle$ be an indexed collection of finite subsets of S.

Then, a necessary and sufficient condition for the existence of a system of distinct representatives is for every $1 \leq k$ and choice of k distinct indices, $i_1, \ldots i_k$ we have $|S_{i_1} \cup \ldots \cup S_{i_k}| \geq k$

Proof. Clearly, if a system exists, then the condition holds.

Conversely, suppose the condition holds.

We work with the propositional language with sentence symbols $C_{n,x}$ for $x \in S_n$ and $n \geq 1$.

Let Σ be the set of wffs of the following form

1. $\neg(C_{n,x} \wedge C_{m,x})$, $x \in S_n \cap S_m$
2. $\neg(C_{n,x} \wedge C_{n,y})$, $x \neq y \in S_n$
3. For each $n \geq 1$, letting $S_n = \{x_1, \ldots x_{t_n}\}$ we add $C_{n,x} \vee \ldots \vee C_{n,x_{t_n}}$

By 2 and 3 we choose exactly one element from each set, and by 1 they are distinct.

It only remains to check that Σ is satisfiable.

By compactness, it is enough to check that Σ is finitely satisfiable.

Let $\Sigma_0 \subset \Sigma$ be any finite subset of Σ.

Let $n_1, \ldots n_N$ be the finitely many indices mentioned in Σ_0.

Then, $S_{n_1}, \dots S_{n_N}$ clearly satisfies Hall's Condition.

By Hall's Theorem, for finite collection, there exists a system of distinct representatives $x_{n_i} \in S_{n_i}$, $1 \le i \le N$.

Let ν_0 be a truth assignment such that if $1 \le i \le N$ and $x \in S_{n_i}$ then $\nu_0(C_{n_i,x}) = T$ iff $x = x_{n_i}$. Then ν_0 satisfies Σ_0. □

We are now almost ready to prove the compactness theorem. The basic idea is that it would be much easier if for every sentence symbol A_n, either $A_n \in \Sigma$ or $(\neg A_n) \in \Sigma$.

Then, the only possible truth assignment satisfying Σ is $\nu(A_n) = T$ iff $A_n \in \Sigma$.

Presumably, this works.

So our strategy will be to extend Σ until we reach this special case.

For technical reasons, we extend Σ so that for every α, either $\alpha \in \Sigma$ or $(\neg\alpha) \in \Sigma$.

Lemma 3.12. *Let Σ be a finite satisfiable set of wffs. For each wff α, either $\Sigma \cup \{\alpha\}$ is finitely satisfiable or $\Sigma \cup \{(\neg\alpha)\}$ is finitely satisfiable.*

Proof. Suppose $\Sigma \cup \{\alpha\}$ isn't finitely satisfiable.

Then, there exists a finite subset $\Sigma_0 \subset \Sigma$ such that $\Sigma_0 \cup \{\alpha\}$ is not satisfiable. Thus, $\Sigma_0 \models \{(\neg\alpha)\}$

We claim that $\Sigma \cup \{(\neg\alpha)\}$ is finitely satisfiable.

Let $\Delta \subseteq \Sigma \cup \{\neg\alpha\}$ be any finite subset.

If $\Delta \subset \Sigma$, then Δ is satisfiable, so we can suppose $\Delta = \Delta_0 \cup \{\neg\alpha\}$ for some finite set $\Delta_0 \subset \Sigma$.

Let ν be a truth assignment which satisfies the finite subset $\Sigma_0 \cup \Delta_0$ of Σ. since $\Sigma_0 \models \neg\alpha$, we must have $\overline{\nu}(\neg\alpha) = T$.

Hence, $\overline{\nu}$ satisfies Δ_0 and $\neg\alpha$.

So, $\Sigma \cup \{\neg\alpha\}$ is finitely satisfiable. □

Now, we shall prove the compactness theorem.

Proof. Let $\alpha_1, \dots, \alpha_n, \dots$ be an enumeration of all wffs.

We shall inductively define and increasing sequence of sets of wffs $\Delta_0 \subseteq \Delta_1 \subseteq \dots$ such that

1. $\Delta_0 = \Sigma$
2. Δ_n is finitely satisfiable
3. Either $\alpha_n \in \Delta_n$ or $\neg\alpha_n \in \Delta_n$

Assume inductively that we have defined Δ_n.

Then, define $\Delta_{n+1} = \Delta_n \cup \{\alpha_{n+1}\}$ if $\Delta_n \cup \{\alpha_{n+1}\}$ is finitely satisfiable and $\Delta_{n+1} = \Delta_n \cup \{\neg\alpha_{n+1}\}$ otherwise.

By lemma, Δ_{n+1} is finitely satisfiable.

So, the inductive construction can be accomplished.

Finally, let $\Delta = \cup_n \Delta_n$

Suppose $\Phi \subset \Delta$ is a finite subset. Then, $\exists n$ such that $\Phi \subset \Delta_n$. Since Δ_n is satisfiable, we know that Φ is satisfiable, so Δ is finitely satisfiable.

Let $\alpha = \alpha_n$, then either $\alpha_n \in \Delta_n$ or $\neg\alpha_n \in \Delta_n$. Since $\Delta_n \subset \Delta$, for each wff α either $\alpha \in \Delta$ or $\neg\alpha \in \Delta$

Finally, define a truth assignment by $\nu(A_\ell)$ if true iff $A_\ell \in \Delta$.

Then, we want to show that for any wff α,$\overline{\nu} = T$ iff $\alpha \in \Delta$.

We argue by induction on the length $m \geq 1$ of the wff α.

First, suppose $m = 1$, then, α is a sentence symbol A_t and the result follows.

Now, suppose $m > 1$, and result holds for all shorter wffs.

Then, α has one of the following forms $(\neg\beta), (\beta\wedge\gamma), (\beta\vee\gamma), (\beta \Rightarrow \gamma), (\beta \Leftrightarrow \gamma)$

Case I - Suppose α is $\neg\beta$. Then, $\overline{\nu}(\neg\beta) = T$ iff $\overline{\nu}(\beta) = F$, which is iff $\beta \notin \Delta$, which is iff $\neg\beta \in \Delta$

Case II - Suppose α is $\beta \wedge \gamma$.

First suppose $\overline{\nu}(\beta \wedge \gamma) = T$,

Then, $\overline{\nu}(\beta) = T$ or $\overline{\nu}(\gamma) = T$, and so $\beta \in \Delta$ or $\gamma \in \Delta$.

Since Δ is finitely satisfiable, $\{\beta, \neg(\beta \vee \gamma)\} \not\subset \Delta$ and $\{\gamma, \neg(\beta \vee \gamma)\} \not\subset \Delta$ so $\neg(\beta \vee \gamma) \notin \Delta$, thus, $\beta \vee \gamma \in \Delta$ Suppose $\beta \vee \gamma \in \Delta$.

Since $\{\neg\beta, \neg\gamma, \beta \vee \gamma\} \not\subset \Delta$, it follows that $\neg\beta \notin \Delta$ or $\neg\gamma \notin \Delta$.

Hence, $\beta \in \Delta$ or $\gamma \in \Delta$. By induction hypothesis, $\overline{\nu}(\beta) = T$ or $\overline{\nu}(\gamma) = T$. Hence, $\overline{\nu}(\beta \vee \gamma) = T$

The other cases are similar. □

Definition 3.16 (Tree)**.** *A partial order $\langle T, < \rangle$ is a tree iff the following conditions are satisfied*

1. *There exists a least element $t_0 \in T$ called the root.*
2. *For each $t \in T$ the set of its predecessors, $\mathrm{Pr}_T(t) = \{s \in T : s < t\}$ is a finite set which is linearly ordered by $<$.*

Definition 3.17 (Complete Binary Tree)**.** *The complete binary tree T_2 is $T_2 = \{f | f : \{0, \ldots, n-1\} \to \{0,1\}$ for some $n \geq 0\}$ ordered by $f < g$ iff $f \subset g$*

Definition 3.18. *Let $\langle T, < \rangle$ be a tree*

1. *If $t \in T$, then the height of t is defined to be $\mathrm{ht}_T(t) = |\mathrm{Pr}_T(t)|$*
2. *For each $n \geq 0$, the n^{th} level of T is $\mathrm{Lev}_n(T) = \{t \in T : \mathrm{ht}_T(t) = n\}$*
3. *For each $t \in T$, the set of immediate successors is $\mathrm{succ}_T(t) = \{s \in T : t < s, \mathrm{ht}_T(s) = \mathrm{ht}_T(t) + 1\}$*
4. *T is finitely branching if each $t \in T$ has a finitely, possibly empty, set of immediate successors.*
5. *A branch $\mathscr{B}$ of T is a maximal linearly ordered subset of T.*

Theorem 3.13. *Consider the complete binary tree T_2.*

if $f : \mathbb{N} \to \{0, 1\}$ is any function, then we obtain a corresponding branch $\mathscr{B}_f = \{f \restriction \{0, \ldots, n-1\} : n \geq 0\}$

Every branch has this form.

Does every infinite tree have an infinite branch?

Clearly not, as there is the tree with a root, and then a countable set of successors to that root, and nothing else.

Lemma 3.14 (König's Lemma)**.** *If T is an infinite, finitely branching tree, then T has an infinite branch.*

Remark - if $\mathscr{B}$ is such a branch, then necessarily, $|\mathscr{B} \cap \mathrm{Lev}_n(T)| = 1$ for all $n \in \mathbb{N}$.

