1 Weak Induction

2 Summation notation, product notation

One should read

$$\sum_{k=m}^{n} a_m$$

as the value of `result` after executing this code:

```
result = 0;
for (k = m; k <= n; k = k + 1) {
    result = result + a_m.
}
```

Ideally, most of the time you should see the above sum as just a compactified way to write

$$a_m + a_{m+1} + \cdots + a_n$$

Notice that this code does not make sense if $m > n$, because the index k is **always** incremented. In this case we always take the sum to be 0 by default. So a sum like

$$\sum_{k=1}^{0} k$$

is equal to 0, not 1.

Similarly for products. one should read

$$\prod_{k=m}^{n} a_m$$

as the value of `result` after executing this code:

```
result = 1;
for (k = m; k <= n; k = k + 1) {
    result = result * a_m.
}
```

Again this code does not make sense if $m > n$. In this case we always take the product to be 1 by default.

The following equations are some useful properties related to summations.

$$\sum_{i=m}^{n}(a_i + b_i) = \sum_{i=m}^{n} a_i + \sum_{i=m}^{n} b_i$$

The above property is often colloquially referred to as "splitting a sum".

$$\sum_{i=m}^{n} ca_i = c\sum_{i=1}^{m} a_i$$

if c is a constant that does not depend on the index i.

$$\sum_{i=m}^{n} a_i = a_m + \sum_{i=m+1}^{n} a_i$$

$$\sum_{i=m}^{n} a_i = a_n + \sum_{i=n}^{n-1} a_i$$

Note that the above two equations make sense if $n \leq m$. (What happens when $n = m$?)

By yourself come up with some analogous formulas for products.

3 The Principle of Mathematical Induction

Definition 1. A proposition $P(n)$ is a logical statement involving some value n.

It is very helpful to consider an example or two. For example, define $P(n)$ to be the logical statement that $n = 1$. In other words, $P(n) \equiv (n = 1)$. Then $P(n) \equiv T$ if and only if $n = 1$, which is true but is silly to say. Another example: define $P(n) \equiv (2 \mid n)$. Then

$$P(n) \equiv \begin{cases} T, & 2 \mid n \\ F, & 2 \nmid n \end{cases}$$

But as of now we aren't really interested in examples like this. We'd like to know if there is a way to show that $P(n) \equiv T$ for $n \geq k$ for some integer k, for example.

For example, we'd like to figure out whether or not

$$\sum_{i=1}^{n} (2i - 1) = n^2$$

for all n. It seems true! But how might we prove it? This leads us to a technique called *mathematical induction*, a powerful technique which lets us prove classes of statements indexed by the natural numbers. The technique of mathematical induction essentially relies on the following theorem. We will prove this theorem is true in a future section using a property of the natural numbers called the **Well-Ordering Principle**.

Theorem 1. *Let a be any natural number. And let $P(k)$ be a proposition about $k \in \mathbb{N}$. Assume the following claims are true:*

- *$P(a) \equiv T$*
- *Assuming $P(k)$ is true for any natural number $k \geq a$, we can prove that $P(k+1)$ is true.*

Then $P(k)$ is true for all $k \geq a$.

Essentially, suppose you have an indexed family of propositions $P(n)$ which you want to prove true for $n \geq a$. A proof by mathematical induction is essentially the same as satisfying the hypotheses of the above theorem. Essentially, in a proof by induction you show the following:

1. First we show that $P(a) \equiv T$.
2. Next, assuming that $P(k)$ is true for $k \geq a$, prove that $P(k+1)$ is true.

Here is an example of this in action. We will prove the first equality stated at the beginning of the chapter.

Proposition 1.

$$\sum_{i=1}^{n}(2i-1) = n^2$$

for all n for all natural numbers $n \geq 1$.

