THEORY OF COMPUTATION
Recursively Enumerable Sets - 12 part 3

Prof. Dan A. Simovici

UMB

Diagonalization is a proof technique broadly used for constructing counter examples.

We discuss diagonalization in two contexts:

- proving that certain sets are not countable, and
- proving that certain sets are not r.e.

Definition

Two sets, A, B have the same *cardinality*, written $A \sim B$, if there exists a bijection $f : A \longrightarrow B$.

Example

The set of even numbers, $E = \{n \mid n = 2k, \text{ for some } k \in \mathbb{N}\}$ and the set $\mathbb{N}$ have the same cardinality, because $f : \mathbb{N} \longrightarrow E$ defined by $f(n) = 2n$ is a bijection.

Theorem

The relation $\sim$ *is an equivalence relation.*

Proof.

For every set A, $1_A : A \longrightarrow A$ is a bijection. Therefore, $A \sim A$ for every A, so $\sim$ is reflexive. If $f : A \longrightarrow B$ is a bijection, then $f^{-1} : B \longrightarrow A$ is a bijection, so $A \sim B$ implies $B \sim A$, which shows that $\sim$ is symmetric. Transitivity follows from the fact that the composition of two bijections is a bijection. $\square$

Theorem

If $A \sim B$, then $\mathcal{P}(A) \sim \mathcal{P}(B)$.

Proof.

Let $f : A \longrightarrow B$ be a bijection between A and B. Define the mapping $F : \mathcal{P}(A) \longrightarrow \mathcal{P}(B)$ by
$F(L) = \{b \in B \mid b = f(a) \text{ for some } a \in L\}$ for every $L \in \mathcal{P}(A)$. It is easy to verify that F is a bijection. Thus, $\mathcal{P}(A) \sim \mathcal{P}(B)$. □

Definition

A set A is *countable* if it has the same cardinality as a subset of $\mathbb{N}$. A is *finite* if there is an integer $k \in \mathbb{N}$ such that A has the same cardinality as a subset of $\{0, 1, \ldots, k-1\}$.

Note that any finite set is countable.

Theorem

If A is finite, then there is a unique $k \in \mathbb{N}$ for which $A \sim \{0, 1, \ldots, k-1\}$. In this case, we write $|A| = k$ and say that "A has k elements."

Proof.

Assume A is finite. Let $M = \{m \in \mathbb{N} \mid A$ has the same cardinality as some subset of $\{0, 1, \ldots, m-1\}\}$. Since A is finite, $M \neq \emptyset$, so M has a least element, k, which clearly satisfies the requirements of the theorem. □

Often it is desirable to be able explicitly to enumerate the elements of A. If A is finite, with $|A| = k$, then there is a bijection $f : \{0, 1, \ldots k-1\} \longrightarrow A$, and we can enumerate $A = \{a_0, a_1, \ldots, a_{k-1}\}$, where $a_i = f(i)$.
If A is infinite but countable, we write $|A| = \aleph_0$ and say "A is countably infinite." [1] The following theorem permits us to enumerate countably infinite sets.

[1] The symbol $\aleph$ (pronounced "aleph") is the first letter of the Hebrew alphabet. This notation is standard in set theory.

Theorem

If $|A| = \aleph_0$, then there is a bijection $f : \mathbb{N} \longrightarrow A$.

Proof.

Since A is countable, there is a bijection $g : A \longrightarrow S \subseteq \mathbb{N}$. To define $f : \mathbb{N} \longrightarrow A$ inductively, we simultaneously define both f and a subset of S. Let $f(0) = g^{-1}(s_0)$, where s_0 is the smallest element in S. Assume $\{f(0), f(1), \ldots f(k-1)\}$ and $\{s_0, s_1, \ldots s_{k-1}\}$ have been defined. Then define $f(k) = g^{-1}(s_k)$, where s_k is the smallest element in $S - \{s_0, s_1, \ldots s_{k-1}\}$. Since A is infinite, S is also infinite, so $S - \{s_0, s_1, \ldots s_{k-1}\} \neq \emptyset$, and a smallest element always exists. □

Proof cont'd

Proof.

