IV. Proof Techniques

A. Sequences and Summations

1. Definition: A sequence is a function from a subset of \( Z \) (usually either \( \mathbb{N} = \{0, 1, 2, 3, \ldots\} \) or \( \mathbb{Z}^+ = \{1, 2, 3, 4, \ldots\} \) to another set \( S \). We use \( a_n \) to denote the image of the integer \( n \). We call \( a_n \) a term of the sequence.

2. We use \( \{a_n\} \) to denote the whole sequence. Note the conflict with set notation.

Example: \( a_n = 1/n \), \( n = 1, 2, \ldots, \infty \) or \( n = 1, 2, \ldots \)

Then: \( a_1 = 1/1 = 1, \ a_2 = 1/2, \ a_3 = 1/3, \ldots \)

3. Definition: A geometric progression is a sequence of the form \( a, ar, ar^2, \ldots, ar^n \) \((n \text{ can be } \infty)\), where the initial term \( a \) and the common ratio \( r \) are real.

a. Example: \((-1)^n, \ n = 1, 2, \ldots\)

   = \(-1, 1, -1, 1, \ldots\)

b. Example: \(2 \cdot (1/3)^n, \ n = 1, 2, \ldots\)

   = \(2/3, 2/9, 2/27, \ldots\)

c. Example 3: \(4 \cdot 5^n, \ n = 0, 1, 2, \ldots\)

   = 4, 20, 100, \ldots\)
4. Definition: An arithmetic progression
is a sequence of the form
\[ a, a+d, a+2d, \ldots, a+nd \]
where the initial term \( a \) and the common difference \( d \) are real numbers.

a. Example: \[ s_n = -1 + 4n, \quad n = 0, 1, 2, \ldots \]
\[ = -1, 3, 7, \ldots \]

b. Example: \[ t_n = 7 - 3n, \quad n = 1, 2, 3, \ldots \]
\[ = 4, 1, -2, -5, \ldots \]

5. Finite sequences of the form \( a_1, a_2, \ldots, a_n \) are often used in computer science where
they are referred to as strings. The
length of the string is the number of terms
in the string. The empty string has no
terms and is denoted by \( \lambda \).

6. A common problem is to determine
the formula for a sequence from the
first few elements.

Examples:

a. \( 1, \frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \ldots \)
   This involves powers of 2.
   So, \( \frac{1}{2^n} \) is a good guess
   which works, starting from \( n = 0 \).

b. \( 1, 3, 5, 7, 9, \ldots \)
   Each term differs by 2.
   Here, \( 1 + 2n, \quad n = 0, 1, 2, \ldots \) works.

c. \( 1, -1, 1, -1, \ldots \)
   Each term is multiplied by -1.
   \[ a_n = (-1)^n \]
   is the natural result,
   \( n = 0, 1, \ldots \).
NOTE:
We are making guesses here, not constructing proofs! One could have:
1, 1/2, 1/4, 1/8, 2, 1, 1/2, 1/4, 4, 2, 1, 1/2, ... which has a completely different formula.

To construct a proof, you need a rule for all n, not just a few examples.

d. A more complicated example
\( f(n) = 1, 7, 25, 77, 241, 727 \)
(1) First try: difference - 6, 18, 54, 162
(2) Second try: factors
18 = 3 x 6, 54 = 3 x 18, 162 = 3 x 54

Conclusion: \( f(n) = 3^n - 2 \)
Why does this work?
(1) The first difference eliminates the constant term
\( b_n = a_{n+1} - a_n = (3^{n+1} - 2) - (3^n - 2) = 3^n - 2 \)
\( = 3^n (3 - 1) = 2 \cdot 3^n \)
(2) The factors eliminate the constant factor
\( b_{1n} / b_n = 2 \cdot 3 / 2 = 3 \)

7. There are many important integer sequences.
The book "Encyclopedia of Integer Sequences" by Sloane and Plouffe lists thousands of them. Over 8000 are known.

