Introduction to Set Theory

George Voutsadakis[1]

[1]Mathematics and Computer Science
Lake Superior State University

LSSU Math 400

Subsection 1

Cardinality of Sets

Equipotent Sets

- A basic question about a set is: "How many elements does it have?"
- We can define the statement "sets A and B have the same number of elements" without knowing anything about numbers.
- Think of the problem of determining whether the set of all patrons in a theater has the same number of elements as the set of all seats.
  - To find the answer, the ushers need not count the patrons or the seats.
  - It is enough if they check that each patron sits in one, and only one, seat, and each seat is occupied by one, and only one, theater goer.

Definition (Equipotency)

Sets A and B are **equipotent** (have **the same cardinality**), denoted $|A| = |B|$, if there is a one-to-one function f with domain A and range B.

Some Examples

(a) $\{\emptyset, \{\emptyset\}\}$ and $\{\{\{\emptyset\}\}, \{\{\{\emptyset\}\}\}\}$ are equipotent; let $f(\emptyset) = \{\{\emptyset\}\}$ and $f(\{\emptyset\}) = \{\{\{\emptyset\}\}\}$.

(b) $\{\emptyset\}$ and $\{\emptyset, \{\emptyset\}\}$ are not equipotent.

(c) The set of all positive real numbers is equipotent with the set of all negative real numbers; set $f(x) = -x$ for all positive real numbers x.

Properties of Equipotency

Theorem

(a) A is equipotent to A.
(b) If A is equipotent to B, then B is equipotent to A.
(c) If A is equipotent to B and B is equipotent to C, then A is equipotent to C.

(a) Id_A is a one-to-one mapping of A onto A.
(b) If f is a one-to-one mapping of A onto B, f^{-1} is a one-to-one mapping of B onto A.
(c) If f is a one-to-one mapping of A onto B and g is a one-to-one mapping of B onto C, then $g \circ f$ is a one-to-one mapping of A onto C.

Comparing Cardinalities

Definition

The cardinality of A is **less than or equal to** the cardinality of B, denoted $|A| \leq |B|$, if there is a one-to-one mapping of A into B.

- Notice that $|A| \leq |B|$ means that $|A| = |C|$, for some subset C of B.
- We also write $|A| < |B|$ to mean that $|A| \leq |B|$ and not $|A| = |B|$, i.e., that there is a one-to-one mapping of A onto a subset of B, but there is no one-to-one mapping of A onto B.
- This is not the same thing as saying that there exists a one-to-one mapping of A onto a proper subset of B.

  Example: There exists a one-to-one mapping of the set $\mathbb{N}$ onto a proper subset of $\mathbb{N}$, but of course $|\mathbb{N}| = |\mathbb{N}|$.

Lemma on Comparing Cardinalities

Lemma

(a) If $|A| < |B|$ and $|A| = |C|$, then $|C| < |B|$.
(b) If $|A| \leq |B|$ and $|B| = |C|$, then $|A| \leq |C|$.
(c) $|A| \leq |A|$.
(d) If $|A| \leq |B|$ and $|B| \leq |C|$, then $|A| \leq |C|$.

- We prove (a). Assume $|A| < |B|$ and $|A| = |C|$. There exists a one-to-one mapping $f : A \to B$, but no one-to-one mapping of A onto B, and there exists a one-to-one mapping $g : A \to C$ of A onto C.
  - $f \circ g^{-1} : C \to B$ is a one-to-one mapping, whence $|C| \leq |B|$.
  - Assume there exists a one-to-one mapping $h : C \to B$ of C onto B. Then $h \circ g : A \to B$ is a one-to-one mapping of A onto B, which contradicts $|A| < |B|$. Thus, no one-to-one mapping from C onto B exists.

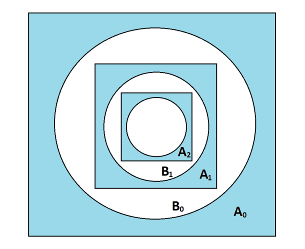
It follows that $|C| < |B|$.

Key Lemma for Antisymmetry

Lemma

If $A_1 \subseteq B \subseteq A$ and $|A_1| = |A|$, then $|B| = |A|$.

Let f be a one-to-one mapping of A onto A_1. By recursion, we define two sequences of sets $A_0, A_1, \ldots, A_n, \ldots$ and $B_0, B_1, \ldots, B_n, \ldots$. Let $A_0 = A$, $B_0 = B$. For each n, $A_{n+1} = f[A_n]$ and $B_{n+1} = f[B_n]$. Since $A_0 \supseteq B_0 \supseteq A_1$, it follows by induction $A_n \supseteq A_{n+1}$, for all n. Define $C_n = A_n - B_n$, $C = \bigcup_{n=0}^{\infty} C_n$ and $D = A - C$ (C is blue part).



We have $f[C_n] = C_{n+1}$, so $f[C] = \bigcup_{n=1}^{\infty} C_n$. We define a one-to-one mapping g of A onto B:

$$g(x) = \begin{cases} f(x), & \text{if } x \in C \\ x, & \text{if } x \in D \end{cases}$$

Both $g \upharpoonright C$ and $g \upharpoonright D$ are one-to-one functions, and their ranges are disjoint. Thus g is a one-to-one function and maps A onto $f[C] \cup D = B$.

The Cantor-Bernstein Theorem

The Cantor-Bernstein Theorem

If $|X| \leq |Y|$ and $|Y| \leq |X|$, then $|X| = |Y|$.

- If $|X| \leq |Y|$, then there exists a one-to-one function f that maps X into Y. If $|Y| \leq |X|$, then there exists a one-to-one function g that maps Y into X. To show that $|X| = |Y|$ we have to exhibit a one-to-one function which maps X onto Y.
  Let us apply first f and then g. The function $g \circ f$ maps X into X and is one-to-one. Clearly, $g[f[X]] \subseteq g[Y] \subseteq X$. Moreover, since f and g are one-to-one, we have $|X| = |g[f[X]]|$ and $|Y| = |g[Y]|$. Thus the theorem follows from the preceding lemma, by taking $A = X$, $B = g[Y]$, $A_1 = g[f[X]]$.

Cardinal Numbers

- The question of whether $\leq$ is linear, i.e., whether $|A| \leq |B|$ or $|B| \leq |A|$ holds for all A and B, requires the Axiom of Choice.
- It is both conceptually and notationally useful to define $|A|$, "the number of elements of the set A", as an actual set.

Assumption

There are sets called **cardinal numbers** (or **cardinals**) with the property that, for every set X there is a unique cardinal $|X|$ (the **cardinal number** of X, the **cardinality** of X) and sets X and Y are equipotent if and only if $|X|$ is equal to $|Y|$.

- In effect, we are assuming existence of a unique "representative" for each class of mutually equipotent sets.
- This assumption can be proved with the help of the Axiom of Choice.
- For certain classes of sets, including finite sets, cardinal numbers can be defined without the Axiom of Choice.

Subsection 2

Finite Sets

Finite and Infinite Sets

- Finite sets can be defined as those sets whose size is a natural number.

Definition (Finite and Infinite Sets)

A set S is **finite** if it is equipotent to some natural number $n \in \mathbb{N}$. We then define $|S| = n$ and say that S **has** n **elements**. A set is **infinite** if it is not finite.

- By our definition, cardinal numbers of finite sets are the natural numbers.
- Obviously, natural numbers are themselves finite sets, and $|n| = n$, for all $n \in \mathbb{N}$.
- To show that the cardinal number of a finite set is unique, we prove

Lemma

If $n \in \mathbb{N}$, then there is no one-to-one mapping of n onto a proper subset $X \subset n$.

Proof of the Lemma

Lemma

If $n \in \mathbb{N}$, then there is no one-to-one mapping of n onto a proper subset $X \subset n$.