First, we will prove that Compactness implies König.

Proof. Let T be an infinite finitely branching tree. Then $\mathrm{Lev}_n(T)$ is finite for all $n \in \mathbb{N}$, so T is countable.

We use the propositional language with sentence symbols B_t for $t \in T$.

Let Σ be the following set of wffs for each $n \geq 0$, if $\mathrm{Lev}_n(T) = \{t_1, \ldots, t_\ell\}$ then we include:

1. $B_{t_1} \vee \ldots \vee B_{t_\ell}$
2. $\neg(B_{t_i} \wedge B_{t_j})$ for $1 \leq i < j \leq \ell$
3. $B_s \Rightarrow B_t$ for all $s, t \in T$ such that $t < s$

So, by compactness, it is enough to show that Σ is finitely satisfiable.

Let $\Sigma_0 \subset \Sigma$ be an arbitrary finite subset. There exists $n \in \mathbb{N}$ such that if $t \in T$ is mentioned in Σ_0 then $\mathrm{ht}_T(t) < n$ then $v_0(B_t) = T$ iff $t < t_0$.

Clearly, v_0 satisfies Σ_0, thus Σ is finitely satisfiable. $\square$

Now, we shall prove König's Lemma without using compactness.

Proof. We define an induction on $n \geq 0$, a sequence of elements $t_n \in \mathrm{Lev}_n(T)$ such that

1. t_0 is the root
2. if $m < n$ then $t_m < t_n$
3. $\{s \in T : t_n < s\}$ is infinite.

Clearly, t_0 satisfies 2 and 3.

Suppose, inductively, that we have defined t_n. Let $\{a_1, \ldots, a_r\}$ be the set of immediate successors to t_n.

If $t_n < s$, and $\mathrm{ht}_T(s) > n + 1$ then there exists $1 \leq i \leq r$ such that $a_i < s$.

By the Pigeon Hole Principle, there exists $1 \leq i \leq r$ such that $\{s \in T : a_i < s\}$ is infinite.

So, we can choose $t_{n+1} = a_i$.

Then, t_{n+1} satisfies 2 and 3 above. And so, by induction, we have $\mathscr{B} = \{t_n : n \geq 0\}$, an infinite branch. $\square$

So now, an application of König's Lemma

Theorem 3.15 (Erdös). *Let $\Gamma = \langle V, E\rangle$ be a countably infinite graph. Then, Γ is k-colorable iff every finite subgraph of Γ is k-colorable.*

Proof. It is obvious that if it is k-colorable then every finite subgraph is.

Suppose that every finite subgraph is k-colorable.

Let $V = \{v_0, v_1, \ldots\}$

For each $n \geq 1$, let $\Gamma_n = \{v_1, \ldots, v_n\}$

Let C_n be the nonempty set of colorings $\chi : \Gamma_n \to \{1, \ldots, k\}$

Then $|C_n| < k^n$, so C_n is finite.

Let T be the tree such that $\mathrm{Lev}_0(T) = \emptyset$ and $\mathrm{Lev}_n(T) = C_n$ for $n \geq 1$.

If $n < m$ and $\chi \in C_n$, $\theta \in C_m$ we define $\chi < \theta$ iff $\theta \restriction \{v_1, \ldots v_n\} = \chi$

Then, T is an infinite, finitely branching tree. By König's Lemma, there exists an infinite branch $\mathscr{B}$ through T.

For each $n \geq 1$, let $\chi_n \in \mathscr{B} \cap \mathrm{Lev}_n(T)$.

Define $\chi = \bigcup_{n\geq 1} \chi_n$

Clearly, $\chi : v \to \{1, \ldots, k\}$, and suppose $s, t \in v$ are adjacent vertices. Then, there is some $n \geq 1$ such that $s, t \in \Gamma_n$.

Since χ_n is a k-coloring of Γ_n, $\chi(s) = \chi_n(s) \neq \chi_n(t) = \chi(t)$

Thus, χ is a k-coloring. $\square$

Now we will finish proving that König's Lemma is equivalent to the Compactness Theorem

Proof. Let $\{A_1, A_2, \ldots, A_n, \ldots\}$ be the sentences in our language.

Let T be the tree such that

1. $\mathrm{Lev}_0(T) = \emptyset$
2. for $n \geq 1$, $\mathrm{Lev}_n(T) =$ the partial truth assignments $\nu : \{A_1, \ldots, A_n\} \to \{T, F\}$ such that if $\alpha \in \Sigma$ only involves a subset of $\{A_1, \ldots, A_n\}$, then $\overline{\nu}(\alpha) = T$
3. If $\nu, \tau \in T$ with $\nu \in \mathrm{Lev}_m(T)$ and $\tau \in \mathrm{Lev}_n(T)$ with $m < n$, we set $\nu < \tau$ iff $\tau \restriction \{A_1, \ldots, A_n\} = \nu$

Clearly each level $\mathrm{Lev}_n(T)$ is finite, so T is finitely branching.

Let Σ_n be the set of wffs $\alpha \in \Sigma$ which only involve $A_1, \ldots, A_n$. If Σ_n if finite, then Σ_n is satisfiable.

Hence, we can suppose $\Sigma_n = \{\alpha_1, \ldots, \alpha_n, \ldots\}$ is infinite.

For each $\ell \geq 1$, let $\Delta_\ell = \{\alpha_1, \ldots, \alpha_\ell\}$

Then there exists $w_\ell : \{A_1, \ldots, A_n\} \to \{T, F\}$ satisfying Δ_ℓ

By the Pigeonhole Principle, there exists a fixed w such that $w_\ell > w$ for infinitely many $\ell \geq 1$

Clearly w satisfies $\Sigma_n = \bigcup_\ell \Delta_\ell$

Thus, T is an infinite, finitely branching tree. By König's Lemma, there exists an infinite branch $\mathscr{B}$ through T.

Let $\nu_n \in \mathscr{B} \cap \mathrm{Lev}_n(T)$ and define $\nu = \bigcup_n \nu_n$ is a truth assignment which satisfies Σ. $\square$

4 First Order Logic

Definition 4.1 (Alphabet of a First Order Language)**.** *The Alphabet of a First Order Language consists of*

1. *Symbols Common to All Languages*
   (a) *Parentheses* (,)
   (b) *Connectives* $\Rightarrow, \neg$
   (c) *Variables* $v_1, v_2, \dots$
   (d) *Quantifier* $\forall$
   (e) *Equality* $=$
2. *Symbols Particular to the Language (Non logical Symbols)*
   (a) *For each* $n \geq 1$ *a possibly empty countable set of* $n-$*place predicate symbols*
   (b) *A possibly empty countable set of constant symbols*
   (c) *For each* $n \geq 1$ *a possibly empty countable set of* $n-$*ary function symbols*

Example 4.1. *The language of arithmetic is* $\{+, \times, <, 0, 1\}$*, where* $+, \times$ *are* 2*-ary function symbols,* $<$ *is a* 2*-ary predicate symbol and* $0, 1$ *are constants.*

Remark 4.1. *Clearly, an alphabet is countable.*

Definition 4.2 (Expression)**.** *An expression is a finite sequence of symbols from the alphabet.*

Definition 4.3 (Terms)**.** *The set* T *of terms is defined inductively as follows*

1. *Each constant symbol and each variable is a term*
2. *If* f *is an* n*-ary function symbol and* $t_1, \dots, t_n$ *are terms, then* $ft_1, \dots, t_n$ *is a term.*

Definition 4.4 (Atomic Formula)**.** *An atomic formula is an expression of the form* $Pt_1, \dots, t_n$ *where* P *is an* n*-ary predicate symbol.*

Remark- $=$ is a 2-ary predicate symbol, so every language has atomic formulas.

Definition 4.5 (Well-Formed Formulas). *The set of wffs is defined inductively by*

1. *Each atomic formula is a wff*
2. *if α, β are wffs, and v is a variable, then $(\neg\alpha), (\alpha \Rightarrow \beta), \forall v\alpha$ are wffs*

As usual, there exists a unique readability theorem.
Abbreviations
We usually write

1. $(\alpha \vee \beta)$ instead of $((\neg\alpha) \Rightarrow \beta)$
2. $(\alpha \wedge \beta)$ instead of $(\neg(\alpha \Rightarrow (\neg\beta)))$
3. $\exists v\alpha$ instead of $(\neg\forall v(\neg\alpha))$
4. $u = t$ instead of $= ut$
5. $u \neq t$ instead of $(\neg = ut)$
6. etc

We also use common sense in the use of parentheses.

Definition 4.6 (Free Variable). *Let x be a variable and α be a wff*

1. *if α is atomic then x occurs free in α iff x occurs in α*
2. *x occurs free in $(\neg\alpha)$ iff x occurs free in α*
3. *x occurs free in $(\alpha \to \beta)$ iff x occurs free in α or x occurs free in β*
4. *x occurs free in $\forall v\alpha$ iff x occurs free in α and $x \neq v$.*

Definition 4.7 (Sentence). *A sentence σ is a wff with no free variables.*

4.1 Truth and Models

Definition 4.8 (A structure for a first order language). *A structure $\mathscr{A}$ for the first order language $\mathscr{L}$ consists of*

1. *A nonempty set A, the universe of $\mathscr{A}$*
2. *For each n-place predicate symbol P, an n-ary relation $P^{\mathscr{A}} \subset A \times A \times \ldots \times A = A^n$*
3. *For each constant symbol c, an element $c^{\mathscr{A}} \in A$*
4. *For each n-ary function symbol, an n-ary operation $f^{\mathscr{A}} : A^n \to A$*

An Example: Suppose $\mathscr{L}$ has the following non logical symbols: A 2-place predicate symbol R, a constant c and a 1-ary function symbol f.