8. Summation
a. Suppose we wish to sum the elements of a sequence \( S = a_1, a_2, ..., a_n \),
we would write
\[ a_m + a_{m+1} + a_{m+2} + \ldots + a_n = \sum_{j=m}^{n} a_j \]

b. NOTE: \( j \) is referred to as the index of summation or more generally a dummy variable. That means that it can be changed without changing the meaning of the sum.

\[ \sum_{j=m}^{n} a_j \text{ is the same as } \sum_{i=m}^{n} a_i \equiv \sum_{k=m}^{n} a_k \]

This is also the same as

\[ \sum_{j=m-1}^{n-1} a_j = a_m + a_{m+1} + \ldots + a_n \]

since the elements that have been summed hasn’t changed. This sort of variable transformation is often useful.

c. \( m \) is referred to as the lower limit and \( n \) is referred to as the upper limit.

d. Example (1) Express the sum of \( 1, 1/2, 1/3, \ldots, 1/100 \). The most obvious way to do it is to write

\[ S = \text{sum} = \sum_{j=1}^{100} 1/j \text{ or } \sum_{k=1}^{100} 1/k \]

We could also use \( \sum_{j=0}^{99} 1/(j+1) \)

Example (2). \( \sum_{j=1}^{5} j^2 = 1+4+9+16+25 = 55 \)
9. Geometric sum

a. These sums appear often in practice and can be evaluated explicitly

Theorem: If $a$ and $r$ are real numbers and $r \neq 0$, then

$$
\sum_{j=0}^{n} a r^j = \begin{cases} 
\frac{a r^{n+1} - a}{r - 1} & \text{if } r \neq 1 \\
(n+1) a & \text{if } r = 1 
\end{cases}
$$

Proof: We let $S = \sum_{j=0}^{n} a r^j$

We then have

$$
rs = r \sum_{j=0}^{n} a r^j \\
= \sum_{j=0}^{n} a r^{j+1} \\
= \sum_{k=1}^{n+1} a r^k \quad \text{[Note change of variables]} \\
= \sum_{k=0}^{n+1} a r^k + (a r^{n+1} - a) \quad \text{[We have added and subtracted the "0" element and treated the "n+1" element explicitly]} \\
= S + (a r^{n+1} - a)
$$

We now have an algebraic expression for $S$, except if $r = 1$. Solving for $S$ we obtain

$$
S = \frac{a r^{n+1} - a}{r - 1}
$$

If $r = 1$, we obtain $\sum_{j=0}^{n} a = (n+1) a \quad \square$

b. Example: $a = 1, n = 4, r = 2$

$$
\sum_{j=0}^{4} 2^j = 1 + 2 + 4 + 8 + 16 = 31
$$
\[
\sum_{j=0}^{4} 2^j = \frac{2 \cdot 2^4 - 1}{2 - 1} = 31
\]

c. If \( |r| < 1 \), we can extend the limit to infinity

\[
\sum_{j=0}^{\infty} r^j = \left[ \lim_{n \to \infty} \sum_{j=0}^{n} r^j \right] \to \sum_{j=0}^{\infty} r^j = \frac{1}{1-r} - 1 = \frac{0}{r-1} = \frac{1}{1-r}
\]

By taking the derivative of both sides, we can derive important related formulae

\[
\frac{d}{dr} \sum_{j=0}^{\infty} r^j = \sum_{j=0}^{\infty} j r^{j-1} = \frac{d}{dr} \frac{1}{1-r} = \frac{1}{(1-r)^2}
\]

These formulae appear very often in practice.

Note: This is a very bad network!

d. Example. Consider a packet that is propagating through the nodes of a network. At each node, \( \frac{1}{2} \) are dropped

\[
1 \rightarrow \begin{array}{c}
1 \\
\downarrow \frac{1}{2}
\end{array} \rightarrow \begin{array}{c}
2 \\
\downarrow \frac{1}{4}
\end{array} \rightarrow \begin{array}{c}
3 \\
\downarrow \frac{1}{4}
\end{array} \rightarrow \begin{array}{c}
\vdots
\end{array}
\]

How far does a packet get on average?