- By induction on n.
  - For $n = 0$, the assertion is trivially true.
  - Assume that it is true for n. We proceed to prove it for $n+1$. If the assertion is false for $n+1$, then there is a one-to-one mapping f of $n+1$ onto some $X \subset n+1$. There are two possible cases: Either $n \in X$ or $n \notin X$.
    - If $n \notin X$, then $X \subseteq n$ and $f \restriction n$ maps n onto a proper subset $X - \{f(n)\}$ of n, a contradiction.
    - If $n \in X$, then $n = f(k)$ for some $k < n$. We consider the function g on n defined as follows: $g(i) = \begin{cases} f(i), & \text{for all } i \neq k,\ i < n \\ f(n), & \text{if } i = k < n \end{cases}$. The function g is one-to-one and maps n onto $X - \{n\}$, a proper subset of n, a contradiction.

A Corollary of the Ordering Properties

Corollary

(a) If $n \neq m$, then there is no one-to-one mapping of n onto m.

(b) If $|S| = n$ and $|S| = m$, then $n = m$.

(c) $\mathbb{N}$ is infinite.

(a) If $n \neq m$, then either $n \subset m$ or $m \subset n$. Thus, there is no one-to-one mapping of n onto m.

(b) Immediate from (a).

(c) The successor function is a one-to-one mapping of $\mathbb{N}$ onto its proper subset $\mathbb{N} - \{0\}$. Thus, $|\mathbb{N}| \neq n$, for all $n \in \mathbb{N}$.

- If $m, n \in \mathbb{N}$ and $m < n$ in the ordering of $\mathbb{N}$, then $m \subset n$. Thus, $m = |m| < |n| = n$, where $<$ is the ordering of cardinal numbers. Hence there is no need to distinguish between the two orderings, and we denote both by $<$.

Subsets of Finite Sets are Finite

Theorem (Subsets of Finite Sets are Finite)

If X is a finite set and $Y \subseteq X$, then Y is finite. Moreover, $|Y| \leq |X|$.

- Assume $X = \{x_0, \ldots, x_{n-1}\}$, where $\langle x_0, \ldots, x_{n-1}\rangle$ is a one-to-one sequence, and $Y \neq \emptyset$. To show that Y is finite, we construct a one-to-one finite sequence whose range is Y. We use the Recursion Theorem.
  - $k_0 =$ the least k such that $x_k \in Y$;
  - $k_{i+1} =$ the least k such that $k > k_i$, $k < n$, and $x_k \in Y$ (if such k exists).

  With $A = n = \{0, 1, \ldots, n-1\}$, $a = \min\{k \in n : x_k \in Y\}$ and
  $$g(t,i) = \begin{cases} \min\{k \in n : k > t \text{ and } x_k \in Y\}, & \text{if such } k \text{ exists} \\ \text{undefined}, & \text{otherwise} \end{cases},$$ this satisfies the premises of the Recursion Theorem. Thus, it defines a sequence $\langle k_0, \ldots, k_{m-1}\rangle$. When we let $y_i = x_{k_i}$, for all $i < m$, then $Y = \{y_i : i < m\}$. By induction, it is shown $m < n$ ($k_i \geq i$ whenever defined, so, in particular, $m - 1 \leq k_{m-1} \leq n-1$).

Images of Finite Sets are Finite

Theorem (Images of Finite Sets are Finite)

If X is a finite set and f is a function, then $f[X]$ is finite. Moreover, $|f[X]| \leq |X|$.

- Let $X = \{x_0, \ldots, x_{n-1}\}$. Again, we use recursion to construct a finite one-to-one sequence whose range is $f[X]$. We use the version with $f(n+1) = g(f \restriction n)$:
  - $k_0 = 0$;
  - $k_{i+1} =$ the least $k > k_i$ such that $k < n$ and $f(x_k) \neq f(x_{k_j})$, for all $j \leq i$, (if it exists).

  Set $y_i = f(x_{k_i})$. Then $f[X] = \{y_0, \ldots, y_{m-1}\}$ for some $m \leq n$.
- As a consequence, if $\langle a_i : i < n \rangle$ is any finite sequence (with or without repetition), then the set $\{a_i : i < n\}$ is finite.

The Union of Finite Sets is Finite

Lemma

If X and Y are finite, then $X \cup Y$ is finite. Moreover, $|X \cup Y| \leq |X| + |Y|$, and, if X and Y are disjoint, then $|X \cup Y| = |X| + |Y|$.

- If $X = \{x_0, \ldots, x_{n-1}\}$, $Y = \{y_0, \ldots, y_{m-1}\}$, where $\langle x_0, \ldots, x_{n-1}\rangle$ and $\langle y_0, \ldots, y_{m-1}\rangle$ are one-to-one finite sequences, consider the finite sequence $z = \langle x_0, \ldots, x_{n-1}, y_0, \ldots, y_{m-1}\rangle$ of length $n + m$. Clearly, z maps $n + m$ onto $X \cup Y$. So $X \cup Y$ is finite and $|X \cup Y| \leq n + m$ by the preceding theorem.
  If X and Y are disjoint, z is one-to-one and $|X \cup Y| = n + m$.

The Union of Finitely Many Finite Sets is Finite

Theorem

If S is finite and if every $X \in S$ is finite, then $\bigcup S$ is finite.

- By induction on the number of elements of S.
  - The statement is true if $|S| = 0$.
  - Assume that the statement is true for all S with $|S| = n$.
    Let $S = \{X_0, \ldots, X_{n-1}, X_n\}$ be a set with $n+1$ elements, each $X_i \in S$ being a finite set. By the induction hypothesis, $\bigcup_{i=0}^{n-1} X_i$ is finite. We also have
    $$\bigcup S = (\bigcup_{i=0}^{n-1} X_i) \cup X_n,$$
    which is, therefore, finite by the preceding lemma.

Power Set of a Finite Set is Finite

Theorem (Power Set of a Finite Set is Finite)

If X is finite, then $\mathcal{P}(X)$ is finite.

- By induction on $|X|$.
  - If $|X| = 0$, i.e., $X = \emptyset$, then $\mathcal{P}(X) = \{\emptyset\}$ is finite.
  - Assume that $\mathcal{P}(X)$ is finite whenever $|X| = n$. Let Y be a set with $n+1$ elements: $Y = \{y_0, \ldots, y_n\}$. Let $X = \{y_0, \ldots, y_{n-1}\}$. Note that:
    - $\mathcal{P}(Y) = \mathcal{P}(X) \cup U$, where $U = \{u : u \subseteq Y \text{ and } y_n \in U\}$.
    - $|U| = |\mathcal{P}(X)|$ because there is a one-to-one mapping of U onto $\mathcal{P}(X)$: $f(u) = u - \{y_n\}$, for all $u \in U$.

  Hence $\mathcal{P}(Y)$ is a union of two finite sets and, consequently, finite.

Infinite Sets Have More Elements than Finite Sets

Theorem (Infinite Sets Have More Elements than Finite Sets)

If X is infinite, then $|X| > n$, for all $n \in \mathbb{N}$.

- It suffices to show that $|X| \geq n$, for all $n \in \mathbb{N}$. This can be done by induction.
  - Certainly $0 < |X|$.
  - Assume that $|X| \geq n$. Then, there is a one-to-one function $f : n \to X$. Since X is infinite, there exists $x \in (X - \text{ran} f)$. Define $g = f \cup \{(n, x)\}$. g is a one-to-one function on $n + 1$ into X. We conclude that $|X| \geq n + 1$.

Alternative Definition of Finite Sets

- We briefly discuss another approach to finiteness that does not use natural numbers.
- A set X is **finite** if and only if there exists a relation $\prec$ such that
  - (a) $\prec$ is a linear ordering of X.
  - (b) Every nonempty subset of X has a least and a greatest element in $\prec$.
- Note that this notion of finiteness agrees with the one we defined using finite sequences:
  - If $X = \{x_0, \ldots, x_{n-1}\}$, then $x_0 \prec \cdots \prec x_{n-1}$ describes a linear ordering of X satisfying the properties.
  - If $(X, \prec)$ satisfies (a) and (b), we construct, by recursion, a sequence $\langle f_0, f_1, \ldots \rangle$. The sequence exhausts all elements of X, but the construction must come to a halt after a finite number of steps. Otherwise, the infinite set $\{f_0, f_1, f_2, \ldots\}$ has no greatest element in $(X, \prec)$.