Then, $\mathscr{A}$ is a structure for $\mathscr{L}$ where:

$A = \{1, 2, 3, 4\}$

$R^{\mathscr{A}} = \{\langle 1,2\rangle, \langle 2,3\rangle, \langle 3,4\rangle, \langle 4,1\rangle\}$

$c^{\mathscr{A}} = 2$ and

$f^{\mathscr{A}} : A \to A$ is $1 \mapsto 2 \mapsto 3 \mapsto 4 \mapsto 1$

Now, we will attempt to define what it means for a statement to be true in a first order language.

Let $\mathscr{L}$ be a first order language.

For each sentence σ of $\mathscr{L}$, and each structure $\mathscr{A}$ for $\mathscr{L}$, we want to define $\mathscr{A} \models \sigma$ as "$\mathscr{A}$ satisfies σ", or "σ is true in $\mathscr{A}$"

Example $\mathscr{N} = \langle \mathbb{N}, +, \times, <, 0, 1\rangle$, clearly, $\mathscr{N} \models \exists x(x + 1 = 1 + 1 + 1)$

First, we are forced to define a more general notion.

Definition 4.9 ($\mathscr{A} \models \varphi$ with s)**.** *Let φ be any wff, $\mathscr{A}$ a structure for $\mathscr{L}$, and $s : V \to A$ where V is the set of variables.*

Then, we define $\mathscr{A} \models \varphi[s]$, "$\mathscr{A}$ satisfies φ with s"

The intuitive meaning is that: φ is true in $\mathscr{A}$ when each free variable v of φ is interpreted as $s(v) \in A$.

Step 1 *Let T be the set of terms of $\mathscr{L}$. We first define an extension $\overline{s} : T \to A$ as follows:*

1. *For each variable v, $\overline{s}(v) = s(v)$*
2. *For each constant symbol c, $\overline{s}(c) = c^{\mathscr{A}}$*
3. *If f is an n-place function symbol and $t_1, \ldots, t_n$ are terms, then*

$$\overline{s}(ft_1, \ldots, t_n) = f^{\mathscr{A}}(\overline{s}(t_1), \ldots, \overline{s}(t_n))$$

Step 2 *Atomic formulas:*

1. $\mathscr{A} \models = t_1 t_2[s]$ *iff* $\overline{s}(t_1) = \overline{s}(t_2)$
2. *If P is an n-ary predicate symbol and $t_1, \ldots, t_n$ are terms, then $\mathscr{A} \models Pt_1, \ldots, t_n[s]$*
   iff $\langle \overline{s}(t_1), \ldots, \overline{s}(t_n)\rangle \in P^{\mathscr{A}}$

Step 3 *Other wffs*

1. $\mathscr{A} \models (\neg\varphi)[s]$ *iff* $\mathscr{A} \not\models \varphi[s]$
2. $\mathscr{A} \models (\varphi \to \psi)[s]$ *iff* $\mathscr{A} \not\models \varphi[s]$ *or* $\mathscr{A} \models \psi[s]$
3. $\mathscr{A} \models \forall v\varphi[s]$ *iff for all* $a \in A$, $\mathscr{A} \models \varphi[s(v|a)]$ *where* $s(v, a) : V \to A$, $s(v|a)(x) = s(x)$ *for* $x \neq v$ *and* $= a$ *for* $x = v$.

Theorem 4.1. *Assume $s_1, s_2 : V \to A$ agree on all free variables (if any) on the wff φ. Then, $\mathscr{A} \models \varphi[s_1]$ iff $\mathscr{A} \models \varphi[s_2]$*

Proof. We argue by induction on the complexity of φ.

Suppose φ is atomic.

First suppose φ is $= t_1t_2$. Then, by the homework, $\overline{s_1}(t_1) = \overline{s_2}(t_1)$ and $\overline{s_1}(t_2) = \overline{s_2}(t_2)$.

Hence, $\mathscr{A} \models = t_1t_2[s_1]$ iff $\overline{s_1}(t_1) = \overline{s_1}(t_2)$ iff $\overline{s_2}(t_1) = \overline{s_2}(t_2)$ iff $\mathscr{A} \models = t_1t_2[s_2]$

Next, suppose φ is $Pt_1, t_2, \dots t_n$

Then, $\overline{s_1}(t_i) = \overline{s_2}(t_i)$ for $1 \leq i \leq n$.

Hence, $\mathscr{A} \models Pt_1, \dots, t_n[s_1]$ iff $\langle \overline{s_1}(t_1), \dots, \overline{s_1}(t_2)\rangle \in P^{\mathscr{A}}$ iff $\langle \overline{s_2}(t_1), \dots, \overline{s_2}(t_2)\rangle \in P^{\mathscr{A}}$ iff $\mathscr{A} \models Pt_1, \dots, t_n[s_2]$

Next, suppose $\varphi = (\neg\psi)$

Then, $\mathscr{A} \models \neg\psi[s_1]$ iff $\mathscr{A} \not\models \psi[s_1]$ iff $\mathscr{A} \not\models \psi[s_2]$ by the inductive hypothesis, iff $\mathscr{A} \models (\neg\psi)[s_2]$

The case where $\varphi = (\psi \Rightarrow \theta)$ is similar.

Finally, we suppose that $\varphi = \forall x\psi$

Clearly, if $a \in A$, then $s_1(x|a)$ and $s_2(x|a)$ agree on all free variables of ψ.

$\mathscr{A} \models \forall x\psi[s_1]$ iff for all $a \in A$, $\mathscr{A} \models \psi[s_1(x|a)]$ iff for all $a \in A$ $\mathscr{A} \models \psi[s_2(x|a)]$ iff $\mathscr{A} \models \forall x\psi[s_1]$. □

Corollary 4.2. *If σ is a sentence, then either $\mathscr{A} \models \sigma[s]$ for all $s : V \to A$ or $\mathscr{A} \not\models \sigma[s]$ for all $s : V \to A$.*

Definition 4.10 ($\mathscr{A} \models \sigma$)**.** *Let σ be a sentence. Then, $\mathscr{A} \models \sigma$ iff $\mathscr{A} \models \sigma[s]$ for all $s : V \to A$*

Definition 4.11 (Satisfies)**.** *Let Σ be a set of wffs*

1. *$\mathscr{A}$ satisfies Σ with s iff $\mathscr{A} \models \sigma[s]$ for all $\sigma \in \Sigma$*
2. *Σ is satisfiable iff there exists a structure $\mathscr{A}$ for $\mathscr{L}$ and a function $s : V \to A$ such that $\mathscr{A}$ satisfies Σ with s.*
3. *Σ is finitely satisfiable iff any finite subset of Σ is satisfiable*

Theorem 4.3 (Compactness Theorem)**.** *If Σ is finitely satisfiable, then Σ is satisfiable.*

An Application of Compactness

Let $\mathscr{L}$ be the language of arithmetic mentioned before.

Let $\mathrm{Th}(\mathbb{N}) = \{\sigma : \sigma \text{ is a sentence which is true in } \langle \mathbb{N}, +, \times, <, 0, 1\rangle\}$

Consider the following set Σ of wffs: $\mathrm{Th}(\mathbb{N}) \cup \{x > \underbrace{1 + \ldots + 1}_{n} : n \geq 1\}$

We claim that Σ is finitely satisfiable.

Let $\Sigma_0 \subset \Sigma$ be finite.

Then, $\Sigma_0 = T \cup \{x > \underbrace{1 + \ldots + 1}_{n_1}, \ldots, \underbrace{x > 1 + \ldots + 1}_{n_t}\}$ with $T \subset \mathrm{Th}(\mathbb{N})$ is a finite subset and $n_1, \ldots, n_t \geq 1$

Let $m > \max\{n_1, \ldots, n_t\}$. Let $s : V \to \mathbb{N}$ satisfy $s(x) = m$.

Then, $\langle \mathbb{N}, +, \times, <, 0, 1\rangle$ satisfies Σ_0.

By compactness, Σ is satisfiable.

Then, $\mathscr{A}$ satisfies $\text{Th}(\mathbb{N})$ and yet $s(x) = c > \underbrace{1^{\mathscr{A}} + \ldots + 1^{\mathscr{A}}}_{n}$ for any number n

So, c is an infinite, or nonstandard, natural number. Furthermore, we can assume $\mathscr{A}$ is countable, and so we get the structure $\mathbb{N} < \mathbb{Q} \times \mathbb{Z}$.

Thus, the statements that are true about $\mathbb{N}$ in first order logic do not uniquely identify $\mathbb{N}$.

