Discrete Mathematics

Unit 1- Theorems

Schroeder-Bernstein's Theorem

Given two sets X and Y , we will write X ∼ Y to denote the existence of a bijection from X to Y . One easily checks that ∼ is transitive, i.e. if X ∼ Y and Y ∼ Z, then X ∼ Z. The purpose of this note is to prove the following result:

Theorem 1 (Cantor-Schroder-Bernstein) - If f : A → B and g : B → A are both injections, then A ∼ B.

In other words, the theorem states that if A and B are sets, and there are injections $f : A \to B$ and $g : B \to A$, then there is a bijection $h : A \to B$.

Here's the strategy of the proof : First, we apply f to all of A to obtain a set B1 ⊆ B. Next, apply g to all of B1 to get a set A2 ⊆ A. Iterating this, we keep bouncing back and forth between smaller and smaller subsets of A and B until the process stabilizes and we end up with some sets A ⊆ A and B ⊆ B for which f(A) = B and g(B) = A. This implies that A ∼ B. The next task is to show that A − A ∼ B − B, which turns out to be not so hard. Finally, we conclude that A ∼ B.

PROOF OUTLINE

1. We may assume that A and B are disjoint.

2. For x in A, form the sequence x0 = x, x1 = g −1 (x0), x2 = f −1 (x1), x3 = g −1 (x2), ...

3. Note that the even-indexed terms lie in A and the odd-indexed terms lie in B.

4. For each x in A, two scenarios are possible:

(a) For some n, xn+1 does not exist and the sequence terminates. In this case, n is said to be the order of x.

(b) The sequence {xn} is infinite (perhaps, periodic). The order of x is then said to be infinite.

5. Observe that A is a union of three disjoint subsets, Aodd, Aeven, and A∞, consisting of elements of respectively odd, even, and infinite order.

6. Similarly, B is a disjoint union of Bodd, Beven, and B∞.

7. Observe that f maps Aeven onto Bodd, and A∞ onto B∞.

8. Observe that g maps Beven onto Aodd.

9. Conclude that x 7→ (f(x), x ∈ Aeven ∪ A∞ g −1 (x), x ∈ Aodd is a bijection A → B.

The Well-Ordering Principle

The well-ordering principle says that the positive integers are **well-ordered.** An **ordered set** is said to be **well-ordered** if each and every nonempty subset has a smallest or least element.

- Note that this property is not true for subsets of the integers (in which there are arbitrarily small negative numbers) or the positive real numbers (in which there are elements arbitrarily close to zero).
- Well-ordering principle states that The set N is well-ordered.
- Example. The following sets are well-ordered:

(1) $N \cup \{0\}$

(2) $N \cup \{-1, 0\}$

(3) $N \cup \{-3, -2, -1\}$

(4) $\{n \in N : n > 5\}$

- Example. The following sets are NOT well-ordered.

(1) R (the open interval (0, 2) is a non-empty subset of R but it has no smallest element)

(2) Z (the set of negative integers is a non-empty subset of Z but with no smallest element)

(3) the interval [0, 1] (because (0, 1) is a non-empty subset of [0, 1] without smallest element)

Recursive Definition

A ***recursive definition*** (sometimes called an ***inductive definition***) for a sequence $(a_n)_{n\in\mathbb{N}}$ consists of a ***recurrence relation***: an equation relating a term of the sequence to previous terms (terms with smaller index) and an ***initial condition***: a list of a few terms of the sequence (one less than the number of terms in the recurrence relation).

Here are a few recursive definitions for sequences:

- $a_n = 2a_{n-1}$ with $a_0 = 1$.
- $a_n = 2a_{n-1}$ with $a_0 = 27$.
- $a_n = a_{n-1} + a_{n-2}$ with $a_0 = 0$ and $a_1 = 1$.

In these cases, if you are given n, you cannot calculate a_n directly, you first need to find a_{n-1} (or a_{n-1} and a_{n-2}).

The division algorithm

The division algorithm for integers states that given any two integers *a* and *b*, with $b > 0$, we can find integers *q* and *r* such that $0 \leq r < b$ and $a = bq + r$.