Another Definition of Finite Sets

- We mention another definition of finite sets not involving natural numbers.

  We say that X is **finite** if every nonempty family of subsets of X has a $\subseteq$-maximal element, i.e., if $\emptyset \neq U \subseteq \mathcal{P}(X)$, then, there exists $z \in U$, such that that for no $y \in U$, $z \subset y$.
- Yet another possible approach to finiteness involves an attempt to define **finite sets** as those sets which are not equipotent to any of their proper subsets. However, it is impossible to prove equivalence of this definition with the original one without using the Axiom of Choice.

Subsection 3

Countable Sets

Countable and At Most Countable Sets

- The Axiom of Infinity provides us with an example of an infinite set - the set $\mathbb{N}$ of all natural numbers.
- We investigate the cardinality of $\mathbb{N}$: i.e., we are interested in sets that are equipotent to the set $\mathbb{N}$.

Definition (Countable Set)

A set S is **countable** if $|S| = |\mathbb{N}|$. A set S is **at most countable** if $|S| \leq |\mathbb{N}|$.

- A set S is countable if there is a one-to-one mapping of $\mathbb{N}$ onto S, i.e., if S is the range of an infinite one-to-one sequence.

Infinite Subsets of Countable Sets

Theorem

An infinite subset of a countable set is countable.

- Let A be a countable set, and let $B \subseteq A$ be infinite. There is an infinite one-to-one sequence $\langle a_n \rangle_{n=0}^{\infty}$ whose range is A.
  - We let $b_0 = a_{k_0}$, where k_0 is the least k such that $a_k \in B$.
  - Having constructed b_n, we let $b_{n+1} = a_{k_{n+1}}$, where k_{n+1} is the least k such that $a_k \in B$ and $a_k \neq b_i$, for every $i \leq n$. Such k exists since B is infinite.

  The existence of the sequence $\langle b_n \rangle_{n=0}^{\infty}$ follows easily from the Recursion Theorem. It is easily seen that $B = \{b_n : n \in \mathbb{N}\}$ and that $\langle b_n \rangle_{n=0}^{\infty}$ is one-to-one. Thus B is countable.

Corollary

A set is at most countable if and only if it is either finite or countable.

- If a set S is at most countable then it is equipotent to a subset of a countable set. So it is either finite or countable.

Range of an Infinite Sequence

- The range of an infinite one-to-one sequence is countable.
- If $\langle a_n \rangle_{n=0}^{\infty}$ is an infinite sequence which is not one-to-one, then the set $\{a_n\}_{n=0}^{\infty}$ may be finite (e.g., this happens if it is a constant sequence). However, if the range is infinite, then it is countable.

Theorem (Range of an Infinite Sequence)

The range of an infinite sequence $\langle a_n \rangle_{n=0}^{\infty}$ is at most countable, i.e., either finite or countable. (In other words, the image of a countable set under any mapping is at most countable.)

- By recursion, we construct a sequence $\langle b_n \rangle$ (with either finite or infinite domain) which is one-to-one and has the same range as $\langle a_n \rangle_{n=0}^{\infty}$.
  - We let $b_0 = a_0$;
  - Having constructed b_n, we let $b_{n+1} = a_{k_{n+1}}$, where k_{n+1} is the least k such that $a_k \neq b_i$, for all $i \leq n$. (If no such k exists, then we consider the finite sequence $\langle b_i : i \leq n \rangle$.)

  The sequence $\langle b_i \rangle$ is one-to-one and its range is $\{a_n\}_{n=0}^{\infty}$.

Partitioning a Countable Set into Countable Subsets

- Not all properties of size carry over from finite sets to the infinite case.
- A countable set S can be decomposed into two disjoint parts, A and B, such that $|A| = |B| = |S|$; that is inconceivable if S is finite (unless $S = \emptyset$).
- Consider the set $E = \{2k : k \in \mathbb{N}\}$ of all even numbers, and the set $O = \{2k+1 : k \in \mathbb{N}\}$ of all odd numbers. Both E and O are infinite, hence countable. Thus we have $|\mathbb{N}| = |E| = |O|$, while $\mathbb{N} = E \cup O$ and $E \cap O = \emptyset$.
- Even more striking: Let p_n denote the n-th prime number, i.e., $p_0 = 2$, $p_1 = 3$, etc. Let

$$S_0 = \{2^k : k \in \mathbb{N}\}, S_1 = \{3^k : k \in \mathbb{N}\}, \ldots, S_n = \{p_n^k : k \in \mathbb{N}\}, \ldots$$

  The sets S_n, $n \in \mathbb{N}$, are mutually disjoint countable subsets of $\mathbb{N}$. Thus, we have $\mathbb{N} \supseteq \bigcup_{n=0}^{\infty} S_n$, where $|S_n| = |\mathbb{N}|$, and the S_n's are mutually disjoint.

The Union of Two Countable Sets is Countable

Theorem

The union of two countable sets is a countable set.

- Let $A = \{a_n : n \in \mathbb{N}\}$ and $B = \{b_n : n \in \mathbb{N}\}$ be countable. We construct a sequence $\langle c_n \rangle_{n=0}^{\infty}$ as follows:

$$c_{2k} = a_k, \quad \text{and} \quad c_{2k+1} = b_k, \quad \text{for all } k \in \mathbb{N}.$$

Then $A \cup B = \{c_n : n \in \mathbb{N}\}$ and, since it is infinite, it is countable.

Corollary

The union of a finite system of countable sets is countable.

- This can be proved by induction on the size of the system, using the preceding theorem.

Need for Axiom of Choice

- One might be tempted to conclude that the union of a countable system of countable sets in countable, but this can only be proved if one uses the Axiom of Choice.
- Without the Axiom of Choice, one cannot even prove the following "evident" theorem:

  If $S = \{A_n : n \in \mathbb{N}\}$ and $|A_n| = 2$ for each n, then $\bigcup_{n=0}^{\infty} A_n$ is countable!

  The difficulty is in choosing, for each $n \in \mathbb{N}$, a unique sequence enumerating A_n. If such a choice can be made, the result holds, as we will show later.

Cartesian Product of Countable Sets

Theorem

If A and B are countable, then $A \times B$ is countable.

- It suffices to show that $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$, i.e., to construct
  - either a one-to-one mapping of $\mathbb{N} \times \mathbb{N}$ onto $\mathbb{N}$ or
  - a one-to-one sequence with range $\mathbb{N} \times \mathbb{N}$.

  We provide three methods:

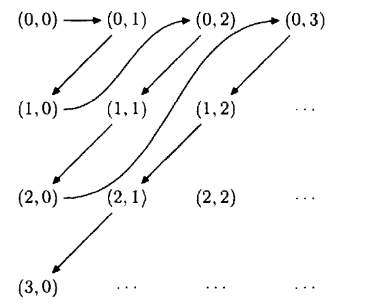
  (a) Consider the function

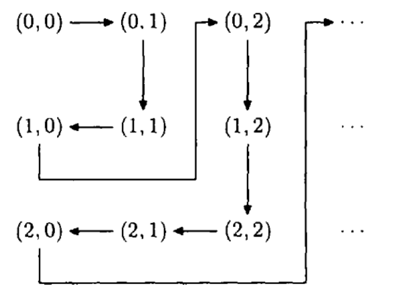
$$f(k, n) = 2^k \cdot (2n + 1) - 1.$$

  f is one-to-one and the range of f is $\mathbb{N}$.

Other Proofs of the Theorem

(b) Construct a sequence of elements of $\mathbb{N} \times \mathbb{N}$ in the manner prescribed by the diagram on the left:





(c) Construct a sequence of elements of $\mathbb{N} \times \mathbb{N}$ in the manner prescribed by the diagram on the right.

Cartesian Products and Countable Systems

Corollary

The cartesian product of a finite number of countable sets is countable. Consequently, $\mathbb{N}^m$ is countable, for every $m > 0$.