Proof. We will prove this equality using mathematical induction. First, we observe for $n = 1$ that

$$\sum_{i=1}^{1}(2i-1) = 1 = 1^2.$$

Now assume that

$$\sum_{i=1}^{k}(2i-1) = k^2.$$

Then

$$\sum_{i=1}^{k+1}(2i-1) = \sum_{i=1}^{k}(2i-1) + 2(k+1) - 1 = k^2 + 2k + 1 = (k+1)^2,$$

so we are done. □

Let's break down this proof a little bit further. Here the statement $P(n)$ is the statement that the equality

$$\sum_{i=1}^{n}(2i-1) = n^2$$

is true for that specific n. In the first part of the proof we show that $P(1)$ is true. In the second part of the proof we show that the truth of $P(k)$ implies the proof of $P(k+1)$. To do this, we split the sum

$$\sum_{i=1}^{k+1}(2i-1) = \sum_{i=1}^{k}(2i-1) + 2(k+1) - 1$$

into two parts. By our hypothesis, the left part is exactly k^2. The rest of the prooof simplifies the sum to achieve the desired conclusion: that is to show

$$\sum_{i=1}^{k+1}(2i-1) = (k+1)^2.$$

4 Exercises

1. Prove by induction the following equalities for appropriate integers. You, the reader, will have to determine the appropriate base case.

   (a)
   $$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}.$$

   (For a solution, peep Jason's lecture!)

   (b)
   $$\sum_{k=1}^{n} k(k+1) = \frac{n(n+1)(n+2)}{3}.$$

   (c)
   $$\sum_{k=1}^{n} k(k+1)(k+2) = \frac{n(n+1)(n+2)(n+3)}{4}.$$

   (d) i.
   $$\sum_{k=0}^{n} 2^k = 2^{k+1} - 1.$$

   ii.
   $$\sum_{k=0}^{n} 3^k = \frac{3^{k+1} - 1}{2}$$

   iii.
   $$\sum_{k=0}^{n} 4^k = \frac{4^{k+1} - 1}{3}.$$

   iv. State the pattern you see, and prove this general result using induction.

   v. Using the so called "high-school" algebra identity
   $$(x-1)(x^n + x^{n-1} + \cdots + x + 1) = x^{n+1} - 1,$$
   give another proof of your general result. This proof is non-inductive (or is it?).

2. Consider the pseudocode for the following recursive function, which takes a list `ls` $= (a_0, \ldots, a_n)$ and a function f and returns a list $(f(a_0), f(a_1), \ldots, f(a_n))$ for any non-negative integer n.

   In the code:

   - `length` is a function returning the length of a list,
   - `ls[0]` accesses the first element of the list.
   - `pop(ls)` returns the original list but without the first element. For example, `pop`$(2, 5, 3) = (5, 3)$.

- `::` represents a push operator. For example, $2::(5,3)$ will be the list $(2,5,3)$.

```
function map(ls, f) =
    if (length(ls) = 0) {
        return () /* the empty list. */
    }
    else {
        return f(ls[0])::map(pop(ls), f);
    }
```

Prove that the code above is **correct**. That is, given any list $(a_0, \dots, a_n)$ prove that `map` will return $(f(a_0), f(a_1), \dots, f(a_n))$. (Hint: you'll need to use induction. What are you inducting on? Once you have this in mind this problem turns out to be very simple.)

3. Take a couple of minutes and try to prove by induction that for any integer $n \geq 1$, we have
$$\sum_{k=1}^{n} \frac{1}{k^2} < 2.$$
(You won't be able to do it!)

Let's prove something seemingly "stronger": Prove by induction that for any integer $n \geq 1$ we have
$$\sum_{k=1}^{n} \frac{1}{k^2} < 2 - \frac{1}{n},$$
which implies the above result.

4. Define a function $f(x, y)$, where x and y are allowed to be **natural numbers.** (which include 0). Suppose f has the following properties:

- $f(n, n) = f(n, 0) = 1$ for all $n \in \mathbb{N}$.
- $f(n+1, k+1) = f(n, k) + f(n, k+1)$ for all natural numbers n and k.
- $f(n, m) = 0$ if $m > n$.

Prove by induction (on $n \geq 0$) that
$$\sum_{i=0}^{n} f(n, i) = 2^n.$$
(Hint: when proving the inductive step, you will have to split the sum and reindex.)