Definition 4.12 (Isomorphism)**.** *Let $\mathscr{A}, \mathscr{B}$ be structures for the first order language $\mathscr{L}$*

A function $f : A \to B$ is an isomorphism iff the following conditions are satisfied:

1. *f is a bijection*
2. *for each n-ary predicate symbol P and $a_1, \ldots, a_n \in A$, then $\langle a_1, \ldots, a_n \rangle \in P^{\mathscr{A}}$ iff $\langle f(a_1), \ldots, f(a_n) \rangle \in P^{\mathscr{B}}$*
3. *for each constant symbol c, $f(c^{\mathscr{A}}) = c^{\mathscr{B}}$*
4. *For each n-ary function symbol h and $a_1, \ldots, a_n \in A$, $f(h^{\mathscr{A}}(a_1, \ldots, a_n)) = h^{\mathscr{B}}(f(a_1), \ldots, f(a_n))$*

Theorem 4.4. *Suppose $\varphi : A \to B$ is an isomorphism if σ is any sentence, then $\mathscr{A} \models \sigma$ iff $\mathscr{B} \models \sigma$*

We will actually prove the more general statement:

Theorem 4.5. *Suppose $\varphi : A \to B$ is an isomorphism, and $s : V \to A$. If α is any wff, then $\mathscr{A} \models \alpha[s]$ iff $\mathscr{B} \models \alpha[\varphi \circ s]$*

We shall need the following technical lemma:

Lemma 4.6. *With the above hypotheses, for each term t, $\varphi(\overline{s}(t)) = \overline{\varphi \circ s}(t)$*

Proof. We argue by induction on the complexity of t.

First suppose that t is a variable x.

Then, $\varphi(\overline{s}(x)) = \varphi(s(x)) = (\varphi \circ s)(x) = \varphi(\overline{s}(x)) = \overline{\varphi \circ s}(x)$

Next, suppose that t is a constant symbol c.

Then, $\varphi(\overline{s}(c)) = \varphi(c^{\mathscr{A}}) = c^{\mathscr{B}} = \overline{\varphi \circ s}(c)$

Suppose that t is $ft_1, \ldots, t_n$, by the inductive hypothesis, we know $\varphi(\overline{s}(t_i)) = \overline{\varphi \circ s}(t_i)$.

Thus, $\varphi(\overline{s}(ft_1, \ldots, t_n)) = \varphi(f^{\mathscr{A}}(\overline{s}(t_1), \ldots, \overline{s}(t_n))) = \overline{\varphi \circ s}(ft_1, \ldots, t_n))$ ☐

And now we can prove the theorem

Proof. We argue by induction on complexity of a wff α.

Assume α is atomic, say, $Pt_1, \ldots, t_n$

$\mathscr{A} \models Pt_1, \ldots, t_n[s]$ iff $\langle s(t_1), \ldots, s(t_n) \rangle \in P^{\mathscr{A}}$

iff $\langle\varphi(\overline{s}(t_1)),\ldots,\varphi(\overline{s}(t_n))\rangle \in P^{\mathscr{B}}$
iff $\langle\overline{\varphi\circ s}(t_1),\ldots,\overline{\varphi\circ s}(t_n)\rangle \in P^{\mathscr{B}}$
Next, suppose $\alpha = \neg\beta$, which is similar, as is $\alpha = \beta \Rightarrow \gamma$
Finally, suppose $\alpha = \forall v\beta$. Then, $\mathscr{A} \models \forall v\beta[s]$
iff for all $a \in A$, $\mathscr{A} \models \beta[s(v|a)]$
iff for all $a \in A$, $\mathscr{B} \models \beta[\varphi\circ s(v|a)]$
iff for all $a \in A$, $\mathscr{B} \models \beta[(\varphi\circ s)(v|\varphi(a))]$
As φ is surjective, for all $b \in B$, $\mathscr{B} \models \beta[(\varphi\circ s)(v|b)]$ □

Definition 4.13 (Models)**.** *Let T be a set of sentences*
$\mathscr{A}$ is a model of T iff $\mathscr{A} \models \sigma$ for all $\sigma \in T$
$\mathrm{Mod}(T)$ *is the class of models of T.*

Abbreviation: if E is a binary predicate symbol, then we write xEy instead of Exy.

Example 4.2. *Let T be the following:*
$\neg(\exists x)xEx$
$(\forall x)(\forall y)xEy \Rightarrow yEx$
Then, $\mathrm{Mod}(T)$ *is the class of graphs*

Definition 4.14 (Axiomatizable)**.** *Let $\mathscr{C}$ be a class of structures.*
$\mathscr{C}$ is axiomatizable iff there exists a set of sentences T such that $\mathscr{C} = \mathrm{Mod}(T)$
If there exists a finite set of sentences T, such that $\varphi = \mathrm{Mod}(T)$ then φ is finitely axiomatizable.

Theorem 4.7. *$\mathscr{C}$ is finitely axiomatizable iff $\mathscr{C}$ can be axiomatized by a single sentence.*

Example 4.3. *The class of graphs is finitely axiomatizable*
The class of infinite graphs is axiomatizable
Is the class of finite graphs axiomatizable? Is the class of infinite graphs finitely axiomatizable?

Theorem 4.8. *Let T be a set of sentences in a first order language.*
If T has arbitrarily large finite models, then T has an infinite model.

Proof. For each $n \geq 1$, let θ_n be the sentence which says "There exist at least n elements".
Consider the set of sentences $\Sigma = T \cup \{\theta_n : n \geq 1\}$
We claim that Σ is finitely satisfiable
Suppose $\Sigma_0 \subset \Sigma$ is any finite subset. Then, $\Sigma_0 = T_0 \cup \{\theta_{n_1},\ldots,\theta_{n_t}\}$
Let $m = \max\{n_1,\ldots,n_t\}$, then T has a finite models $\mathscr{A}$ of size greater than m.
Clearly, $\mathscr{A}$ is a model of Σ_0.
By compactness, there exists a model $\mathscr{B}$ of Σ. Thus, $\mathscr{B}$ is an infinite model of T. □

Corollary 4.9. *The class $\mathscr{F}$ of finite graphs is not axiomatizable.*

Corollary 4.10. *The class $\mathscr{C}$ of infinite graphs is not finitely axiomatizable.*

Definition 4.15 (Semantically Implies)**.** *Let Σ be a set of wffs and let φ be a wff.*

Then, Σ logically/semantically implies φ, written $\Sigma \models \varphi$ iff for every structure $\mathscr{A}$ for $\mathscr{L}$ and every $s : V \to A$, if $\mathscr{A}$ satisfies Σ with s, then $\mathscr{A}$ satisfies φ with s.

Definition 4.16 (Valid)**.** *The wff φ is valid iff $\emptyset \models \varphi$*

Now we will return to the development of syntax. Λ will denote the set of logical axioms, defined later.

Definition 4.17 (Deduction)**.** *Let Γ be a set of wffs and let φ be a wff. A deduction of φ from Γ is a finite sequence of wffs $\langle \alpha_1, \alpha_2, \ldots, \alpha_n \rangle$ such that $\alpha_n = \varphi$ and for each $1 \leq i \leq n$ either $\alpha_i \in \Gamma \cup \Lambda$ or there exist $k, j < i$ such that α_k is $\alpha_j \Rightarrow \alpha_i$*

In the latter case, we say that α_i follows from α_j and $\alpha_j \Rightarrow \alpha_i$ by modus ponens (MP).

Definition 4.18 (Theorem)**.** *φ is a theorem of Γ, written, $\Gamma \vdash \varphi$ iff there exists a deduction of φ from Γ.*

And now we finally arrive at the two main theorems of the course.

Theorem 4.11 (The Soundness Theorem)**.** *If $\Gamma \vdash \varphi$ then $\Gamma \models \varphi$*

Theorem 4.12 (Gödel's Completeness Theorem)**.** *If $\Gamma \models \varphi$ then $\Gamma \vdash \varphi$.*

Definition 4.19 (The Logical Axioms, Λ)**.** *φ is a generalization of ψ iff for some $n \geq 0$ and variables $x_1, \ldots, x_n$ we have that φ is $\forall x_1 \ldots \forall x_n \psi$. When $n = 0$ we see that ψ is a generalization of ψ.*

The logical axioms are all generalizations of all wffs of the following forms:

1. *Tautologies*
2. *$(\forall x \alpha \Rightarrow \alpha^x_t)$, where α^x_t means to substitute t for all instances of x in α when t is substitutable for x in α.*
3. *$(\forall x(\alpha \Rightarrow \beta)) \Rightarrow (\forall x \alpha \Rightarrow \forall x \beta)$*
4. *$(\alpha \Rightarrow \forall x \alpha)$ where x does not occur free in α.*
5. *$x = x$*
6. *$(x = y \Rightarrow (\alpha \Rightarrow \alpha'))$ where α is atomic and α' is the result of replacing some, possibly none, of the occurrences of x with y.*

Explanations. A tautology is a wff which can be obtained from a propositional tautology by substituting wffs.

α^x_t is the result of substituting t for each free occurrence of x in α. We say t is substitutable for x in α if no variable of t becomes bound by a quantifier in α^x_t.

Now, we will prove the Soundness theorem, which is easy.

We will make use of the following result

Lemma 4.13. *Each logical axiom is valid.*

And now, the proof of Soundness.

Proof. We argue by the minimum length $n \geq 1$ of a deduction of φ from Γ, that $\Gamma \models \varphi$.

If $n = 1$, then $\varphi \in \Gamma \cup \Lambda$.

Clearly, if $\varphi \in \Gamma$, then $\Gamma \models \varphi$

Suppose $\varphi \in \Lambda$. Then φ is valid, and so $\Gamma \models \varphi$.

Next suppose $n > 1$.

Let $\langle \alpha_1, \ldots, \alpha_n \rangle$ be a deduction of φ from Γ. Then, φ must follow by modus ponens, and so there are earlier wffs ψ and $(\psi \Rightarrow \varphi)$.

Since initial segments of deductions are also deductions, we have that $\Gamma \vdash \psi$ and $\Gamma \vdash (\psi \Rightarrow \varphi)$ by deductions of length less than n.