- This statement can be proved by induction.

Theorem

Let $\langle A_n : n \in \mathbb{N} \rangle$ be a countable system of at most countable sets, and let $\langle a_n : n \in \mathbb{N} \rangle$ be a system of enumerations of the A_n, i.e., for each $n \in \mathbb{N}$, $a_n = \langle a_n(k) : k \in \mathbb{N} \rangle$ is an infinite sequence, and $A_n = \{a_n(k) : k \in \mathbb{N}\}$. Then $\bigcup_{n=0}^{\infty} A_n$ is at most countable.

- Define $f : \mathbb{N} \times \mathbb{N} \to \bigcup_{n=0}^{\infty} A_n$ by $f(n, k) = a_n(k)$. f maps $\mathbb{N} \times \mathbb{N}$ onto $\bigcup_{n=0}^{\infty} A_n$. Thus, the latter is at most countable by the preceding theorems.

Cartesian Power and Countable Systems of Countable Sets

Theorem

If A is countable, then the set $\mathrm{Seq}(A)$ of all finite sequences of elements of A is countable.

- It is enough to prove the theorem for $A = \mathbb{N}$. As $\mathrm{Seq}(\mathbb{N}) = \bigcup_{n=0}^{\infty} \mathbb{N}^n$, the theorem follows from the preceding thorem, if we can produce a sequence $\langle a_n : n \geq 1 \rangle$ of enumerations of $\mathbb{N}^n$. We do that by recursion. Let g be a one-to-one mapping of $\mathbb{N}$ onto $\mathbb{N} \times \mathbb{N}$. Define recursively:
  - $a_1(i) = \langle i \rangle$, for all $i \in \mathbb{N}$;
  - $a_{n+1}(i) = \langle b_0, \ldots, b_{n-1}, i_2 \rangle$, where $g(i) = (i_1, i_2)$ and $\langle b_0, \ldots, b_{n-1} \rangle = a_n(i_1)$, for all $i \in \mathbb{N}$.

  The idea is to let $a_{n+1}(i)$ be the $(n+1)$-tuple resulting from the concatenation of the (i_1)-th n-tuple (in the previously constructed enumeration of n-tuples, a_n) with i_2. An easy proof by induction shows that a_n is onto $\mathbb{N}^n$, for all $n \geq 1$, and therefore $\bigcup_{n=1}^{\infty} \mathbb{N}^n$ is countable. Since $\mathbb{N}^0 = \{\langle\rangle\}$, $\bigcup_{n=0}^{\infty} \mathbb{N}^n$ is also countable.

Set of Finite Subsets of a Countable Set

Corollary

The set of all finite subsets of a countable set is countable.

- The function F defined by $F(\langle a_0, \ldots, a_{n-1} \rangle) = \{a_0, \ldots, a_{n-1}\}$ maps the countable set $\mathrm{Seq}(A)$ onto the set of all finite subsets of A. Since the first set is countable, the second is countable also.

Integers, Rationals and Equivalence Classes

Theorem

The set of all integers $\mathbb{Z}$ and the set of all rational numbers $\mathbb{Q}$ are countable.

- $\mathbb{Z}$ is countable because it is the union of two countable sets: $\mathbb{Z} = \{0, 1, 2, 3, \ldots\} \cup \{-1, -2, -3, \ldots\}$. $\mathbb{Q}$ is countable because the function $f : \mathbb{Z} \times (\mathbb{Z} - \{0\}) \to \mathbb{Q}$ with $f(p, q) = p/q$ maps a countable set onto $\mathbb{Q}$.

Theorem

An equivalence relation on a countable set has at most countably many equivalence classes.

- Let E be an equivalence relation on a countable set A. The function F defined by $F(a) = [a]_E$ maps the countable set A onto the set A/E. Thus, A/E is at most countable.

Closures in Structures

Theorem

Let $\mathfrak{A}$ be a structure with the universe A, and let $C \subseteq A$ be at most countable. Then $\overline{C}$, the closure of C, is also at most countable.

- We have shown that $\overline{C} = \bigcup_{n=0}^{\infty} C_i$, where $C_0 = C$ and $C_{i+1} = C_i \cup F_0[C_i^{f_0}] \cup \cdots \cup F_{n-1}[C_i^{f_{n-1}}]$. It therefore suffices to produce a system of enumerations of $\langle C_i : i \in \mathbb{N}\rangle$. Let $\langle c(k) : k \in \mathbb{N}\rangle$ be an enumeration of C, and let g be a mapping of $\mathbb{N}$ onto the countable set $(n+1) \times \mathbb{N} \times \mathbb{N}^{f_0} \times \cdots \times \mathbb{N}^{f_{n-1}}$. We define a system of enumerations $\langle a_i : i \in \mathbb{N}\rangle$ recursively as follows:
  - $a_0(k) = c(k)$;
  - $a_{i+1}(k) = \begin{cases} F_p(a_i(r_p^0), \ldots, a_i(r_p^{f_p - 1})), & \text{if } 0 \leq p \leq n-1 \\ a_i(q), & \text{if } p = n \end{cases}$, where

    $g(k) = \langle p, q, \langle r_0^0, \ldots, r_0^{f_0 - 1}\rangle, \ldots, \langle r_{n-1}^0, \ldots, r_{n-1}^{f_{n-1}-1}\rangle\rangle$.

  The definition of a_{i+1} is designed so as to make it transparent that if a_i enumerates C_i, a_{i+1} enumerates C_{i+1} (with many repetitions). By induction, a_i enumerates C_i, for each $i \in \mathbb{N}$, as required.

Aleph-Naught $\aleph_0$

Definition (Aleph-Naught)

$|A| = \mathbb{N}$, for all countable sets A.

- We use the symbol $\aleph_0$ (aleph-naught) to denote the cardinal number of countable sets, i.e., the set of natural numbers, when it is used as a cardinal number.
- Here is a summary of some of the results of this section using the new notation:
  (a) $\aleph_0 > n$, for all $n \in \mathbb{N}$;
  if $\aleph_0 \geq \kappa$, for some cardinal number κ, then $\kappa = \aleph_0$ or $\kappa = n$, for some $n \in \mathbb{N}$.
  (b) If $|A| = \aleph_0$, $|B| = \aleph_0$, then $|A \cup B| = \aleph_0$, $|A \times B| = \aleph_0$.
  (c) If $|A| = \aleph_0$, then $|\mathrm{Seq}(A)| = \aleph_0$.

Subsection 4

Linear Orderings

The sets $\mathbb{N}, \mathbb{Z}$ and $\mathbb{Q}$

- We cannot distinguish among the sets $\mathbb{N}$, $\mathbb{Z}$ and $\mathbb{Q}$ solely on the basis of their cardinality. The three sets "look" quite different and to capture the difference, we have to consider the way they are ordered.
- The ordering of $\mathbb{N}$ by size is quite different from the usual ordering of $\mathbb{Z}$ (for example, $\mathbb{N}$ has a least element and $\mathbb{Z}$ does not).
- Both are quite different from the usual ordering of $\mathbb{Q}$ (for example, between any two distinct rational numbers lie infinitely many rationals, while between any two distinct integers lie only finitely many integers).
- Linear orderings are an important tool in the study of various properties of sets.

Similarity of Linearly Ordered Sets

Definition (Similarity of Linearly Ordered Sets)

Linearly ordered sets $(A, <)$ and $(B, \prec)$ are **similar** (have the **same order type**) if they are isomorphic, i.e., if there is a one-to-one mapping f on A onto B such that for all $a_1, a_2 \in A$,

$$a_1 < a_2 \text{ holds if and only if } f(a_1) \prec f(a_2) \text{ holds.}$$

- Similar ordered sets "look alike"; their orderings have the same properties. It follows that:
  - $(\mathbb{N}, <)$ and $(\mathbb{Z}, <)$ are not similar;
  - Likewise, $(\mathbb{Z}, <)$ and $(\mathbb{Q}, <)$ are not similar;
  - $(\mathbb{N}, <)$ and $(\mathbb{Q}, <)$ are not similar either.