5. A *triomino* is an "L" shaped tile formed by 3 adjacent squares of a chessboard. We say that an arrangement of triominos is a *tiling* of a chessboard if every square of the chessboard is covered without any triominos overlapping.

Prove by induction that for all integers $n \geq 1$ the $2^n \times 2^n$ sized chessboard missing one square (in ANY location) can be tiled. The fact that $3 \mid (2^n 2^n - 1 = 4^n - 1)$ is a consequence of problem 1diii.

6. (Challenge Problem): Prove Euler's Formula: For any convex polyhedron, the formula

$$v - e + f = 2$$

holds, where v is the number of vertices, e is the number of edges, and f is the number of faces. You will want to induct on the number of vertices for $v \geq 4$ (because the notion of "face") doesn't make sense for $v < 4$. Your proof will probably not be completely rigorous, and that's okay. (Hints: For the base case, a tetrahedron is the only You cannot solve this problem by just chopping off a vertex, as in general the vertices which are adjacent to the vertex you are attempting to chop off are not generally going to be all in a shared plane. Look up "edge contraction" if you are stuck without ideas about the inductive step.)

5 Strong Induction

6 Principle of Strong Induction

Here is the Principle of Strong Induction:

Theorem 2. *Suppose $P(n)$ is a proposition, and that the following statements hold:*

- *$P(0)$ is true,*
- *If $P(i)$ is true for all $0 \leq i \leq n$, then we can prove that $P(n+1)$ is true.*

Then $P(n)$ holds for all $n \in \mathbb{N}$.

Proof. In fact, this theorem actually directly follows from the Principle of Weak Induction. To see this clearly, define the proposition $Q(n)$ to be equivalent to the claim that $P(i)$ is true for $0 \leq i \leq n$. Then by the hypotheses:

- $Q(0)$ is true,
- If $Q(n)$ is true, then $P(n+1)$ is true. This essentially means that if $Q(n)$ is true, then $P(i)$ is true for all $0 \leq i \leq n+1$, implying that $Q(n+1)$ is true.

So by the Principle of Weak Induction $Q(n)$ is true for all natural numbers n, which implies that $P(n)$ is true for all natural numbers n as well. □

The Principle of Strong Induction is seemingly "stronger" than the Principle of Weak Induction. The reason behind this is because of the nature of the theorem's "induction hypothesis", which assumes the truth of $P(i)$ for all i up to a value n. We may apply this principle to prove certain statements where in order to complete the inductive step assumptions about more than just the previous steps are needed. Here is a particular example of this.

7 Exercises

1. Determine whether or not $P(n)$ is true for all $n \geq 0$ given that P satisfies the rules in part (a), part (b), etc. (No proof is needed)

   (a)
   - $P(0)$, $P(1)$, $P(2)$ are true.
   - If $P(n)$ is true, then $P(n+3)$ is true.

   (b)
   - $P(0)$ and $P(1)$ are true,
   - If $P(n)$ is true, then $P(2n)$ is true,
   - If $P(n)$ is true, then $P(n-1)$ is true.

   (c) Challenge Problem:
   - $P(0)$, $P(1)$ are true.
   - If n is odd, then $P(n)$ is true if and only if $P(3n+1)$ is.
   - If n is even, then $P(n)$ is true if and only if $P(n/2)$ is.

2. In discussion, I presented the following notion of strong induction (which we called Weak Induction++):

   Theorem 3. *Let $P(n)$ be a proposition, and suppose the following statements hold:*

   - *$P(0)$ and $P(1)$ is true.*
   - *If $P(n-1)$ and $P(n)$ are true for $n \geq 1$, then $P(n+1)$ is true.*

   The conclusion is that $P(n)$ is true for all $n \in \mathbb{N}$.

   Generalize this theorem to multiple base cases.

3. Recall during discussion when we proved that $a_n \leq (7/4)^{n+1}$, we stated an inductive hypothesis which was similar to that in Theorem 1. Explain why we couldn't state and prove the inductive hypothesis with only one base case $n = 0$, mimicking the format of the above theorem. (Recall that for $n \geq 2$, we had $a_n = a_{n-1} - a_{n-2}$.)