The numbers *q* and *r* should be thought of as the quotient and remainder that result when *b* is divided into *a*. Of course the remainder r is non-negative and is always less that the divisor, *b*.

Examples:

1. If $a = 9$ and $b = 2$, then $q = 4$ and $r = 1$.
2. If $a = 12$ and $b = 17$, then $q = 0$ and $r = 12$.

We know that $a = bq + r$. Dividing on both sides of the equation by b yields

3. $a/b = q + r/b$.

Thus it follows that $q \leq a/b$. (Remember that $0 \leq r < b$.)

The Euclidian Algorithm: Greatest Common Divisor

GCD of two numbers is the largest number that divides both of them. A simple way to find GCD is to factorize both numbers and multiply common prime factors.

The Euclidean Algorithm for finding GCD(A,B) is as follows:

- If A = 0 then GCD(A,B)=B, since the GCD(0,B)=B, and we can stop.
- If B = 0 then GCD(A,B)=A, since the GCD(A,0)=A, and we can stop.
- Write A in quotient remainder form (A = B·Q + R)
- Find GCD(B,R) using the Euclidean Algorithm since GCD(A,B) = GCD(B,R)

The algorithm is based on the below facts.

- If we subtract a smaller number from a larger (we reduce a larger number), GCD doesn't change. So if we keep subtracting repeatedly the larger of two, we end up with GCD.
- Now instead of subtraction, if we divide the smaller number, the algorithm stops when we find remainder 0.

Example:

Find the GCD of 270 and 192

- A=270, B=192
- A ≠0
- B ≠0
- Use long division to find that 270/192 = 1 with a remainder of 78. We can write this as: 270 = 192 * 1 +78
- Find GCD(192,78), since GCD(270,192)=GCD(192,78)
  A=192, B=78

- A ≠0
- B ≠0
- Use long division to find that 192/78 = 2 with a remainder of 36. We can write this as:
- 192 = 78 * 2 + 36
- Find GCD(78,36), since GCD(192,78)=GCD(78,36)
  A=78, B=36

- A ≠0
- B ≠0
- Use long division to find that 78/36 = 2 with a remainder of 6. We can write this as:
- 78 = 36 * 2 + 6
- Find GCD(36,6), since GCD(78,36)=GCD(36,6)
  A=36, B=6

- A ≠0
- B ≠0
- Use long division to find that 36/6 = 6 with a remainder of 0. We can write this as:
- 36 = 6 * 6 + 0
- Find GCD(6,0), since GCD(36,6)=GCD(6,0)
  A=6, B=0

- A ≠0
- B =0, GCD(6,0)=6
  So we have shown:

  GCD(270,192) = GCD(192,78) = GCD(78,36) = GCD(36,6) = GCD(6,0) = 6

  GCD(270,192) = 6

Fundamental Theorem of Arithmetic

It states that every positive integer n, n ≥ 2, can be expressed as the product of one or more prime numbers.

Let's prove that this is true. Recall that a number n is prime if its only positive factors are one and n. On the contrary, n is composite if it's not prime. Since a factor of a number must be no larger than the number itself, this means that a composite number n always has a factor larger than 1 but smaller than n. This, in turn, means that we can write n as a*b, where a and b are both larger than 1 but smaller than n.

Proof by induction on n.

Base: 2 can be written as the product of a single prime number, 2.

Induction: Suppose that every integer between 2 and k can be written as the product of one or more primes. We need to show that k + 1 can be written as a product of primes. There are two cases:

Case 1: k + 1 is prime. Then it is the product of one prime, i.e. itself.

Case 2: k + 1 is composite. Then k + 1 can be written as a*b, where a and b are integers such that a and b lie in the range [2, k].

By the induction hypothesis, a can be written as a product of primes p1p2 . . .pi and b can be written as a product of primes q1q2 . . .qj .

So then k + 1 can be written as the product of primes (p1p2 . . .pi)*(q1q2 . . .qj).

In both cases k + 1 can be written as a product of primes, which is what we needed to show.