Order Types

- Similarity behaves like an equivalence relation:
  (a) $(A, <)$ is similar to $(A, <)$.
  (b) If $(A, <)$ is similar to $(B, \prec)$, then $(B, \prec)$ is similar to $(A, <)$.
  (c) If $(A_1, <_1)$ is similar to $(A_2, <_2)$ and $(A_2, <_2)$ is similar to $(A_3, <_3)$, then $(A_1, <_1)$ is similar to $(A_3, <_3)$.
- Just as in the case of cardinal numbers, it is possible to assume that with each linearly ordered set there is associated an object called its **order type** so that similar ordered sets have the same order type.
- To avoid technical problems connected with a formal definition of order types, we use them only as a figure of speech, which can be avoided by talking about similar sets instead.
- We define rigorously order types of well-ordered sets (the most important special case) later.

Linearly Ordered Finite Sets are Well-Ordered

Lemma

Every linear ordering on a finite set is a well-ordering.

- We show that every nonempty finite subset B of a linearly ordered set $(A, <)$ has a least element. We accomplish this by induction on the number of elements of B.
  - If B has 1 element, the claim is clearly true.
  - Assume that it is true for all n-element sets. Let B have $n+1$ elements. Then $B = \{b\} \cup B'$, where B' has n elements and $b \notin B'$. By the inductive hypothesis, B' bas a least element b'.
    - If $b' < b$, then b' is the least element of B.
    - Otherwise, b is the least element of B.

  In either case, B has a least element.

Finite Equipotent Linear Orderings are Similar

Theorem

If $(A_1, <_1)$ and $(A_2, <_2)$ are linearly ordered sets and $|A_1| = |A_2|$ is finite, then $(A_1, < 1)$ and $(A_2, <_2)$ are similar.

- We proceed by induction on $n = |A_1| = |A_2|$.
  - If $n = 0$, then $A_1 = A_2 = \emptyset$ and $(A_1, <_1)$, $(A_2, <_2)$ are isomorphic.
  - Assume that the claim is true for all linear orderings of n-element sets. Let $|A_1| = |A_2| = n + 1$. We proved that $<_1$ and $<_2$ are well-orderings, so let a_1 (a_2, respectively) be the least element of $(A_1, <_1)$ ($(A_2, <_2)$, respectively). Now $|A_1 - \{a_1\}| = |A_2 - \{a_2\}| = n$, so by the inductive hypothesis, there is an isomorphism g between $(A_1 - \{a_1\}, <_1 \cap (A_1 - \{a_1\})^2)$ and $(A_2 - \{a_2\}, <_2 \cap (A_2 - \{a_2\})^2)$. Define $f : A_1 \to A_2$ by $f(a_1) = a_2$ and $f(a) = g(a)$, for all $a \in A_1 - \{a_1\}$. It is easy to check that f is an isomorphism between $(A_1, <_1)$ and $(A_2, <_2)$.
- Thus, for finite sets order types correspond to cardinal numbers.
- Linear orderings of infinite sets are much more interesting.

Inverse of a Linear Ordering

Lemma

If $(A, <)$ is a linear ordering, then $(A, <^{-1})$ is also a linear ordering.

- The proof is omitted.
- Example: The inverse of the ordering $(\mathbb{N}, <)$ is the ordering $(\mathbb{N}, <^{-1})$:

$$\ldots <^{-1} 4 <^{-1} 3 <^{-1} 2 <^{-1} 1 <^{-1} 0.$$

Notice that it is similar to the ordering of negative integers by size:

$$\ldots - 4 < -3 < -2 < -1.$$

It is not a well-ordering.

Sum of Linearly Ordered Sets

Lemma

Let $(A_1, <_1)$ and $(A_2, <_2)$ be linearly ordered sets and $A_1 \cap A_2 = \emptyset$. The relation $<$ on $A = A_1 \cup A_2$ defined by

$$a < b \quad \text{if and only if} \quad \begin{array}{l} a, b \in A_1 \text{ and } a <_1 b \\ \text{or } a, b \in A_2 \text{ and } a <_2 b \\ \text{or } a \in A_1, b \in A_2. \end{array}$$

is a linear ordering.

- This proof is also omitted.
- The set A is ordered by putting all elements of A_1 before all elements of A_2.
- We say that the linearly ordered set $(A, <)$ is the **sum** of the linearly ordered sets $(A_1, <_1)$ and $(A_2, <_2)$.

Example of a Sum

- The order type of the sum does not depend on the particular orderings $(A_1, <_1)$ and $(A_2, <_2)$, only on their types.
- Example: The linearly ordered set $(\mathbb{Z}, <)$ of all integers is similar to the sum of the linearly ordered sets $(\mathbb{N}, <^{-1})$ and $(\mathbb{N}, <)$ ($<$ denotes the usual ordering of numbers by size).

Lexicographic Ordering of Product

Lemma

Let $(A_1, <_1)$ and $(A_2, <_2)$ be linearly ordered sets. The relation $<$ on $A = A_1 \times A_2$ defined by $(a_1, a_2) < (b_1, b_2)$ if and only if $a_1 <_1 b_1$ or $(a_1 = b_1$ and $a_2 <_2 b_2)$ is a linear ordering.

- Transitivity: If $(a_1, a_2) < (b_1, b_2)$ and $(b_1, b_2) < (c_1, c_2)$, we have either $a_1 <_1 b_1$ or $(a_1 = b_1$ and $a_2 <_2 b_2)$.
  - In the first case $a_1 <_1 b_1$ and $b_1 \leq_1 c_1$ gives $a_1 <_1 c_1$.
  - In the second case, either $b_1 <_1 c_1$ and $a_1 <_1 c_1$ again, or $b_1 = c_1$ and $b_2 <_2 c_2$, so that $a_1 = c_1$ and $a_2 <_2 c_2$.
- Asymmetry: This follows immediately from asymmetry of $<_1$ and $<_2$.
- Linearity: Given (a_1, a_2) and (b_1, b_2), one of the following occurs:
  (a) $a_1 <_1 b_1$ (so $(a_1, a_2) < (b_1, b_2)$);
  (b) $b_1 <_1 a_1$ (so $(b_1, b_2) < (a_1, a_2)$);
  (c) $a_1 = b_1$ and $a_2 <_2 b_2$ (so $(a_1, a_2) < (b_1, b_2)$);
  (d) $a_1 = b_1$ and $b_2 <_2 a_2$ (so $(b_1, b_2) < (a_1, a_2)$);
  (e) $a_1 = b_1$ and $a_2 = b_2$ (so $(a_1, a_2) = (b_1, b_2)$).
- $<$ is the **lexicographic ordering** (**lexicographic product**) of $A_1 \times A_2$.

Product of a Sequence of Linearly Ordered Sets

Theorem

Let $\langle (A_i, <_i) : i \in I \rangle$ be an indexed system of linearly ordered sets, where $I \subseteq \mathbb{N}$. The relation $\prec$ on $\prod_{i \in I} A_i$ defined by

$$f \prec g \quad \text{iff} \quad \begin{array}{l} \text{diff}(f, g) = \{i \in I : f_i \neq g_i\} \neq \emptyset \text{ and } f_{i_0} <_{i_0} g_{i_0}, \\ \text{where } i_0 \text{ is the least element of } \text{diff}(f, g) \end{array}$$

is a linear ordering of $\prod_{i \in I} A_i$ (it is called its **lexicographic ordering**).

- Transitivity: Assume that $f \prec g$ and $g \prec h$. Let i_0 and j_0 be the least elements of $\text{diff}(f, g)$ and $\text{diff}(g, h)$, respectively. If $i_0 < j_0$, we have $f_{i_0} <_{i_0} g_{i_0}$ and $g_{i_0} = h_{i_0}$, so $f_{i_0} <_{i_0} h_{i_0}$ and i_0 is the least element of $\text{diff}(f, h)$. So $f \prec h$. The cases $i_0 = j_0$ and $i_0 > j_0$ are similar.
- Asymmetry: $f \prec g$ and $g \prec f$ is impossible because it would mean that $f_{i_0} < g_{i_0}$ and $g_{i_0} < f_{i_0}$, for $i_0 =$ the least element of $\text{diff}(f, g) = \text{diff}(g, f)$.