Let $\mathscr{A}$ be any structure and $s : V \to A$. Suppose $\mathscr{A} \models \Gamma[s]$. By the inductive hypothesis, $\mathscr{A} \models \psi$ and $\mathscr{A} \models (\psi \Rightarrow \varphi)$

Hence, $\Gamma \models \varphi$ □

Definition 4.20 (Inconsistent)**.** *A set Γ of wffs is inconsistent iff there exists a wff β such that $\Gamma \vdash \beta$ and $\Gamma \vdash \neg\beta$.*

Otherwise, Γ is consistent.

Corollary 4.14. *If Γ is satisfiable, then Γ is consistent.*

Proof. Suppose that Γ is satisfiable, say, $\mathscr{A}$ is a structure, $s : V \to A$ and $\mathscr{A} \models \Gamma[s]$.

Suppose Γ is inconsistent, then $\Gamma \vdash \beta$ and $\Gamma \vdash \neg\beta$

By Soundness, $\Gamma \models \beta$ and $\Gamma \models \neg\beta$

Then, $\Gamma \models \beta[s]$ and $\Gamma \models \neg\beta[s]$, which is impossible. □

Now, we shall begin working toward Completeness.

First, we must prove a number of meta-theorems.

Theorem 4.15 (Generalization Theorem)**.** *If $\Gamma \vdash \varphi$ and x does not occur free in Γ then $\Gamma \vdash \forall x\varphi$*

Proof. We argue by induction on the minimum length of a deduction of φ from Γ.

Suppose that $n = 1$.

Then, $\varphi \in \Gamma \cup \Lambda$. If $\varphi \in \Lambda$, then $\forall x\varphi \in \Lambda$, so done.

If $\varphi \in \Gamma$, then, as x is not free in Γ, x does not occur free in φ. So $\varphi \Rightarrow \forall x\varphi$ is in Λ. And so a deduction from Γ of $\forall x\varphi$ is 1-φ, 2-$\varphi \Rightarrow \forall x\varphi$ and 3-$\forall x\varphi$, by modus ponens.

Next, suppose that $n > 1$.

Then, in a proof of minimum length n, φ follows from earlier wffs ψ and $\psi \Rightarrow \varphi$.

By the induction hypothesis, $\Gamma \vdash \forall x\psi$ and $\Gamma \vdash \forall x(\psi \Rightarrow \varphi)$.

So, a deduction of $\forall x\varphi$ from Γ would proceed by first deducing $\forall x\psi$, then $\forall x(\psi \Rightarrow \varphi)$. Then, by the logical axioms, we have $\forall x(\psi \Rightarrow \varphi) \Rightarrow (\forall x\psi \Rightarrow \forall x\varphi)$. And so, by modus ponens, we get $\forall x\psi \Rightarrow \forall x\varphi$, and another modus ponens gives us $\forall x\varphi$. $\square$

Definition 4.21 (Tautologically Implies). $\{\alpha_1, \ldots, \alpha_n\}$ *tautologically implies* β *iff* $(\alpha_1 \Rightarrow (\alpha_2 \Rightarrow (\ldots(\alpha_n \Rightarrow \beta)))\ldots)$ *is a tautology.*

Theorem 4.16 (Rule T). *If* $\Gamma \vdash \alpha_1, \ldots, \Gamma \vdash \alpha_n$ *and* $\{\alpha_1, \ldots, \alpha_n\}$ *tautologically implies* β*, then* $\Gamma \vdash \beta$*.*

Proof. Obvious, by repeated application of modus ponens. $\square$

Theorem 4.17 (Deduction Theorem). *If* $\Gamma \cup \{\gamma\} \vdash \varphi$ *then* $\Gamma \vdash (\gamma \Rightarrow \varphi)$

Proof. We argue by induction on the minimal length of a deduction of φ from $\Gamma \cup \{\gamma\}$.

Suppose $n = 1$.

First, suppose $\varphi \in \Gamma \cup \Lambda$. Then, the following is a deduction of $\gamma \Rightarrow \varphi$. 1-$\varphi$, 2-$(\varphi \Rightarrow (\gamma \Rightarrow \varphi))$ and 3-$\gamma \Rightarrow \varphi$

Second, assume $\varphi = \gamma$.

Then, $\gamma \Rightarrow \varphi$ is a tautology, and so of course $\Gamma \vdash (\gamma \Rightarrow \varphi)$

Suppose $n > 1$.

Then, in a proof of minimal length n, we must have that φ follows from earlier wffs ψ and $(\psi \Rightarrow \varphi)$ by modus ponens.

By induction hypothesis, $\Gamma \vdash (\gamma \Rightarrow \psi)$ and $\Gamma \vdash (\gamma \Rightarrow (\psi \Rightarrow \varphi))$

Clearly, $\{(\gamma \Rightarrow \psi), (\gamma \Rightarrow (\psi \Rightarrow \varphi))\}$ tautologically implies $\gamma \Rightarrow \varphi$.

By Rule T, $\Gamma \vdash (\gamma \Rightarrow \varphi)$ $\square$

Theorem 4.18 (Contraposition). $\Gamma \cup \{\varphi\} \vdash \neg\psi$ *iff* $\Gamma \cup \{\psi\} \vdash \neg\varphi$

Proof. Suppose $\Gamma \cup \{\varphi\} \vdash \neg\psi$

By deduction theorem, $\Gamma \vdash (\varphi \Rightarrow \neg\psi)$

By rule T, $\Gamma \vdash (\psi \Rightarrow \neg\varphi)$

Hence, $\Gamma \cup \{\psi\} \vdash \psi$, so $\Gamma \vdash (\psi \Rightarrow \neg\varphi)$

Hence, $\Gamma \cup \{\psi\} \vdash \varphi$

The other direction is similar. $\square$

Theorem 4.19 (Reductio Ad Absurdum). *If* $\Gamma \cup \{\varphi\}$ *is inconsistent, then* $\Gamma \vdash \neg\varphi$

Proof. Since $\Gamma \cup \{\varphi\}$ is inconsistent, there exists a wff β such that $\Gamma \cup \{\varphi\} \vdash \beta$ and $\Gamma \cup \{\varphi\} \vdash \neg\beta$

By deduction theorem, $\Gamma \vdash (\varphi \Rightarrow \beta)$ and $\Gamma \vdash (\varphi \Rightarrow \neg\beta)$

Clearly, $\{(\varphi \Rightarrow \beta), (\varphi \Rightarrow \neg\beta)\}$ tautologically implies $\neg\varphi$

By rule T, $\Gamma \vdash \neg\varphi$ $\square$

Remark 4.2. *If* Γ *is inconsistant, then* $\Gamma \vdash \alpha$ *for every wff* α

Proof. Suppose that $\Gamma \vdash \beta$ and $\Gamma \vdash \neg\beta$. Clearly $(\beta \Rightarrow (\neg\beta \Rightarrow \alpha))$ is a tautology. By Rule T, $\Gamma \vdash \alpha$. $\square$

Remark 4.3. *Thus, to prove the consistancy of ZFC, it is enough to show that ZFC$\nvdash 0 = 1$.*

Applications: Some theorems about equality:

1. $\vdash \forall x(x = x)$

   Proof. $\forall x(x = x) \in \Lambda$ $\square$

2. $\forall x \forall y(x = y \Rightarrow y = x)$

   Proof. $\vdash x = y \Rightarrow (x = x \Rightarrow y = x)$ by axiom 6. $\vdash x = x$ by axiom 5, $\vdash x = y \Rightarrow y = x$ by Rule T and axioms 1,2. $\vdash \forall y(x = y \Rightarrow y = x)$ by Generalization $\square$

3. $\forall x \forall y \forall z(x = y \Rightarrow (y = z \Rightarrow x = z))$

   Proof. We have $y = x \Rightarrow (y = z \Rightarrow x = z)$ by axiom 6. Then $\vdash x = y \Rightarrow y = x$ by the previous statement, so we have by Rule T and 1,2 $\vdash (x = y \Rightarrow (y = z \Rightarrow z = x))$, and so by Generalization three applied three times, we have $\vdash \forall x \forall y \forall z(x = y \Rightarrow (y = z \Rightarrow z = x))$. $\square$

Theorem 4.20 (Generalization on Constants)**.** *Assume that $\Gamma \vdash \varphi$ and c is a constant symbol which doesn't occur in Γ. Then there exists a variable y which doesn't occur in φ scuh that $\Gamma \vdash \forall y \varphi^c_y$. Furthermore, there exists a deduction of $\forall y \varphi^c_y$ from Γ in which c doesn't occur.*

Remark 4.4. *This says that if we suppose $\Gamma \vdash \varphi(c)$ and c does not occur in Γ, then for a suitable variable y, we have that $\Gamma \vdash \forall y \varphi(y)$.*

More importantly, suppose that Γ is a consistant set of formulas in the language $\mathscr{L}$. Let $\mathscr{L}^+ = \mathscr{L} \cup \{c\}$ where c is a new constant symol. Then Γ remains constant in $\mathscr{L}^+$.

Proof. Suppose that (*)=$\langle \alpha_1, \ldots, \alpha_n \rangle$ is a deduction of φ from Γ. Let y be a variable with any α_i. We claim that (**)=$\langle (\alpha_1)^c_y, \ldots, (\alpha_n)^c_y \rangle$ is a deduction of φ^c_y from Γ. We will check that for all $i \leq n$, either $(\alpha_i)^c_y \in \Gamma \cup \Lambda$ or follows by MP. We will break into cases.

