NOTES ON INFINITE SETS AND CARDINALITY

Last update: Wednesday, Sep. 3

Suppose A and B are sets. We say that $|A| \geq |B|$ (the *cardinality* of A is greater or equal to the cardinality of B) if there exists an infective mapping $f : B \to A$. We say that $|A| = |B|$ (A and B are *equipollent*) if $|A| \geq |B|$ and $|A| \leq |B|$.

Theorem 1 (Cantor-Schroeder-Bernstein)**.** *The sets A and B are equipollent if and only if there exists a bijection from A to B.*

Proof. Suppose $f : A \to B$ and $g : B \to A$ are injections. We shall construct a bijection $h : A \to B$, using "pieces" of f and g^{-1} (here, we view g^{-1} as a function from $g(B)$ to B).

Let $C_0 = A \backslash g(B)$. For $k \in \mathbb{N}$, let $C_k = g(f(C_k))$. Finally, let $C = \cup_{k=0}^{\infty} C_k$. Note that the sets C_k are mutually disjoint. Indeed, $C_0 \cap g(B) = \emptyset$, hence $C_0 \cap C_k = \emptyset$ for each k. Let $S = \{k \geq 0 : C_k \cap \cup_{i>k} C_i \neq \emptyset\}$. Note that $C_0 \cap g(B) = \emptyset$, hence $C_0 \cap C_i = \emptyset$ for each i, and therefore, $0 \notin S$. Let m be the least element of S. We shall show that $m - 1 \in S$, thus obtaining a contradiction. Indeed, suppose $a \in C_m \cap C_i$, for some $i > m$. Then $a = g(f(a_0))$, where a_0 belongs to both C_{m-1} and C_{i-1}.

Now define $h : A \to B$ by setting $h(a) = f(a)$ if $a \in C$, and $h(a) = g^{-1}(a)$ if $a \notin C$ (note that $A \backslash C \subset g(B)$, hence h is well-defined. It remains to show that h is both injective and surjective.

Injectivity. Suppose $a_1, a_2 \in A$ satisfy $h(a_1) = h(a_2)$, and show that $a_1 = a_2$. If both a_1 and a_2 belong to C, then we have $f(a_1) = f(a_2)$, hence $a_1 = a_2$ by the injectivity of f. The case of $a_1, a_2 \notin C$ is handled similarly. Now suppose $a_1 \in C$, and $a_2 \notin C$. By the definition of C, $a_1 \in C_k$ for some $k \geq 0$. Then $h(a_1) = f(a_1) = g^{-1}(a_2)$, hence $a_2 = g(f(a_1))$, which implies $a_2 \in C_{k+1}$, yielding a contradiction.

Injectivity. We have to show that, for every $b \in B$, there exists $a \in A$ s.t. $b = h(a)$. For $b \in f(C)$, $a = f^{-1}(b)$ will do. Show that, for $b \notin f(C)$, $g(b) \notin C$. Indeed, otherwise $g(b) \in C_k$ for some $k \in \mathbb{N}$. But g is injective, hence $b = f(a)$, for some $a \in C_{k-1}$. This is impossible. Thus, $h(a) = b$ for $a = g(b)$. ■

In class, we proved that $\mathbb{Z}$ is countable. Now we establish:

Proposition 2. *The set $\mathbb{Q}$ is countable.*

Sketch of the proof. By Theorem 1, we have to establish the existence of bijections $f : \mathbb{N} \to \mathbb{Q}$ and $g : \mathbb{Q} \to \mathbb{N}$. f is easy to construct. Moreover, any non-zero rational number r has a unique representation as $r = p/q$, where $p \in \mathbb{Z} \backslash \{0\}$, $q \in \mathbb{N}$, and p, q are coprime. This defines an injection from $\mathbb{Q}$ to $\mathbb{Z} \times \mathbb{Z}$, which, in turn, can be mapped injectively to $\mathbb{N} \times \mathbb{N}$. We showed in class that there exists a bijection between $\mathbb{N}$ and $\mathbb{N} \times \mathbb{N}$. ■

In general, denumerable sets are the “smallest” infinite sets.