First, we verify that the fraction of packets dropped is \( \frac{1}{2} \).

\[
S = \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \ldots = \sum_{j=1}^{\infty} \left( \frac{1}{2} \right)^j = \frac{1}{2} \sum_{j=1}^{\infty} \left( \frac{1}{2} \right)^j = \frac{1}{2} \sum_{j=0}^{\infty} \left( \frac{1}{2} \right)^j
\]

\[
= \frac{1}{2} \cdot \frac{1}{1 - \frac{1}{2}} = 1
\]

The distance is given by:

\[
D = \sum_{j=1}^{\infty} j \left( \frac{1}{2} \right)^j = \frac{1}{2} \sum_{j=0}^{\infty} j \left( \frac{1}{2} \right)^{j+1} = \frac{1}{2} \left( \frac{1}{1 - \frac{1}{2}} \right)^2 = 2
\]
10. Other sums
   a. double sums
   \[ \sum_{i=m}^{n} \sum_{j=p}^{q} a_{i,j} = (a_{m} + a_{m+1} + \ldots + a_{n})(b_{p} + b_{p+1} + \ldots + b_{q}) \]

   Example: \[ \sum_{i=1}^{4} \sum_{j=1}^{3} i \cdot j = (1+2+3+4)(1+2+3) = 10 \cdot 6 = 60 \]

   b. Sum over a set
   \[ \sum_{s \in S} f(s) \] indicates that the sum is over elements of the set \( S \)

   Example: \[ \sum_{s \in \{0, 2, 4\}} s = 0 + 2 + 4 = 6 \]

5. Power series. [Note: The sum of a sequence is often called a series]

   \[ \sum_{k=1}^{n} k = \frac{n(n+1)}{2} \]

   Example: \( n = 4 \), \( 1 + 2 + 3 + 4 = 10 = \frac{5 \cdot 4}{2} \)

   \[ \sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6} \]

   Example: \( n = 3 \), \( 1^2 + 2^2 + 3^2 = 1 + 4 + 9 = 14 = \frac{3 \cdot 4 \cdot 7}{6} \)

Note: They are related to the result

\[ \int x^m \, dx = \frac{x^{m+1}}{m+1} + C \]

How?
11. Cardinality

a. We already defined cardinality for finite sets as the number of elements in a set. We now extend the concept to infinite sets.

Two sets $A$ and $B$ are said to have the same cardinality if the elements of the two sets can be put in one-to-one correspondence.

This definition of equal cardinality is consistent with our definition for finite sets, because any finite sets with the same number of elements can be put in one-to-one correspondence. That cannot be done if they have different number of elements.

\[
\begin{array}{cccc}
\bigcirc & \bigcirc & \bigcirc & \bigcirc \\
\downarrow & \downarrow & \downarrow & \downarrow \\
\bigcirc & \bigcirc & \bigcirc & ?
\end{array}
\]

- same number
- different number

b. A set that is finite or has the same cardinality as positive integers is referred to as countable. Any other set is uncountable.

c. Theorem: The set of all integers is countable.
Proof: Let $f(n) = \frac{n-1}{2}$ when $n$ is odd
Let $f(n) = -\frac{n}{2}$ when $n$ is even

\[
\begin{array}{cccccccc}
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\
\downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\end{array}
\]

... $f: \mathbb{Z}^+ \rightarrow \mathbb{Z}$
Query: How do you prove that it is not possible for a set to have two different cardinalities?

Since this function maps every element of \( \mathbb{Z}^+ \) into a distinct element of \( \mathbb{Z} \). Hence, this function is onto. To show that it is one-to-one, we must show that each element of \( \mathbb{Z} \) has a pre-image in \( \mathbb{Z}^+ \). For any \( m \in \mathbb{Z} \), we define \( g(m) = 2m+1 \) if \( m \geq 0 \) and \( g(m) = -2m \) if \( m < 0 \)

By comparison with \( f(m) \), we see that \( g(m) \) maps \( m \in \mathbb{Z} \) into its pre-image.