1. Suppose that $\alpha_i \in \Gamma$. Then α_i doesn't involve c, and so $(\alpha_i)^c_y = \alpha_i \in \Gamma$.
2. Suppose $\alpha_i \in \Lambda$. Then it is easily checked that $(\alpha_i)^c_y \in \Lambda$.
3. Suppose that there exist $j, k < i$ such that α_k is $(\alpha_j \Rightarrow \alpha_i)$. Then $(\alpha_k)^c_y$ is $((\alpha_j)^c_y \Rightarrow (\alpha_i)^c_y)$. So $(\alpha_i)^c_y$ follows by Modus Ponens from $(\alpha_j)^c_y$ and $(\alpha_k)^c_y$.

Let Φ be the elements of Γ which actually occur in (**). Then $\Phi \vdash \varphi^c_y$. As y does not occur free in Φ, By generalization, $\Phi \vdash \forall y \varphi^c_y$.

Hence $\Gamma \vdash \forall y \varphi^c_y$. Finally note that c certainly doesn't occur in (**).

Recall the proof of generalization, and we see that c also doesn't occur in the proof of $\forall y \varphi^c_y$ from Γ. $\square$

Corollary 4.21. *Suppose that $\Gamma \vdash \varphi^x_c$ where c is a constant that doesn't occur in $\Gamma \cup \{\varphi\}$. Then $\Gamma \vdash \forall x \varphi$ via a deduction in which c does not occur.*

Proof. By the above theorem, $\Gamma \vdash \forall y (\varphi^x_c)^c_y$ for some variable y which doesn't occur in φ^x_c. Since c doesn't occur in φ, we have that $(\varphi^x_c)^c_y = \varphi^x_y$. Thus, $\Gamma \vdash \forall y \varphi^x_y$.

By the exercise, teh following is a logical axiom: $\forall y \varphi^x_y \Rightarrow \varphi$. Thus $\forall x \varphi^x_y \vdash \varphi$.

Since x doesn't occur free in $\forall y \varphi^x_y$, generalization igves $\forall y \varphi^x_y \vdash \forall x \varphi$.

By deduction, $\vdash (\forall y \varphi^x_y \Rightarrow \forall x \varphi)$, and since $\Gamma \vdash \forall y \varphi^x_y$ by Modus Ponens, wE get $\Gamma \vdash \forall x \varphi$. $\square$

Theorem 4.22 (Existence of Alphabetic Variants). *Let φ be a wff, t a term and x a variable. Then there exists a wff φ' (which differs from φ only in the quantified variables) such that*

1. *$\varphi \vdash \varphi'$ and $\varphi' \vdash \varphi$*
2. *t is a substitute for x in φ'*

Proof. Omitted, see Enderton $\square$

4.2 The Completeness Theorem

Finally, we are ready to begin a proof of the completeness theorem.

Theorem 4.23 (The Completeness Theorem). *If $\Gamma \models \varphi$ then $\Gamma \vdash \varphi$.*

We will make use of the following:

Lemma 4.24. *The following are equivalent:*

1. *The Completeness Theorem*
2. *If Γ is consistant then Γ is satisfiable.*

Proof. $1 \Rightarrow 2$: Suppose that Γ is consistant. Then there exists a wff φ such that $\Gamma \nvdash \varphi$. By completeness, $\Gamma \not\models \varphi$. Hence there exists a structure $\mathscr{A}$ and a function $s : V \to A$ such that $\mathscr{A}$ satisfies Γ with s, but $\mathscr{A} \not\models \varphi[s]$. In particular, $\mathscr{A}$ satisfies Γ with s.

$2 \Rightarrow 1$: Suppose that $\Gamma \nvdash \varphi$. By reductio ad absurdum, $\Gamma \cup \{\neg\varphi\}$ is consistent. Thus, it is satisfiable, and so $\Gamma \not\models \varphi$. $\square$

We now prove the following version of the completeness theorem:

Theorem 4.25 (Completeness)**.** *If Γ is a consistent set of wffs in a countable language $\mathscr{L}$, then there exists a countable structure $\mathscr{A}$ for $\mathscr{L}$ and a function $s : V \to A$ such that $\mathscr{A}$ satisfies Γ with s.*

We will proceed in several lemmas.

Lemma 4.26. *Expand $\mathscr{L}$ to a language $\mathscr{L}^+$ by adding a countably infinite set of new constant symbols. Then Γ remains consistant in $\mathscr{L}^+$.*

Proof. Suppose not. Then there exists a wff β of $\mathscr{L}^+$ such that $\Gamma \vdash (\beta \wedge \neg\beta)$ in $\mathscr{L}^+$.

Suppose that $c_1, \ldots, c_n$ include the new constants, if any, which appear in β. By generalization on constants, there exist variables $y_1, \ldots, y_n$ such that $\Gamma \vdash \forall y_1, \ldots, \forall y_n, \beta' \wedge \neg\beta'$ in $\mathscr{L}$ where β' is the result of replacing each c_i with y_i. Since y_i is substitutable for y_i in β', $\Gamma \vdash \beta' \wedge \neg\beta'$ in $\mathscr{L}$. This is a contradiction. $\square$

Lemma 4.27 (Add Witnesses)**.** *Let $\langle\varphi_1, x_1\rangle, \ldots, \langle\varphi_n, x_n\rangle$ enumerate all pairs $\langle\varphi, x\rangle$ where φ si a wff of $\mathscr{L}^+$ and x is a variable. Let θ_1 be the wff $\neg\forall x_1\varphi_1 \Rightarrow (\neg\varphi_1)^{x_1}_{c_1}$ where c_1 is the first new constnat which doesn't occur in φ. If $n > 1$ then θ_n is the wff $\neg\forall x_n\varphi_n \Rightarrow (\neg\varphi_n)^{x_n}_{c_n}$ where c_n is the first new constant symbol which doesn't occur in $\varphi_1, \ldots, \varphi_n, \theta_1, \ldots, \theta_{n-1}$. Let $\Theta = \Gamma \cup \{\theta_n | n \geq 1\}$. Then Θ is consistant.*

Proof. Suppose not. Then let $n \geq 0$ be the least integer such that $\Gamma \cup \{\theta_1, \ldots, \theta_{n+1}\}$ is inconsistant. Then by reductio ad absurdum, $\Gamma \cup \{\theta_1, \ldots, \theta_n\} \vdash \neg\theta_{n+1}$. Recall that θ_{n+1} has the form $\neg\forall x\varphi \Rightarrow (\neg\varphi)^x_c$. By rule T, we have $\Gamma \cup \{\theta_1, \ldots, \theta_n\} \vdash \neg\forall x\varphi$ adn $\Gamma \cup \{\theta_1, \ldots, \theta_n\} \vdash \varphi^x_c$.

Since c doesn't occur in $\Gamma \cup \{\theta_1, \ldots, \theta_n\} \cup \{\varphi\}$, we have $\Gamma \cup \{\theta_1, \ldots, \theta_n\} \Rightarrow \forall x\varphi$. This contradicts θ_{n+1} being the first contradiction, or the consistency of Γ if $n = 0$. $\square$

Lemma 4.28. *We can extend Θ to a consistent set of wffs Δ such that for every wff φ of $\mathscr{L}^+$, either $\varphi \in \Delta$ or $\neg\varphi \in \Delta$.*

Proof. Let $\alpha_1, \ldots, \alpha_n, \ldots$ be an enumeration of the wffs of $\mathscr{L}^+$. We shall define inductively an increasing sequence $\Delta_0 \subset \Delta_1 \subset \ldots$ of consistent sets of wffs. Let $\Delta_0 = \Theta$.

Suppose inductively that Δ_n has been defined. If $\Delta_n \cup \{\alpha_{n+1}\}$ is consitent, then let $\Delta_{n+1} = \Delta_n \cup \{\alpha_{n+1}\}$. If it is inconsistent, then by reductio ad absurdum, $\Delta_n \vdash \neg\alpha_{n+1}$, and so we let $\Delta_{n+1} = \Delta_n \cup \{\neg\alpha_{n+1}\}$. Clearly $\Delta = \cup\Delta_n$ satisfies our requirements. $\square$

Notice now that Δ is deductively closed. That is, if $\Delta \vdash \varphi$, then $\varphi \in \Delta$. Otherwise if $\varphi \notin \Delta$, then $\neg\varphi \in \Delta$, and so $\Delta \vdash \varphi$ and $\Delta \vdash \neg\varphi$, contradicting the consistency.

Lemma 4.29. *For each of the following wffs, $\Delta \vdash \varphi$ and so $\varphi \in \Delta$:*

1. $\forall x(x = x)$

2. $(\forall x)(\forall y)(x = y \Rightarrow y = x)$

3. $(\forall x)(\forall y)(\forall z)((x = y \land y = z) \Rightarrow x = z)$

4. *For each* n*-ary preducate symbol* P*,* $\forall x_1, \ldots, \forall x_n, \forall y_1, \ldots, \forall y_n((x_1 = y_1 \land \ldots \land x_n = y_n) \Rightarrow Px_1 \ldots x_n = Py_1 \ldots y_n)$

5. *For each* n*-ary function symbol* f*,* $\forall x_1, \ldots, \forall x_n, \forall y_1, \ldots \forall y_n((x_1 = y_1 \land \ldots \land x_n = y_n) \Rightarrow fx_1 \ldots x_n = fy_1 \ldots y_n)$

Similarly, since Δ *is deductively closed and* $\forall x \forall y(x = y \Rightarrow y = x) \in \Delta$*, we have that if* t_1, t_2 *are terms, then* $(t_1 = t_2 \Rightarrow t_2 = t_1) \in \Delta$*.*

Lemma 4.30. *We construct a structure* $\mathscr{A}$ *for our language* $\mathscr{L}^+$ *as follows: Let* T *be the set of terms of* $\mathscr{L}^+$ *and define a binary relation* E *on* T *by* $t_1 E t_2$ *iff* $(t_1 = t_2) \in \Delta$*.*

Then E *is an equivalence relation.*

Proof. Let $t \in T$. Then $(t = t) \in \Delta$, and so tEt for all t, so E is reflexive.