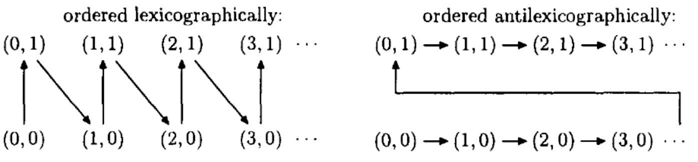
Product of a Sequence of Linearly Ordered Sets (Cont'd)

- Linearity: If $\mathrm{diff}(f,g)=\emptyset$, we have $f=g$. Otherwise, if i_0 is the least element of $\mathrm{diff}(f,g)$, either $f_{i_0}<_{i_0}g_{i_0}$ or $f_{i_0}>_{i_0}g_{i_0}$, holds and, consequently, either $f\prec g$ or $f\succ g$.
- In particular, if $(A_i,<_i)=(A,<)$, for all $i\in I=\mathbb{N}$, $\prec$ is the lexicographic ordering of the set $A^{\mathbb{N}}$ of all infinite sequences of elements of A.

Antilexicographic Ordering

- One can also choose to compare second coordinates before comparing the first coordinates and so define the **antilexicographic ordering** $\prec$ of $A_1 \times A_2$:

  $(a_1, a_2) \prec (b_1, b_2)$ if and only if $a_2 <_2 b_2$ or $(a_2 = b_2$ and $a_1 <_1 b_1)$.
- The proof that $\prec$ is a linear ordering is entirely analogous to the lexicographic case.
- The two orderings are generally quite different.
- Example: The lexicographic and antilexicographic products of $A_1 = \mathbb{N} = \{0, 1, 2, \ldots\}$ and $A_2 = \{0, 1\}$ (both ordered by size):
  - The first ordering is similar to $(\mathbb{N}, <)$.
  - The second is not (it is the sum of two copies of $(\mathbb{N}, <)$).



Dense Ordered Sets

- It is rather surprising that there is a universal linear ordering of countable sets, i.e., such that every countable linearly ordered set is similar to one of its subsets.

Definition (Dense Ordered Set)

An ordered set $(X, <)$ is **dense** if it has at least two elements and if, for all $a, b \in X$, $a < b$ implies that there exists $x \in X$, such that $a < x < b$.

- Let us call the least and the greatest elements of a linearly ordered set (if they exist) the **endpoints** of the set.
- The most important example of a countable dense linearly ordered set is the set $\mathbb{Q}$ of all rational numbers, ordered by size.
  - The ordering is dense because, if r, s are rational numbers and $r < s$, then $x = \frac{r+s}{2}$ is also a rational number, and $r < x < s$.
  - Moreover, $(\mathbb{Q}, <)$ has no endpoints (if $r \in \mathbb{Q}$ then $r+1, r-1 \in \mathbb{Q}$ and $r-1 < r < r+1$).
  - We prove that all countable linearly ordered sets without endpoints have the same order type.

Countable Dense Linear Orders Without Endpoints I

Theorem

Let $(P, \prec)$ and $(Q, <)$ be countable dense linearly ordered sets without endpoints. Then $(P, \prec)$ and $(Q, <)$ are similar.

- Let $\langle p_n : n \in \mathbb{N} \rangle$ be a 1-1 sequence such that $P = \{p_n : n \in \mathbb{N}\}$. Let $\langle q_n : n \in \mathbb{N} \rangle$ be a 1-1 sequence such that $Q = \{q_n : n \in \mathbb{N}\}$. A function h on a subset of P into Q is called a **partial isomorphism from P to Q** if $p \prec p'$ if and only if $h(p) < h(p')$, holds for all $p, p' \in \mathrm{dom} h$.
  - Claim: If h is a partial isomorphism from P to Q such that $\mathrm{dom} h$ is finite, and if $p \in P$ and $q \in Q$, then there is a partial isomorphism $h_{p,q} \supseteq h$ such that $p \in \mathrm{dom} h_{p,q}$ and $q \in \mathrm{ran} h_{p,q}$.
    Let $h = \{(p_{i_1}, q_{i_1}), \ldots, (p_{i_k}, q_{i_k})\}$, where $p_{i_1} \prec p_{i_2} \prec \cdots \prec p_{i_k}$ and, thus, also $q_{i_1} < q_{i_2} < \cdots < q_{i_k}$. If $p \notin \mathrm{dom} h$, we have either $p \prec p_{i_1}$, or $p_{i_e} \prec p \prec p_{i_e+1}$, for some $1 < e < k$, or $p_{i_k} \prec p$. Take the least natural number n such that q_n is in the same relationship to $q_{i_1}, \ldots, q_{i_k}$ as p is to to $p_{i_1}, \ldots, p_{i_k}$.

Countable Dense Linear Orders Without Endpoints II

- We continue with the proof of the Claim:

  More precisely, q_n is such that:

  - if $p \prec p_{i_1}$, then $q_n < q_{i_1}$;
  - if $p_{i_e} \prec p \prec p_{i_e+1}$, then $q_{i_e} < q_n < q_{i_e+1}$;
  - if $p_{i_k} \prec p$, then $q_{i_k} < q_n$.

  The possibility of doing this is guaranteed by the fact that $(Q, <)$ is a dense linear ordering without endpoints. Now $h' = h \cup \{(p, q_n)\}$ is a partial isomorphism. If $q \in \mathrm{ran} h'$, then we are done. If $q \notin \mathrm{ran} h'$, then by the same argument as before (with the roles of P and Q reversed), there is $p_m \in P$ such that $h' \cup \{(p_m, q)\}$ is a partial isomorphism. We take the least such m, and let $h_{p,q} = h' \cup \{(p_m, q)\}$.

We next construct a sequence of compatible partial isomorphisms by recursion: Set $h_0 = \emptyset$ and $h_{n+1} = (h_n)_{p_n, q_n}$, where $(h_n)_{p_n, q_n}$ is the extension of h_n (given by the claim) such that $p_n \in \mathrm{dom}(h_n)_{p_n, q_n}$ and $q_n \in \mathrm{ran}(h_n)_{p_n, q_n}$. Let $h = \bigcup_{n \in \mathbb{N}} h_n$. Then, $h : P \to Q$ is an isomorphism between $(P, \prec)$ and $(Q, <)$.

Universality Theorem

Theorem

Every countable linearly ordered set can be mapped isomorphically into any countable dense linearly ordered set without endpoints.

- Let $(P, \prec)$ be a countable linearly ordered set and let $(Q, <)$ be a countable dense linearly ordered set without endpoints. For every partial isomorphism h from the ordered set $(P, \prec)$ into Q and for every $p \in P$, we define a partial isomorphism $h_p \supseteq h$ such that $p \in \operatorname{dom} h_p$. Then we use recursion.

Subsection 5

Complete Linear Orderings

Gaps in Countable Dense Linear Orderings

- The usual ordering $<$ of the set $\mathbb{Q}$ of rational numbers is universal among countable linear orderings.
- However, when arithmetic operations on $\mathbb{Q}$ are considered, some things are missing:
  - For example, there is no rational number x such that $x^2 = 2$.
  - Another example of this phenomenon appears when one considers decimal representations of rational numbers. Every rational number has a decimal expansion that is either finite (e.g., $\frac{1}{4} = 0.25$) or infinite but periodic from some place onward (e.g., $\frac{1}{6} = 0.1666\ldots$).
    Although it is possible to write down decimal expansions $0.a_1a_2a_3\ldots$, where $\langle a_i \rangle_{i=1}^{\infty}$ is an arbitrary sequence of integers between 0 and 9, unless the sequence is finite or eventually periodic, there is no rational number x such that $x = 0.a_1a_2a_3\ldots$.
- It is clear from this discussion that the ordered set $(\mathbb{Q}, <)$ has gaps.