4. The following problem outlines a proof of the so called **arithmetic-geometric mean inequality**: for all non-negative reals $a_1, \ldots, a_n$ we have

$$\frac{1}{n}\sum_{i=1}^{n} a_i \geq \sqrt[n]{\prod_{i=1}^{n} a_i}.$$

   (a) When $n = 1$ this inequality is trivially true. For $n = 2$: Note that for all $a > 0$ there is $b > 0$ such that $b^2 = a$. Use this fact and the fact that $(x-y)^2 \geq 0$ for all (non-negative) x and y to show directly that the inequality is true when $n = 2$.

   (b) Suppose this inequality is true for $n = k$. Using the $n = 2$ case, show that this inequality is true for $n = 2k$.

(c) Supposing this inequality is true for $n = k$, show that this inequality is true for $n = k - 1$.

(d) Conclude that we are done. (This method of proof is called **Cauchy Induction**.)

5. Suppose that there are n people that board a flight. They seat themselves one at a time. The first person has forgotten which seat he is assigned, and picks a random seat to sit in. Each subsequent person either sits in their designated seat, or if it is already occupied, they sit in a remaining seat randomly (as in uniformly random).

   (a) When $n = 2$, what is the probability that the last person (person 2) sits in the seat that he is assigned?

   (b) What about when $n = 3$? $n = 4$?

   (c) Make a conjecture for general n and prove your conjecture using strong induction.

8 Proving the Induction Principle

8.1 The Well Ordering Principle

We have (?) stated the principle of Mathematical Induction. In the following sections, we attempt to demonstrate that the principle of Mathematical Induction is a statement that requires "proof". The main technical detail needed to prove this principle is the well ordering principle of the natural numbers. First we indicate what it means for a set to be well ordered.

Definition 2. Let S is a set with an order relation $\leq$ on $S \times S$. Then S (along with the order relation $<$) is called well ordered if every subset of S has a least element.

In other words, for any non-empty subset $T \subset S$ there exists $t_0 \in T$ such that $t_0 \leq t$ for all $t \in T$.

Example 1. The set $\mathbb{Z}$ is not well ordered, for $\mathbb{Z}$ has no least element. In that case, consider the set $Y = \mathbb{Z} \cup \{-\infty\}$ with the usual order relation plus the order $-\infty < a$ for all $a \in \mathbb{Z}$. Then Y has a least element (namely, $-\infty$) but is not well ordered, for the subset $\mathbb{Z}$ of Y has no least element.

The above example leads us to a first elementary observation: any subset of a well ordered set is well ordered. This simply follows from the fact that a subset of a subset is a subset of the original set.

With these preliminary details we can state the well ordering principle of the natural numbers. Usually, this is taken as an **axiom** of the natural numbers[1]. This means that we take it to be the

> The set of natural numbers $\mathbb{N}$, along with the usual ordering $<$, is a well ordered set.

This makes it possible to come up with various interesting examples of well ordered sets.

[1] If we formally define the natural numbers, then the well ordering principle can actually be proven. But this is beyond the scope of this book (for now).

Example 2. Consider the set $\{1,2\} \times \mathbb{N}$ in the *dictionary order*: we say that $(a,b) < (c,d)$ if $a < c$ or if $a = c$ then $b < d$. Then $\mathbb{N} \times \mathbb{N}$ is well ordered. To see this, let S be a non-empty subset of $\{1,2\} \times \mathbb{N}$. Then consider all the elements of S with 1 as the first component. If this subset is non-empty then it follows by the well ordering principle on $\mathbb{N}$ that there is a least element of the form $(1,k)$. Otherwise, we can apply the same reasoning to conclude that there must be a least element of the form $(2,k)$.

The well ordering principle is powerful. We will first use it to prove the quotient remainder theorem (which was first introduced in (atm nowhere as of now)) here, and we will use it later in Chapter 7 to prove some fundamental results about divisibility.