By construction, if $m_0 < m_1$ then $f(m_1) \notin \{f(0), f(1), \dots f(m_0)\}$, since g is a bijection (and hence g^{-1} is, too.) So, if $f(m_0) = f(m_1)$ then clearly $m_0 = m_1$. We have to check that f is also onto. An easy induction shows that $s_k \geqslant k$, for all $k \in \mathbb{N}$. Let $a \in A$, with $g(a) = m$. Then, $m = s_j$ for some $j \leqslant m$, so $f(s_j) = a$. □

Corollary

If $|A| = \aleph_0$*, then there is a bijection* $g : A \longrightarrow \mathbb{N}$*.*

Proof.

This follows from the fact that the inverse of a bijection is again a bijection. □

If A is countably infinite, then we can "enumerate" A using the the bijection previously defined. Thus, we have

$$A = \{a_0, a_1, a_2, \ldots\},$$

where, just as in the finite case, $a_i = f(i)$.

Next we give a useful characterization of countable sets.

Theorem

A set A is countable if and only if there exists an injection $f : A \longrightarrow \mathbb{N}$.

Proof.

The necessity of the condition is immediate since every bijection is also an injection. Suppose, therefore, that $f : A \longrightarrow \mathbb{N}$ is an injection. Then, the function $g : A \longrightarrow \text{Ran}(f)$ is obviously a bijection between A and $\text{Ran}(f)$, a subset of $\mathbb{N}$, so A is indeed countable. □

Theorem

Let A, B be two countable sets. Then, $A \cup B$ is countable.

Proof.

Assume A, B are two countable sets, and let $f : A \longrightarrow \mathbb{N}$ and $g : B \longrightarrow \mathbb{N}$ be injections. Define $h : A \cup B \longrightarrow \mathbb{N}$ by

$$h(x) = \begin{cases} 2f(x) & \text{if } x \in A - B \\ 2g(x) + 1 & \text{if } x \in B. \end{cases}$$

The function $h : A \cup B \longrightarrow \mathbb{N}$ is easily seen to be an injection; hence, $A \cup B$ is countable. □

Corollary

The union of any finite collection of countable sets is countable.

Theorem

Let A, B, C be sets, where A is countable.

1. *If there is a surjection $f : A \longrightarrow B$, then B is countable.*
2. *If there is an injection $\ell : C \longrightarrow A$, then C is countable.*

Proof.

For the first part of the theorem assume A is countable and $f : A \longrightarrow B$ is a surjection. Since A is countable, there is an injection $g : A \longrightarrow \mathbb{N}$. Define $h : B \longrightarrow \mathbb{N}$ by

$$h(b) = \min\{g(a) \mid f(a) = b\}.$$

We need to verify that h is an injection. Let $b_0, b_1 \in B$ such that $h(b_0) = h(b_1)$. Let $a_i \in A$ be the element such that $h(b_i) = g(a_i)$ for $i = 0, 1$. Then, $g(a_0) = g(a_1)$, and since g is an injection, $a_0 = a_1$, so $f(a_0) = f(a_1)$, and thus $b_0 = b_1$.
For the second part note that the function $g\ell : C \longrightarrow \mathbb{N}$ is an injection; this implies immediately the countability of C. □

Corollary

Let A, B be two sets. If $f : A \longrightarrow B$ is a bijection, then A is countable if and only if B is countable.

Corollary

Any subset of a countable set is countable.

Proof.

Assume $B \subseteq A$, where A is countable. If $B = \emptyset$, then it is clearly countable. If $B \neq \emptyset$, pick $b \in B$, and define $f : A \longrightarrow B$ by

$$f(x) = \begin{cases} x & \text{if } x \in B \\ b & \text{if } x \notin B. \end{cases}$$

The function f is clearly a surjection, so B is countable. □

Theorem

Let $A_0, \ldots, A_{n-1}$ be n countable sets. The Cartesian product $A_0 \times \cdots \times A_{n-1}$ is countable.

Proof.

Since $A_0, \ldots, A_{n-1}$ are countable sets, there exist injections $f_i : A_i \longrightarrow \mathbb{N}$ for $0 \leqslant i \leqslant n-1$. For $(a_0, \ldots, a_{n-1}) \in A_0 \times \cdots \times A_{n-1}$, define

$$h(a_0, \ldots, a_{n-1}) = 2^{f_0(a_0)} \cdot 3^{f_1(a_1)} \cdot \cdots \cdot p_{n-1}^{f_{n-1}(a_{n-1})},$$

where p_{i-1} is the i^{th} prime number for $0 \leqslant i \leqslant n-1$. Since each natural number larger than one can be written uniquely as a product powers of primes, $h : A_0 \times \cdots \times A_{n-1} \longrightarrow \mathbb{N}$ is an injection, so $A_0 \times \cdots \times A_{n-1}$ is countable. □

Example

Let D be a countable set. The set $\mathbf{Seq}_n(D) = D^n$ is a countable set for every $n \in \mathbb{N}$.