Gaps in Linearly Ordered Sets

Definition (Gap in Linearly Ordered Set)

Let $(P, <)$ be a linearly ordered set. A **gap** is a pair (A, B) of sets such that:

(a) A and B are nonempty disjoint subsets of P and $A \cup B = P$.

(b) If $a \in A$ and $b \in B$, then $a < b$.

(c) A does not have a greatest element and B does not have a least element.

- Example: Let $B = \{x \in \mathbb{Q} : x > 0 \text{ and } x^2 > 2\}$ and $A = \mathbb{Q} - B = \{x \in \mathbb{Q} : x < 0 \text{ or } (x > 0 \text{ and } x^2 < 2)\}$. It is not difficult to check that (A, B) is a gap in $\mathbb{Q}$.
- Similarly, an infinite decimal expansion which is not eventually periodic gives rise to a gap.

Gaps and Nonexistence of Suprema of Bounded Sets

- A nonempty subset of a linearly ordered set P is called **bounded** if it has both lower and upper bounds.
- A set is **bounded from above** (**from below**) if it has an upper (lower) bound.
- Let (A, B) be a gap in a linearly ordered set. The set A is bounded from above because any $b \in B$ is its upper bound.
  - Claim: A does not have a supremum.
    If c were a supremum of A, then either c would be the greatest element of A or the least element of B, as one can easily verify.
- Let S be a nonempty set, bounded from above. Let $A = \{x : x \leq s, \text{for some } s \in S\}$, $B = \{x : x > s, \text{for every } s \in S\}$. A and B satisfy Properties (a) and (b) in the definition of a gap. If S does not have a supremum, then (A, B) is a gap, since the greatest element of A or the least element of B wold be a supremum of S.

Complete Dense Linearly Ordered Sets

Definition (Complete Dense Linearly Ordered Set)

Let $(P, <)$ be a dense linearly ordered set. P is **complete** if every nonempty $S \subseteq P$ bounded from above has a supremum. Note that $(P, <)$ is complete if and only if it does not have any gaps.

- Not every dense linearly ordered set is complete.
- However, the following theorem guarantees that every dense linearly ordered set can be completed by "filling the gaps".
- Moreover, the result of this completion is essentially uniquely determined.

Completion of Dense Linear Orderings

Theorem (Completion of Dense Linear Orderings Without Endpoints)

Let $(P, <)$ be a dense linearly ordered set without endpoints. Then there exists a complete linearly ordered set $(C, \prec)$ such that

(a) $P \subseteq C$;

(b) If $p, q \in P$, then $p < q$ if and only if $p \prec q$ ($\prec$ agrees with $<$ on P);

(c) P is dense in C, i.e., for any $p, q \in P$, such that $p < q$, there is $c \in C$, such that $p \prec c \prec q$;

(d) C does not have endpoints.

Moreover, this complete linearly ordered set $(C, \prec)$ is unique up to isomorphism over P. I.e., if $(C^*, \prec^*)$ is a complete linearly ordered set which satisfies (a)-(d), then there is an isomorphism h between $(C, \prec)$ and $(C^*, \prec^*)$, such that $h(x) = x$, for all $x \in P$.
The linearly ordered set $(C, \prec)$ is called **the completion of** $(P, <)$.

Proof of Uniqueness

- Let $(C, \prec)$ and $(C^*, \prec^*)$ be two complete linearly ordered sets satisfying (a)-(d). We show there exists an isomorphism $h : C \to C^*$, such that $h(x) = x$, for all $x \in P$.

  If $c \in C$, let $S_c = \{p \in P : p \preccurlyeq c\}$. If $c^* \in C^*$, let $S_{c^*} = \{p \in P : p \preccurlyeq c^*\}$. If S is a nonempty subset of P bounded from above, let $\sup S$ be the supremum of S in $(C, \prec)$ and $\sup^* S$ the supremum of S in $(C^*, \prec^*)$. Then $\sup S_c = c$ and $\sup^* S_{c^*} = c^*$. Define h by $h(c) = \sup^* S_c$.

  h is a mapping of C into C^*.

  - h is onto C^*: Let $c^* \in C^*$. Then $c^* = \sup^* S_{c^*}$. Let $c = \sup S_{c^*}$. Then $S_c = S_{c^*}$ and $c^* = h(c)$.
  - If $c \prec d$ then $h(c) \prec^* h(d)$: If $c \prec d$, by density, there exists $p \in P$, such that $c \prec p \prec d$. Thus, $\sup^* S_c \prec^* p \prec^* \sup^* S_d$. Thus, $h(c) \prec^* h(d)$.
  - The preceding parts imply that h is an isomorphism.
  - $h(x) = x$, for all $x \in P$: If $x \in P$, then $x = \sup S_x = \sup^* S_x$, whence $h(x) = x$.

Cuts

- To prove existence, we introduce the notion of a Dedekind cut.

Definition (Cut)

A **cut** is a pair (A, B) of sets such that:

(a) A and B are disjoint nonempty subsets of P and $A \cup B = P$.

(b) If $a \in A$ and $b \in B$, then $a < b$.

- We recall that a cut is a gap if, in addition, A does not have a greatest element and B does not have a least element.
- Notice that since P is dense, it is not possible that both A has a greatest element and B has a least element.
  - Either B has a least element and A does not have a greatest element,
  - or A has a greatest element and B does not have a least element.

  In the first case, the supremum of A is the least element of B. In the second, the supremum of A is the greatest element of A.
- Hence, we consider only the first case and disregard other cuts.

Dedekind Cuts

Definition (Dedekind Cut)

A cut (A, B) is a **Dedekind cut** if A does not have a greatest element.

- We have two types of Dedekind cuts (A, B):
  (a) Those where $B = \{x \in P : x \geq p\}$, for some $p \in P$; we denote $(A, B) = [p]$.
  (b) Gaps.
- Consider the set C of all Dedekind cuts (A, B) in $(P, <)$ and order C as follows:
  $$(A, B) \preccurlyeq (A', B') \text{ if and only if } A \subseteq A'.$$
  $(C, \preccurlyeq)$ is a linearly ordered set.
- If $p, q \in P$ are such that $p < q$, then we have $[p] \prec [q]$. Thus, $(P', \prec)$, where $P' = \{[p] : p \in P\}$, is isomorphic to $(P, <)$.
- To show that $(C, \prec)$ is a completion of $(P', \prec)$, it suffices to prove
  (c') P' is dense in $(C, \prec)$;
  (d') C does not have endpoints;
  (e) $(C, \prec)$ is complete.

Existence of Completion I

(c') To show that P' is dense in C, let $c, d \in C$ be such that $c \prec d$. This means that $c = (A, B)$, $d = (A', B')$, and $A \subset A'$. Let $p \in P$ be such that $p \in A'$ and $p \notin A$. Moreover, we can assume that p is not the least element of B. Then $(A, B) \prec [p] \prec (A', B')$ and, hence, P' is dense in C. This also shows that $(C, \prec)$ is a densely ordered set.

(d') Similarly, if $(A, B) \in C$, then there is $p \in B$ that is not the least element of B, and we have $(A, B) \prec [p]$. Hence C does not have a greatest element. For analogous reasons, it does not have a least element.

(e) To show that C is complete, let S be a nonempty subset of C, bounded from above. Therefore, there is $(A_0, B_0) \in C$, such that $A \subseteq A_0$ whenever $(A, B) \in S$. To find the supremum of S, let

$$A_S = \bigcup\{A : (A, B) \in S\}, \quad B_S = P - A_S = \bigcap\{B : (A, B) \in S\}.$$

(A_S, B_S) is a cut. (B_S is nonempty because $B_0 \subseteq B_S$.)