Note: Since \( \mathbb{Z}^+ \subset \mathbb{Z} \), it might seem surprising that they have the same cardinality. Intuitively, we would think that \( \mathbb{Z} \) is "bigger" than \( \mathbb{Z}^+ \). Nonetheless, this is the most useful way to extend the concept of number to infinite sets.

Note: This proof isn't rigorous. What is missing? How do we fix it?

**Theorem:** The set of rational numbers \( \mathbb{Q} \) is countable. Proof (in outline): We construct a table with the element of \( \mathbb{Z} \) labeling the horizontal axis and \( \mathbb{Z}^+ \) labeling the vertical axis.

<table>
<thead>
<tr>
<th>0</th>
<th>-1</th>
<th>1</th>
<th>-2</th>
<th>2</th>
<th>-3</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>-1</td>
<td>0/-1</td>
<td>-1/-1</td>
<td>1/1</td>
<td>-2/-1</td>
<td>2/-1</td>
<td>-3/-1</td>
</tr>
<tr>
<td>1</td>
<td>0/1</td>
<td>-1/1</td>
<td>1/1</td>
<td>-2/1</td>
<td>2/1</td>
<td>-3/1</td>
</tr>
<tr>
<td>-2</td>
<td>0/-2</td>
<td>-1/-2</td>
<td>1/-2</td>
<td>-2/-2</td>
<td>2/-2</td>
<td>-3/-2</td>
</tr>
<tr>
<td>2</td>
<td>0/2</td>
<td>-1/2</td>
<td>1/2</td>
<td>-2/2</td>
<td>2/2</td>
<td>-3/2</td>
</tr>
<tr>
<td>-3</td>
<td>0/-3</td>
<td>-1/-3</td>
<td>1/-3</td>
<td>-2/-3</td>
<td>2/-3</td>
<td>-3/-3</td>
</tr>
<tr>
<td>3</td>
<td>0/3</td>
<td>-1/3</td>
<td>1/3</td>
<td>-2/3</td>
<td>2/3</td>
<td>-3/3</td>
</tr>
</tbody>
</table>

This path, snaking through all the elements of the table, will eventually cross every rational number (in fact an infinite number of times).
If we only list the first encounter with each rational, then we have put \( \mathbb{Q} \) into one-to-one correspondence with \( \mathbb{Z}^+ \).

"Sketch" means that we are not being rigorous. What is left out?

E. Theorem: The set of real numbers is uncountable. We sketch a proof based on Cantor diagonalization (Georg Cantor invented the modern notion of cardinality.)

Suppose that we can list the reals between 0 and 1. If we can do that, then we can't list all reals.

Lemma: Every real number can be represented as a continuous decimal.

Lemma: If we exclude decimal representations of the form \( d_1 d_2 \ldots d_n \bar{9} \), then each decimal representation corresponds to a unique real number.

[NOTE: We need this exclusion because \( 0.d_1 d_2 \ldots d_n \bar{9} = 0.d_1 d_2 \ldots (d_n + 1) \)]

Imagine that we have made a list of all the reals between 0 and 1:

\[
\begin{align*}
V_1 &= 0.d_{11}d_{12}d_{13} \ldots \\
V_2 &= 0.d_{21}d_{22}d_{23} \ldots \\
V_3 &= 0.d_{31}d_{32}d_{33} \ldots \\
\end{align*}
\]

we can easily construct a real number that is not on the list:

\[
V_{\text{new}} = 0.d_{11}'d_{22}'d_{33}' \ldots \quad \text{where} \quad d_{11}' \neq d_{11}, \; d_{22}' \neq d_{22}, \; d_{33}' \neq d_{33}
\]
Since \( r_{new} \) is not in the list, the list cannot be complete, and we have a contradiction. 