Theorem

The union of a countable collection of countable sets that are pairwise disjoint, is a countable set.

Proof.

Let K be a countable set, and let each $\{A_k \mid k \in K\}$ be countable. Then there are injections $f : K \longrightarrow \mathbb{N}$ and $g_k : A_k \longrightarrow \mathbb{N}$ for each $k \in K$. Assume that $A_i \cap A_j = \emptyset$ for $i \neq j \in K$. To show that

$$A = \bigcup_{k \in K} A_k \text{ is countable,}$$

we define an injection $h : A \longrightarrow \mathbb{N}$. □

Proof cont'd

Proof.

Let $P = \{p_0, p_1, \ldots\}$ be an enumeration of the prime numbers. Since the sets A_k are pairwise disjoint, given any $a \in A$, there is a unique k with $a \in A_k$. We use this fact to define

$$h(a) = p_{f(k)}^{g_k(a)}.$$

It follows from the Fundamental Theorem of Arithmetic that h is an injection, and thus A is countable. □

Corollary

The union of a countable collection of countable sets is a countable set.

Proof.

Let L be a countable set, and let each $\{A_l \mid l \in L\}$ be countable. Form sets $A'_l = A_l \times \{l\}$. These are clearly pairwise disjoint, so

$$A' = \bigcup_{l \in L} A'_l \text{ is countable.}$$

Let

$$A = \bigcup_{l \in L} A_l.$$

The projection $u_1^2 : A' \longrightarrow A$ is a surjection, and thus A is countable. □

Example

We proved that if D is a countable set, $\mathbf{Seq}_n(D)$ is countable. Therefore, $\mathbf{Seq}(D) = \bigcup\{D^n \mid n \in \mathbb{N}\}$ is countable as a union of a countable collection of sets.

The set $\mathbb{N} \times \mathbb{N}$ is countably infinite, so there exists a bijection $\wp : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$. We saw that $\langle x, y \rangle$ is a pairing function, that is, a bijection $\langle x, y \rangle : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$. An alternative bijection is suggested by the following picture:

	0	1	2	3	$\cdots$
0	0	1	3	6	$\iddots$
1	2	4	7	$\iddots$	
2	5	8	$\iddots$		
3	9	$\iddots$			
$\vdots$					

Let D_m be the diagonal that contains all pairs (i, j) such that $i + j = m$. It is clear that D_m contains $m + 1$ pairs.
Note that the pair (i, j) is located on the diagonal D_{i+j} and that this diagonal is preceded by the diagonals $D_0, \ldots, D_{i+j-1}$ that have a total of $1 + 2 + \cdots + (i + j) = (i + j)(i + j + 1)/2$ elements.
Thus, the pair (i, j) is enumerated on the place $(i + j)(i + j + 1)/2 + i$ and this shows that the mapping $h : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ given by

$$\wp(i, j) = \frac{1}{2}[(i + j)^2 + 3i + j]$$

is a bijection.

It is important to realize that not all sets are countable. Consider $\mathcal{P}(\mathbb{N})$, the power set of $\mathbb{N}$. This certainly has at least as many elements as $\mathbb{N}$, since $\{k\}$ is in $\mathcal{P}(\mathbb{N})$ for each $k \in \mathbb{N}$. However, it has so many more sets that it is not possible to count them all, that is, to arrange all these sets in a list.

Theorem

The set $\mathcal{P}(\mathbb{N})$ is not countable.

Proof.

Assume that $\mathcal{P}(\mathbb{N})$ were countable. Then there would be an bijection $f : \mathbb{N} \longrightarrow \mathcal{P}(\mathbb{N})$; i.e., for each $n \in \mathbb{N}$, we would have a distinct subset $f(n) \subseteq \mathbb{N}$.

We show that the existence of this bijection leads to a contradiction. Define the set $D = \{n \mid n \notin f(n)\}$. Clearly, $D \subseteq \mathbb{N}$, so we must have $D = f(k)$ for some $k \in \mathbb{N}$. We must now have one of two situations: either $k \in D$, or $k \notin D$. □

First, suppose that $k \in D$. Then, by the definition of D, $k \notin f(k)$, but $f(k) = D$, so we have that $k \in D$ implies that $k \notin D$; this cannot be.
Suppose, on the other hand, that $k \notin D$. Then, by the definition of D, $k \in f(k)$, and since $f(k) = D$, we have $k \notin D$ implies $k \in D$. Again, this cannot be. Either way, we have a contradiction. From this, we necessarily conclude that the assumed bijection f cannot exist.