Existence of Completion II

(e) To show that C is complete, we assumed S be a nonempty subset of C, bounded from above. Therefore, there is $(A_0, B_0) \in C$, such that $A \subseteq A_0$ whenever $(A, B) \in S$. To find the supremum of S, we let

$$A_S = \bigcup\{A : (A, B) \in S\}, \quad B_S = P - A_S = \bigcap\{B : (A, B) \in S\}.$$

(A_S, B_S) is a cut. (B_S is nonempty because $B_0 \subseteq B_S$.)
In fact, (A_S, B_S) is a Dedekind cut: A_S does not have a greatest element since none of the A's does.
Since $A_S \supseteq A$ for each $(A, B) \in S$, (A_S, B_S) is an upper bound of S. Let us show that (A_S, B_S) is the least upper bound of S. If $(\overline{A}, \overline{B})$ is any upper bound of S, then $A \subseteq \overline{A}$ for all $(A, B) \in S$, and, so, $A_S = \bigcup\{A : (A, B) \in S\} \subseteq \overline{A}$. Hence, $(A_S, B_S) \preccurlyeq (A, B)$. Thus (A_S, B_S) is the supremum of S.

The Reals as the Completion of the Rationals

- The ordered set $(\mathbb{Q}, <)$ of rationals has a unique completion (up to isomorphism); this is the ordered set of real numbers. The ordering of reals coincides with $<$ on $\mathbb{Q}$, so we use $<$ (rather than $\prec$) for it.

Definition (Real Numbers)

The completion of $(\mathbb{Q}, <)$ is denoted $(\mathbb{R}, <)$; the elements of $\mathbb{R}$ are the **real numbers**.

Theorem

$(\mathbb{R}, <)$ is the unique (up to isomorphism) complete linearly ordered set without endpoints that has a countable subset dense in it.

- Let $(C, \prec)$ be a complete linearly ordered set without endpoints, and let P be a countable subset of C dense in C. Then $(P, \prec)$ is isomorphic to $(\mathbb{Q}, <)$. By the uniqueness of completion, $(C, \prec)$ is then isomorphic to the completion of $(\mathbb{Q}, <)$. Thus, $(C, \prec)$ is isomorphic to $(\mathbb{R}, <)$.

Subsection 6

Uncountable Sets

Uncountability of $\mathbb{R}$

- Georg Cantor proved that uncountable sets exist.
- This discovery provided an impetus for the development of set theory and became a source of its depth and richness.

Theorem (Uncountability of $\mathbb{R}$)

The set $\mathbb{R}$ of all real numbers is uncountable.

- $(\mathbb{R}, <)$ is a dense linear ordering without endpoints. If $\mathbb{R}$ were countable, by a preceding theorem, $(\mathbb{R}, <)$ would be isomorphic to $(Q, <)$. But this is not possible because $(\mathbb{R}, <)$ is complete and $(\mathbb{Q}, <)$ is not.
- This proof relies on the theory of linear orderings.
- Cantor's original proof used his famous "diagonalization argument".

Cantor's Diagonalization Argument

Theorem (Uncountability of $\mathbb{R}$)

The set $\mathbb{R}$ of all real numbers is uncountable.

- Assume that $\mathbb{R}$ is countable, i.e., $\mathbb{R}$ is the range of some infinite sequence $\langle r_n \rangle_{n=1}^{\infty}$. Let $a_0^{(n)}.a_1^{(n)}a_2^{(n)}\ldots$ be the decimal expansion of r_n. (We assume that a decimal expansion does not contain only the digit 9 from some place on, so each real number has a unique decimal expansion.) Let
$$b_n = \begin{cases} 1, & \text{if } a_n^{(n)} = 0 \\ 0, & \text{otherwise} \end{cases}.$$
Let r be the real number whose decimal expansion is $0.b_1b_2b_3\ldots$. We have $b_n \neq a_n^{(n)}$, hence, $r \neq r_n$, for all $n = 1, 2, 3, \ldots$, a contradiction.

Uncountability of the Power Set of $\mathbb{N}$

Theorem

The set of all sets of natural numbers is uncountable; in fact, $|\mathcal{P}(\mathbb{N})| > |\mathbb{N}|$.

- The function $f : \mathbb{N} \to \mathcal{P}(\mathbb{N})$ defined by $f(n) = \{n\}$ is one-to-one, so $|\mathbb{N}| \leq |\mathcal{P}(\mathbb{N})|$.
  We prove that for every sequence $\langle S_n : n \in \mathbb{N} \rangle$ of subsets of $\mathbb{N}$ there is some $S \subseteq \mathbb{N}$ such that $S \neq S_n$, for all $n \in \mathbb{N}$. This shows that there is no mapping of $\mathbb{N}$ onto $\mathcal{P}(\mathbb{N})$, and hence $|\mathbb{N}| < |\mathcal{P}(\mathbb{N})|$. We define the set $S \subseteq \mathbb{N}$ as follows:

$$S = \{n \in \mathbb{N} : n \notin S_n\}.$$

  The number n is used to distinguish S from S_n:
  - If $n \in S_n$, then $n \notin S$.
  - If $n \notin S_n$, then $n \in S$.

  In either case, $S \neq S_n$, as required.

Uncountability of $\mathbb{R}$

- We prove that the set $2^{\mathbb{N}} = \{0,1\}^{\mathbb{N}}$ of all infinite sequences of 0's and 1's is also uncountable. In fact, it has the same cardinality as $\mathcal{P}(\mathbb{N})$ and $\mathbb{R}$.

Theorem

$|\mathcal{P}(\mathbb{N})| = |2^{\mathbb{N}}| = |\mathbb{R}|$.

- For each $S \subseteq \mathbb{N}$ define the characteristic function of S, $\chi_S : \mathbb{N} \to \{0,1\}$: $\chi_S(n) = \begin{cases} 0, & \text{if } n \in S \\ 1, & \text{if } n \notin S \end{cases}$. It is easy to check that the correspondence between sets and their characteristic functions is a one-to-one mapping of $\mathcal{P}(\mathbb{N})$ onto $\{0,1\}^{\mathbb{N}}$.
- To complete the proof, we show that $|\mathbb{R}| \leq |\mathcal{P}(\mathbb{N})|$ and also $|2^{\mathbb{N}}| \leq |\mathbb{R}|$ and use the Cantor-Bernstein Theorem.

Uncountability of $\mathbb{R}$ (Cont'd)

- We first show that $|\mathbb{R}| \leq |\mathcal{P}(\mathbb{N})|$ and, then, $|2^{\mathbb{N}}| \leq |\mathbb{R}|$
  (a) We have constructed real numbers as cuts in the set $\mathbb{Q}$ of all rational numbers. The function that assigns to each real number $r = (A, B)$ the set $A \subseteq \mathbb{Q}$ is a one-to-one mapping of $\mathbb{R}$ into $\mathcal{P}(\mathbb{Q})$. Therefore, $|\mathbb{R}| \leq |\mathcal{P}(\mathbb{Q})|$. As $|\mathbb{Q}| = |\mathbb{N}|$, we have $|\mathcal{P}(\mathbb{Q})| = |\mathcal{P}(\mathbb{N})|$. Hence $|\mathbb{R}| \leq |\mathcal{P}(\mathbb{N})|$.
  (b) To prove $|\mathcal{P}(\mathbb{N})| \leq |\mathbb{R}|$ we use the decimal representation of real numbers. The function that assigns to each infinite sequence $\langle a_n \rangle_{n=0}^{\infty}$ of 0's and 1's the unique real number whose decimal expansion is $0.a_0 a_1 a_2 \ldots$ is a one-to-one mapping of $2^{\mathbb{N}}$ into $\mathbb{R}$. Therefore, we have $|2^{\mathbb{N}}| \leq |\mathbb{R}|$.

  The Cantor-Bernstein Theorem asserts that $|\mathbb{R}| = |\mathcal{P}(\mathbb{N})| = |2^{\mathbb{N}}|$.
- We introduced $\aleph_0$ as a notation for the cardinal of $\mathbb{N}$. Due to the theorem, the cardinal number of $\mathbb{R}$ is usually denoted $2^{\aleph_0}$. The set $\mathbb{R}$ of all real numbers is also referred to as "the continuum"; for this reason, $2^{\aleph_0}$ is called the **cardinality of the continuum**. In this notation, Cantor's Theorem says that $\aleph_0 < 2^{\aleph_0}$.