Theorem 4. *Suppose that a is any integer and b is any positive integer. Then there exist unique integers q and r such that $0 \leq r < b$ and we have*

$$a = qb + r.$$

The numbers q and r are called the ***quotient*** *and* ***remainder*** *of the division of a by b.*

The proof idea is very simple. In the theorem statement, the *remainder* r is intuitively in a sense the "smallest" positive value of remainder we can get by subtracting integer multiples of b from a. We make this reasoning precise by invoking the well ordering principle to explicitly obtain r.

Proof. Let

$$S = \{n \in \mathbb{Z} \mid n = a - kb, k \in \mathbb{Z}, n \geq 0\}.$$

That is, S is all the non-negative values $a - kb$ where k ranges across integer values. Then S is a subset of $\mathbb{N} \cup \{0\}$, which is well ordered because $\mathbb{N}$ is well ordered (by the well ordering principle). It follows that S has a least element r. Let q be the value such that $a - qb = r$ (which is possible precisely because r is contained in S). Then $a = qb + r$.

Now all that is left is to show that this representation $a = qb + r$ is unique. To show this suppose that there is another pair q' and r' of integers with $0 \leq r' < b$ we also have $a = q'b + r'$. Subtracting both equations we have that

$$0 = (q - q')b + (r - r').$$

Since $0 \leq r, r' < b$ it follows that $|r - r'| < b$ so we get hte equation

$$|q - q'|b < b \implies |q - q'| < 1.$$

Since q and q' are integers it follows that $q = q'$ and hence $r = r'$, showing that this representation $a = qb + r$ is unique. □

8.2 Equivalence of the Well Ordering Principle and the Principle of Mathematical Induction

Now we prove from the Well Ordering principle the Principle of Mathematical Induction. The idea will be as follows: we will consider the *smallest* element such that a proposition is false, and then we will use the assumptions of the Priniciple of Mathematical Induction to derive contradictions. Hence the Principle of Mathematical Induction is true as stated.

In fact, if we assume the Principle of Mathematical Induction as a given statement, we can use it to show the well ordering principle of the natural numbers. But to give a rigorous proof we need the Principle of Strong Induction, which we will prove from the Principle of Weak Induction later.

Theorem 5. *Suppose that $P : \mathbb{N} \to \{T, F\}$ is a boolean function with the following properties:*

- $P(1) \equiv T$
- $P(n) \equiv T \implies P(n+1) \equiv T$ *for all* $n \in \mathbb{N}$.

Then $P(n) \equiv T$ for all $n \in \mathbb{N}$.

Proof. Assume for the sake of contradiction that there is some $s \in \mathbb{N}$ such that $P(s) \equiv F$. Let S be the set of all s where $P(s) \equiv F$. By assumption, $S \neq \varnothing$, and hence by the well ordering principle there is a minimal element $r \in S$. We see that $r \neq 1$ because $P(1) \equiv T$ by assumption. So $r - 1 \in \mathbb{N}$. But since $r \in S$ is minimal, we must have that $P(r-1) \equiv T$ (or else our assumption about r being the minimal element in S would be wrong). But since $P(r-1) \equiv T$, this implies that $P(r) \equiv T$ (by modus ponens). This is a contradiction and the conclusion follows. □

To prove the other direction (namely, that the Principle of Mathematical Induction implies the Well Ordering Principle), we need the stronger principle of Strong Induction. So what we will do is use the Principle of Mathematical Induction to prove the Principle of Strong Induction first.

Theorem 6. *Suppose that the Principle of Mathematical Induction is true. Suppose that $P : \mathbb{N} \to \{T, F\}$ is a boolean function with the following properties:*

- $P(1) \equiv T$
- *If $P(k) \equiv T$ for all $1 \leq k \leq n$ for $n \geq 1$, then $P(n+1) \equiv T$.*

Then $P(n) \equiv T$ for all $n \in \mathbb{N}$.