Suppose that $t_1 E t_2$. Then $(t_1 = t_2) \in \Delta$, and so $(t_2 = t_1) \in \Delta$, so $t_2 E t_2$, so E is symmetric.

Transitivity is similar. $\square$

For each $t \in T$, we define $[t] = \{s \in T | tEs\}$, then we define $A = \{[t] | t \in T\}$.

For any n-ary predicate symbol, we define an n-ary relation $P^{\mathscr{A}}$ on A by $\langle [t_1], \ldots, [t_n] \rangle \in P^{\mathscr{A}}$ iff $Pt_1, \ldots, t_n \in \Delta$.

Lemma 4.31. $P^{\mathscr{A}}$ *is well defined.*

Proof. Suppose that $[s_1] = [t_1], \ldots, [s_n] = [t_n]$. We must show that $Ps_1, \ldots, s_n \in \Delta$ iff $Pt_1, \ldots, t_n \in \Delta$. By hypothesis $(s_i = t_i) \in \Delta$ for each i.

Since $((s_i = t_i \land \ldots \land s_n = t_n) \Rightarrow (Ps_1, \ldots, s_n \iff Pt_1, \ldots, t_n)) \in \Delta$, the result follows. $\square$

For each constant symbol c, we define $c^{\mathscr{A}} = [c]$, and for each n-ary function symbol f, we define an n-ary operation $f^{\mathscr{A}}$ on A by $f^{\mathscr{A}}([t_1], \ldots, [t_n]) = [ft_1, \ldots, t_n]$. As above, $f^{\mathscr{A}}$ is well-defined.

Finally, we define $s : V \to A$ by $s(x) = [x]$.

Lemma 4.32. *For every term* t*,* $\bar{s}(t) = [t]$*.*

Proof. By definition this is true when t is a constant symbol or a variable.

Suppose that $t = ft_1, \ldots, t_n$. By induction, we assume that $\bar{s}(t_i) = [t_i]$ for each i. Thus $\bar{s}(ft_1, \ldots, t_n) = f^{\mathscr{A}}(\bar{s}(t_1), \ldots, \bar{s}(t_n)) = f^{\mathscr{A}}([t_1], \ldots, [t_n]) = [ft_1, \ldots, t_n]$. $\square$

Lemma 4.33 (Substitution Lemma)**.** *If the term* t *is substitutable for* x *in* ψ*, then* $\mathscr{A} \models \psi^x_t[s]$ *iff* $\mathscr{A} \models \psi[s(x|\bar{s}(t))]$*.*

And our final claim:

Lemma 4.34. *For each wff φ of $\mathscr{L}^+$, $\mathscr{A} \models \varphi[s]$ iff $\varphi \in \Delta$*

Proof. We argue by deduction on the complexity of φ. First suppose that φ is atomic. Assume that φ is $t_1 = t_2$. Then $\mathscr{A} \models (t_1 = t_2)[s]$ iff $\bar{s}(t_1) = \bar{s}(t_2)$, iff $[t_1] = [t_2]$, iff $(t_1 = t_2) \in \Delta$.

Now suppose that φ is $Pt_1, \ldots, t_n$. Then $\mathscr{A} \models (Pt_1, \ldots, t_n)[s]$ iff $\langle \bar{s}(t_1), \ldots, \bar{s}(t_n)\rangle \in P^{\mathscr{A}}$, iff $\langle [t_1], \ldots, [t_n]\rangle \in P^{\mathscr{A}}$ iff $Pt_1, \ldots, t_n \in \Delta$.

Next we consider the cases where φ is not atomic.

Suppose that φ is $\neg\psi$. Then $\mathscr{A} \models \neg\psi[s]$ iff $\mathscr{A} \not\models \psi[s]$ iff $\psi \notin \Delta$, iff $\neg\psi \in \mathscr{A}$.

The case φ is $\psi \Rightarrow \theta$ is similar.

Finally, suppose φ is $\forall x\psi$. By construction, for some constant c, $(\neg\forall x\varphi \Rightarrow \neg\varphi^x_c) \in \Delta$. Call this (*).

First suppose that $\mathscr{A} \models \forall x\varphi[s]$, then in particular, $\mathscr{A} \models \psi[s(x|[c])]$, that is, $\mathscr{A} \models \psi[s(x|\bar{s}(x))]$.

By the substitution lemma, $\mathscr{A} \models \psi^x_c[s]$, and hence by the induction hypothesis, $\psi^x_c \in \Delta$. Thus $\neg\psi^x_c \notin \Delta$, so (*) implies that $\neg\forall x\psi \notin \Delta$. Thus $\forall x\psi \in \Delta$.

Conversely, suppose that $\mathscr{A} \not\models \forall x\psi[s]$. Then there exists a term $t \in T$ such that $\mathscr{A} \not\models \psi[s(x|[t])]$, that is, $\mathscr{A} \not\models \psi[s(x|\bar{s}(t))]$.

Let ψ' be an alphabetic variant of ψ such that t is substitutable for x in ψ'. Then $\mathscr{A} \not\models \psi'[s(x|\bar{s}(t))]$. By the substitution lemma, $\mathscr{A} \not\models (\psi')^x_t[s]$, and by the induction hypothesis, $(\psi')^c_t \in \Delta$. Since $(\forall x\psi' \Rightarrow (\psi')^x_t) \in \Lambda \subset \Delta$, we must have $\forall x\psi' \notin \Delta$. Thus $\forall x\psi \notin \Delta$.

Finally, let $\mathscr{A}_0$ be the structure for $\mathscr{L}$ obtained by forgetting the interpretations of the new constants. Then $\mathscr{A}_0$ satisfies Γ with s. ☐

Thus, the completeness theorem holds.

Corollary 4.35. $\Gamma \models \varphi \iff \Gamma \vdash \varphi$.

Theorem 4.36 (Compactness Theorem)**.** *Let Γ be a set of wffs in a countable first order language. If Γ is finitely satifiable, then Γ is satisfiable in some countable structure.*

Proof. Suppose that Γ is finitely satisfiable. Let $\Gamma_0 \subset \Gamma$ be any finite subset, then Γ_0 is satisfiable. Hence, by soundness, Γ_0 is consistent. Since every finite subset of Γ is consistent, Γ is consistent. By completeness, Γ is satisfiable in a countable structure. ☐

Theorem 4.37. *Let T be a set of sentences in a first order language. If the class $\mathscr{C} = Mod(T)$ is finitely axiomatizable, then there exists a finite subset $T_0 \subset T$ such that $\mathscr{C} = Mod(T_0)$*

Proof. Suppose that $\mathscr{C} = Mod(T)$ is finitely axiomatizable. Then there exists a sentence σ such that $\mathscr{C} = Mod(\sigma)$, since $Mot(T) = Mod(\sigma)$, we have $T \models \sigma$. Hence by completeness, $T \vdash \sigma$. Thus, there is a finite set $T_0 \subset T$ such that $T_0 \vdash \sigma$. By soundness $T_0 \models \sigma$. Hence, $\mathscr{C} = Mod(T) \subset Mod(T_0) \subset Mod(\sigma) = \mathscr{C}$. ☐

Definition 4.22. *Let $\mathscr{A}, \mathscr{B}$ be structures for the first order language $\mathscr{L}$. Then $\mathscr{A}$ and $\mathscr{B}$ are elementarily equivalent, written $\mathscr{A} \equiv \mathscr{B}$ iff for every sentence $\sigma \in \mathscr{L}$, $\mathscr{A} \models \sigma$ iff $\mathscr{B} \models \sigma$.*

Remark 4.5. *$\mathscr{A} \simeq \mathscr{B}$ implies $\mathscr{A} \equiv \mathscr{B}$, but the converse is false (eg, nonstandard arithmetic.)*

Definition 4.23 (Complete Set)**.** *A consistent set of sentences is said to be complete iff for every sentence σ, either $T \vdash \sigma$ or $T \vdash \neg\sigma$.*

Definition 4.24 (Theory)**.** *A theory is a set of sentences. A consistant theory is complete if it is as a set of sentences.*

Theorem 4.38. *Let T be a complete theory in a first order langague $\mathscr{L}$. If $\mathscr{A}$ and $\mathscr{B}$ are models of T, then $\mathscr{A} \equiv \mathscr{B}$.*

Proof. Let σ be any sentence. Then $T \vdash \sigma$ or $T \vdash \neg\sigma$. Suppose that $T \vdash \sigma$. By soundness if T is true then σ is true. So $\mathscr{A} \models \sigma$ and $\mathscr{B} \models \sigma$.