An important way to regard this proof is the following. If there were a bijection $f : \mathbb{N} \longrightarrow \mathcal{P}(\mathbb{N})$, then we could have the following list:

$$\begin{array}{ll}
0: & a_{00}\ a_{01}\ a_{02}\ a_{03}\ a_{04} \ldots \\
1: & a_{10}\ a_{11}\ a_{12}\ a_{13}\ a_{14} \ldots \\
2: & a_{20}\ a_{21}\ a_{22}\ a_{23}\ a_{24} \ldots \\
3: & a_{30}\ a_{31}\ a_{32}\ a_{33}\ a_{34} \ldots \\
4: & a_{40}\ a_{41}\ a_{42}\ a_{43}\ a_{44} \ldots \\
5: & a_{50}\ a_{51}\ a_{52}\ a_{53}\ a_{54} \ldots \\
 & \vdots \\
k: & a_{k0}\ a_{k1}\ a_{k2}\ a_{k3}\ a_{k4} \ldots a_{kk}
\end{array}$$

where

$$a_{ij} = \begin{cases} 0 & \text{if } j \notin f(i) \\ 1 & \text{if } j \in f(i). \end{cases}$$

The set D is formed by "going down the diagonal" and spoiling the possibility that $D = f(k)$, for each k.
At row k, we look at a_{kk} in column k. If this is 1, i.e., if $k \in f(k)$, then we make sure that the corresponding position for the set D has a 0 in it by saying that $k \notin D$.
On the other hand, if a_{kk} is a 0, i.e., $k \notin f(k)$, then we force the corresponding position for the set D to be a 1 by putting k into D.
This guarantees that $D \neq f(k)$, because its characteristic functions differs from that of $f(k)$ in column k.

$$
\begin{array}{ll}
0: & \overline{a_{00}}\ a_{01}\ a_{02}\ a_{03}\ a_{04}\ \ldots \\
1: & a_{10}\ \overline{a_{11}}\ a_{12}\ a_{13}\ a_{14}\ \ldots \\
2: & a_{20}\ a_{21}\ \overline{a_{22}}\ a_{23}\ a_{24}\ \ldots \\
3: & a_{30}\ a_{31}\ a_{32}\ \overline{a_{33}}\ a_{34}\ \ldots \\
4: & a_{40}\ a_{41}\ a_{42}\ a_{43}\ \overline{a_{44}}\ \ldots \\
5: & a_{50}\ a_{51}\ a_{52}\ a_{53}\ a_{54}\ \ldots \\
 & \vdots \\
k: & a_{k0}\ a_{k1}\ a_{k2}\ a_{k3}\ a_{k4}\ \ldots\ \overline{a_{kk}}
\end{array}
$$

This proof technique, usually referred to as *diagonalization*, first appeared in an 1891 paper of Georg Cantor (1845–1918); it has found many applications in the theory of computation.

Example

Let F_2 be the set of all functions of the form $f : \mathbb{N} \longrightarrow \{0, 1\}$. Define the mapping $\phi : F_2 \longrightarrow \mathcal{P}(\mathbb{N})$ by $\phi(f) = \{n \in \mathbb{N} \mid f(n) = 1\}$. The function ϕ is a bijection. Indeed, suppose that $\phi(f) = \phi(g)$, that is $\{n \in \mathbb{N} \mid f(n) = 1\} = \{n \in \mathbb{N} \mid g(n) = 1\}$. This means that $f(n) = 1$ if and only if $g(n) = 1$ for $n \in \mathbb{N}$, so $f = g$, which means that ϕ is an injection.

Example cont'd

Example

To prove that ϕ is a bijection consider an arbitrary subset K of $\mathbb{N}$. Then, for its characteristic function f_K (given by $f_K(n) = 1$ if $n \in K$ and $f_K(n) = 0$, otherwise) we have $\phi(f_K) = K$, so ϕ is also a surjection, and therefore, a bijection. Thus, we conclude that the set F_2 is not countable.
If F is the set of functions of the form $f : \mathbb{N} \longrightarrow \mathbb{N}$, then the uncountability of F_2 implies the uncountability of F.