Proof. Define an auxiliary function $Q : \mathbb{N} \to \{T, F\}$ by the following:

$$Q(n) \equiv \begin{cases} T & P(k) \equiv T \text{ for } 1 \leq k \leq n \\ F & \text{otherwise.} \end{cases}$$

Then by assumption, $Q(1) \equiv T$ and $Q(k) \equiv T$ implies that $P(n+1)$ is true, which together with $Q(n)$ implies that $Q(n+1) \equiv T$. Hence by the Principle of Mathematical Induction we have that $Q(n)$ is true for all $n \in \mathbb{N}$ which implies that $P(n)$ is true for all $n \in \mathbb{N}$, as desired. □

The converse statement is also true, this will be left as an exercise. Now that we have the principle of strong induction, we can use it now to prove the well ordering principle. This will show that the Well Ordering Principle and the Principle of Mathematical Induction are equivalent.

Theorem 7. *The Strong Induction Principle implies the Well Ordering Principle. Hence the Well Ordering Principle and the Principle of Mathematical Induction are equivalent.*

Proof. Suppose that $S \subset \mathbb{N}$ is a non-empty set with no least element. Let P be the following proposition:

$$P(n) = \begin{cases} T & n \notin S \\ F & n \in S \end{cases}.$$

So the proposition $P(n)$ reflects whether or not n is in the set S. Since 1 is the least element in $\mathbb{N}$, we know that $1 \notin S$ or else S would have a least element. So $P(1) \equiv T$. Now suppose for any $n \in \mathbb{N}$ that $P(k) \equiv T$ for $1 \leq k \leq n$. Then by the definition of P no natural number less than or equal to n is in S. It follows that $n + 1 \notin S$ or else $n + 1$ would be the least element in S. It follows that $P(n + 1) \equiv T$.

By the Principle of Strong Induction it follows that $P(n) \equiv T$ for all $n \in \mathbb{N}$. This implies that no element $n \in \mathbb{N}$ is in S. So $S = \varnothing$. The Well Ordering Principle follows, as desired. □

9 Exercises

1. Show that the following sets are well-ordered under the ordering described. (It will be helpful to use the fact that $\mathbb{N}$ is well-ordered.

   - $\mathbb{N} \cup \{\omega\}$, where $\omega > n$ for any $n \in \mathbb{N}$ and where $\mathbb{N}$ has the usual ordering.
   - $\mathbb{N} \times \mathbb{N}$ under the dictionary order (which was defined in Example 2).
   - $\mathbb{Z}$ under the following ordering R: aRb if $|a| < |b|$, and if $|a| = |b|$ then $a < b$ if a is negative and b is positive.

2. Show that the following sets are not well-ordered:

   - The set of rationals $\mathbb{Q}$ under the usual ordering.
   - The set $\{2^n \mid n \in \mathbb{Z}\}$ under the usual ordering on $\mathbb{Q}$.
   - The cube $[0, 1] \times [0, 1]$ under the dictionary ordering.

3. Show that for any well-ordered set S with order relation $<$ and any element $r \in S$, either r is a maximal element ($r \geq s$ for all $s \in S$) or r has an immediate successor r^+, that is, a smallest element greater than r. Is every non-minimal element r an immediate successor of some other element?

4. Suppose that a is any integer and b is any positive integer. State and prove when there exist integers q and r such that $r < |b/2|$ and we have

   $$a = qb + r.$$

   When can we ensure that q and r are unique?

5. Prove that the Principle of Strong Induction implies the Principle of Mathematical Induction.

6. Prove the Principle of Strong Induction using the Well Ordering Principle.

7. Suppose that $P(n)$ is a proposition. In each part assume $P(n)$ satisfies the given list of properties and use the Well Ordering Principle to prove that $P(n)$ is true for all $n \geq 0$. After this, generalize.

   (a)
   - $P(0)$, $P(1)$, and $P(2)$ are true,
   - $P(n) \equiv T \implies P(n+3) \equiv T$.

   (b)
   - $P(0)$ and $P(1)$ are true,
   - If $P(n)$ is true, then $P(2n)$ is true,
   - IF $P(n)$ is true, then $P(n-1)$ is true.