Proposition 3. *If A is an infinite set, then $|A| \geq |\mathbb{N}|$.*

Proof. Suppose A is an infinite set with $|A| \leq |\mathbb{N}$, and show that $|A| = |\mathbb{N}|$. Indeed, there exists a bijection $f : A \to A_1 \subset \mathbb{N}$. By the properties of $\mathbb{N}$, A_1 has the lest element, which we call k_1. Then the set $A_2 = A_1 \backslash \{k_1\}$ has the least element $k_2 > k_1$. Define $A_3 = A_2 \backslash \{k_2\}$. Proceeding further in the same manner, we obtain a sequence $k_1 < k_2 < \ldots$ in A_1 (for every m, the set A_m is non-empty, for otherwise, A will have to be finite). Then the map $g : \mathbb{N} \to A_1 : n \mapsto k_n$ is a injection (in fact, it's a bijection, but we do not need this). Therefore, $f^{-1} \circ g : \mathbb{N} \to A$ is an injection, hence $|\mathbb{N}| \leq |A|$. ■

We say that $|A| > |B|$ if $|A| \geq |B|$, and $|A| \neq |B|$.

Recall that the *power set* of A (denoted by $\mathcal{P}(A)$) is set of all its subsets.

Theorem 4 (Cantor). *For any set A, $|\mathcal{P}(A)| > |A|$.*

Remark 5. Elementary combinatorics shows that $|\mathcal{P}(A)| = 2^|A|$ if A is a finite set.

Sketch of the proof of Theorem 4. Consider $f : A \to \mathcal{P}(A)$. Let $X = \{a \in A : a \notin f(a)\}$. Then there is no $x \in A$ s.t. $f(x) = X$. To see this, consider the cases of $x \in X$ and $x \notin X$, obtaining a contradiction in each case. ■

Denote by $2^{\mathbb{N}}$ the set of all sequences of 0s and 1s. It can be identified with $\mathcal{P}(\mathbb{N})$. By the above, the set $2^{\mathbb{N}}$ is uncountable.

Proposition 6. *The sets $2^{\mathbb{N}}$ and $(0, 1)$ are equipollent.*

It was shown in class that $\mathbb{R}$ is equipollent with $(0, 1)$. Therefore:

Corollary 7. *$\mathbb{R}$ is uncountable.*

Sketch of the proof of Proposition 6. By Theorem 1, it suffices to exhibit the injections from $2^{\mathbb{N}}$ to $[0, 1]$, and back.

Define $f : 2^{\mathbb{N}} \to [0, 1]$: for $a = (a_1, a_2, \ldots)$, where a_k is either 0 or 1. Set $f(a) = \sum_{k=1}^{\infty} 3^{-k} a_k$. We show that, if $a = (a_1, a_2, \ldots)$ and $b = (b_1, b_2, \ldots)$ are such that $a_k = b_k$ for $k < n$, and $a_n > b_n$, then $f(a) > f(b)$. Indeed,

$$f(a) - f(b) = \sum_{k=n}^{\infty} 3^{-k}(a_k - b_k) = 3^{-n} + \sum_{k=n+1}^{\infty} 3^{-k}(a_k - b_k) \geq 3^{-n} - \sum_{k=n+1}^{\infty} 3^{-k} = \frac{3^{-n}}{2} > 0.$$

Define $g : [0, 1] \to 2^{\mathbb{N}}$. Any $x \in (0, 1]$ can be written in a unique way as $x = \sum_{k=1}^{\infty} 2^{-k} a_k$, where (a_k) is a sequence of 0s and 1s, with infinitely many 1s (see the section on binary expansions in the book). Set $g(a) = (a_1, a_2, \ldots)$ for $a \neq 0$, and $g(0) = (0, 0, \ldots)$. ■

Back to: the syllabus, the main page of the course.