On the other hand, if $T \vdash \neg\sigma$, then by soundness we have $\mathscr{A} \models \neg\sigma$ and $\mathscr{B} \models \neg\sigma$. □

Theorem 4.39 (Los-Vaught Test)**.** *Let T be a consistent theory in a countable language $\mathscr{L}$. Suppose*

1. *T has no finite models*
2. *If $\mathscr{A}$ are countably infinite models of T, then $\mathscr{A} \simeq \mathscr{B}$.*

Then T is complete.

Proof. Suppose that T satisfies the two conditions. Assume for contradiction that T is not complete. Then there is a sentence σ such that $T \nvdash \sigma$ and $T \nvdash \neg\sigma$. By reduction ad absurdum, $T \cup \{\sigma\}$ and $T \cup \{\neg\sigma\}$ are both consistent. BY completeness, there exist countable models $\mathscr{A}$ and $\mathscr{B}$ of $T \cup \{\sigma\}$ and $T \cup \{\neg\sigma\}$ respectively. By the first property, they are countably infinite, and by the second, $\mathscr{A} \simeq \mathscr{B}$, contradiction. □

Corollary 4.40. *T_{DLO} is complete.*

Proof. T_{DLO} has no finite models. Also we have seen by the back and forth argument that any two countable dense linear orders are isomorphism, and so by L-V, we are done. □

Corollary 4.41. $\langle \mathbb{Q}, < \rangle \equiv \langle \mathbb{R}, < \rangle$

Proof. Both are models of the complete theory T_{DLO}. □

The rationals are a linear order win which "every conceivable finite configuration is realized." We next seek a graph theoretic analogue: the infinite random graph.

Definition 4.25. *For $k \geq 1$, let P_k be the dfirst order sentence in the language of graphs which says that if $x_1, \ldots, x_k, y_1, \ldots, y_k$ are distinct vertices, there exists a vertex z such that $z \neq x_i, y_i$ for all i, z is joined to x_i for all i, and zis not joined to y_i for all i.*

We define the theory T_R to be the theory $\{(\exists x)(\exists y)(x \neq y)\} \cup \{P_k | k \geq 1\}$.

Theorem 4.42. *T_R is consistant.*

Proof. By soundness, it is enough to show that it is satisfiable.

Consider the graph $\Gamma = \langle \mathbb{N}, E \rangle$ where n is joind to m iff 2^n appears in the binary expansion of m, or vice versa.

We claim that Γ satisfies P_k for all $k \geq 1$. So let $n_1, \ldots, n_k, m_1, \ldots, m_k$ be distinct natural numbers. Let $\ell \geq \max\{m_1, \ldots, m_k, n_1, \ldots, n_k\}$. Then $z = 2^{n_1} + \ldots + 2^{n_k} + 2^\ell$ is joined to all of $n_1, \ldots, n_k$, and none of the $m_1, \ldots, m_k$. $\square$

Question: Why is T_R called the theory of the random graph?

Answer: Consider a graph $\Gamma^* = \langle \mathbb{N}, E^* \rangle$ defined as follows. For each pair $n \neq m$, we toss a coin. If heads, we join, if tails we don't.

Proposition 4.43. *Γ^* is a model of T_R with probability 1.*

Proof. Suppose that $x_1, \ldots, x_k, y_1, \ldots, y_k \in \mathbb{N}$ are distinct. Fix some $z \notin F = \{x_1, \ldots, x_k, y_1, \ldots, y_k\}$. Then the probability that z works is 2^{-2k}, and so the probability that z doesn't work is $1 - 2^{-2k}$. Let $\mathbb{N} \setminus F = \{z_1, \ldots, z_n, \ldots\}$.

Then the probability that none of the $z_1, \ldots, z_n$ works is $(1 - 2^{-2k})^n$, and $\lim_{n \to \infty} (1 - 2^{-2k})^n = 0$, and so with probability 1, one of them will work. $\square$

Question: Why is T_R claled the theory of THE random graph?

Theorem 4.44. *If G, H are countably infinite models of T_R, then $G \simeq H$.*

Proof. By the back and forth argument. $\square$

Theorem 4.45. *T_R is complete.*

Proof. L-V. $\square$

And now for something (apparently) completely different.

We'll study the basics of finite random graph theory.

Definition 4.26. *$\mathscr{G}_n$ is the set of all graphs with vertex set $\{1, \ldots, n\}$.*

Remark 4.6. *Each $G \in \mathscr{G}_n$ is uniquely deterined by the edge set $E \in \mathscr{P}(T)$ where $T = \{\{k, \ell\} | 1 \leq k < \ell \leq n\}$. Hence $|\mathscr{G}_n| = 2^{|T|} = 2^{\binom{n}{2}} = 2^{n(n-1)/2}$.*

Definition 4.27. *If φ is any sentence in the language of graph theory, then* $\mathrm{Prob}_n(\varphi) = \frac{|\{G \in \mathscr{G}_n : G \models \varphi\}|}{|\mathscr{G}_n|}$

This is the same probability as if we joined each pair of vertices independently with probability 1/2.

Theorem 4.46 (Zero-One Law)**.** *Let φ be any sentence in the langauge of graph theory. THen either $\lim_{n\to\infty} \mathrm{Prob}_n(\varphi) = 1$ or $\lim_{n\to\infty} \mathrm{Prob}_n(\varphi) = 0$.*

We will first prove the following special case:

Theorem 4.47. *For each $k \geq 1$, $\lim_{n\to\infty} \mathrm{Prob}_n(P_k) = 1$.*

Proof. Let $n \geq 2k+1$. Suppose that $G \in \mathscr{G}_n$ and $G \not\models P_k$. Then there exists $X = \{x_1, \ldots, x_k, y_1, \ldots, y_k\}$ such that no z in $\{1, \ldots, n\} \setminus X$ is joined to precisely the first k. For fixed X, probability of this event is $\left(1 - \left(\frac{1}{2}\right)^{2k}\right)^{n-2k}$. So summing over all possible $2k$ subsets of X, we see that $\mathrm{Prob}_n(\neg P_k) = \binom{n}{2k}\left(1 - \left(\frac{1}{2}\right)^{2k}\right)^{n-2k}$. This is a polynomial times an exponential, and so $\mathrm{Prob}_n(\neg P_k) \to 0$, so $\mathrm{Prob}_n(P_k) \to 1$ as $n \to \infty$. □

Now we prove the Zero-One Law.

Proof. The axioms of T_R are true with probability 1. As T_R is complete by L-V, either $T_R \vdash \varphi$ or $T_R \vdash \neg\varphi$.

Assume that $T_R \vdash \varphi$. Then there exists $k_1 < \ldots < k_s$ such that $\Gamma = (\exists x)(\exists y)(x \neq y), P_{k_1}, \ldots, P_{k_s}\} \vdash \varphi$, and hence $\Gamma \models \varphi$.

Let θ be the sentence which says that there are at least $2k_s + 1$ elements. Then clearly $\{\theta, P_{k_s}\} \models \varphi$. Hence, if $n \geq 2k_s + 1$ then $\mathrm{Prob}_n(P_{k_S}) \leq \mathrm{Prob}_n(\varphi) \leq \lim_{n\to\infty} \mathrm{Prob}_n(P_{k_s}) = 1$, and so $1 \leq \mathrm{Prob}(\varphi) \leq 1$.

The other case is similar. □

Open Problem: Let T be a complete theory in a countable first order language. How many countable models can T have up to isomorphism?

Theorem 4.48 (Vaught)**.** *If T is a complete theory in a countable language, then T cannot have exactly two countable models.*

Theorem 4.49. *There exists a complete theory in a countable language which has exactly 3 countable models up to isomorphism.*

Proof. Let $\mathscr{L}$ be the language with nonlogical symbols: a binary predicate symbol $<$, constant symbols $c_1, \ldots, c_n, \ldots, n \in \mathbb{N}^+$. And let T be the theory which says $<$ is a DLO without end points adn $c_n < c_{n+1}$ for $n \in \mathbb{N}^+$. Clearly, T is consistent.

Three models are $\langle \mathbb{Q}, <, n\rangle$, $\langle \mathbb{Q}, <, 1 - 2^{-n}\rangle$ and $\langle \mathbb{Q}, <, \sum_{k=1}^{n} \frac{1}{k^2}\rangle$.

These are the only models, as if $\mathscr{A} = \langle \mathbb{Q}, <, c_n^{\mathscr{A}}\rangle$, then $\lim_{n\to\infty} c_n^{\mathscr{A}} = \infty$, $\lim_{n\to\infty} c_n^{\mathscr{A}} \in \mathbb{Q}$ or $\lim_{n\to\infty} c_n^{\mathscr{A}} \notin \mathbb{Q}$, and each corresponds to

Let $\mathscr{L}_n$ be the language consisting of $<, c_1, \ldots, c_n$. Let T_n be a theory such that $<$ is a DLO and $c_1 < \ldots < c_n$. Clearly $\mathscr{L} = \cup \mathscr{L}_n$, and $T = \cup T_n$. Note that T_n has no finite models, is consistent, and has a unique countable model up to isomorphism, and so by L-V, T is complete.

Let φ be any sentence in $\mathscr{L}$. Then there exists an $n \in \mathbb{N}^+$ such that φ is a sentence in $\mathscr{L}_n$, and hence $T_n \vdash \varphi$ or $T_n \vdash \neg\varphi$, and hence $T \vdash \varphi$ or $T \vdash \neg\varphi$. Thus T is complete. □

Theorem 4.50. *For each $n \geq 3$, there exists a complete theory in a countable language which hs exactly n models up to isomorphism.*