12. Borel Fields

a. There is a sense in which the set of reals is much larger than the set of rationals or integers. If you pick a number “at random” from the set of reals, your probability of picking an integer or a rational is zero.

b. For countable sets, we typically define probabilities on the power set. Example: When flipping a coin, we might say \( P(\emptyset) = 0 \), \( P(H) = \frac{1}{2} \), \( P(T) = \frac{1}{2} \), \( P(H, T) = 1 \).

c. The power set is too large for the reals and contains many strange objects. Instead, we use the Borel set, which contain intervals \( [a, b) \) where \( a, b \in \mathbb{R} \) and all countable combinations of these intervals. The Borel set is still very big. It contains fractal structures, as well as the integers and rationals. However, it becomes meaningful to define probabilities on this set. For example, if \( 0 < a < b < c \), a uniform distribution would assign \( P([a, b]) = (b-a)/c \).
B. Mathematical Induction

1. This technique is used to prove propositions about sequences. It is perhaps the most important single technique in number theory and computer science. It is also unintuitive at first; it seems like "magic." It is very important to become comfortable with this technique.

2. Basic technique:
   Consider a sequence of propositions $P(n)$, $n \in \mathbb{Z}^+$
   For example:
   $P(n) \overset{def}{=} \forall n \in \mathbb{Z}^+, \sum_{j=1}^{n} j = \frac{n(n+1)}{2}$

   The proof technique has two steps:
   (1) Basis step. Show $P(n)$ is true when $n = 1$
   (2) Inductive step. Show: for all $n$, $n \in \mathbb{Z}^+$
      $P(n) \Rightarrow P(n+1)$. That is to say, for all $n$,
      if $P(n)$ is true then $P(n+1)$ must be true.

NOTE: The validity cannot be proved from the techniques that we have already.
It must be assumed. We are making plausibility arguments.

The basic idea is that we have
1. $P(1)$ (basis step)
   1. $P(1) \Rightarrow P(2)$ (inductive step + universal instantiation)
      \[ \vdash P(2) \quad (\text{modus ponens}) \]

   2. $P(3)$ (from 1); $P(2) \Rightarrow P(3)$ (from inductive step);
      \[ \vdash P(3) \quad (\text{modus ponens}) \]
      \[ \vdots \]
      \[ \vdash P(n) \quad (\text{from } n+1); \quad P(n) \Rightarrow P(n+1); \quad \vdash P(n+1) \]
      \[ \vdash P(n+1) \]
      And so on.
3. Examples

a. Proof of an equality
\[ \sum_{j=1}^{n} j = \frac{n(n+1)}{2} \quad \forall n \in \mathbb{Z}^+ \]

Basis step: \( P(1) \) states \( \sum_{j=1}^{1} j = 1 = \frac{1(1+1)}{2} \) (which is true)

Inductive step: Suppose \( P(n) \)
\[ \sum_{j=1}^{n} j = \frac{n(n+1)}{2} \]

Show \( \sum_{j=1}^{n+1} j = \frac{(n+1)(n+2)}{2} \)

\[ \sum_{j=1}^{n+1} j = \sum_{j=1}^{n} j + (n+1) \] (meaning of sum)

\[ = \frac{n(n+1)}{2} + (n+1) \] (inductive hypothesis)

\[ = \frac{n^2 + n + 2n + 2}{2} \] (algebra)

\[ = \frac{n^2 + 3n + 2}{2} = \frac{(n+1)(n+2)}{2} \] (more algebra)

b. Proof of an inequality
\( n < 2^n \quad \forall n \in \mathbb{Z}^+ \)

Basis step: \( P(1) \) states \( 1 < 2^1 = 2 \), which is true

Inductive step: Suppose \( P(n) \)
\( n < 2^n \). Show \( n+1 < 2^{n+1} \)

\( n + 1 < 2^{n+1} \) (algebra)

\( n + 1 < 2^n + 2^n \) (algebra + \( 2^n \geq 1 \) \( \forall n \))

\( n + 1 < 2 \times 2^n = 2^{n+1} \) (algebra, properties of exponents) \( \square \)
c. Proof of a universal theorem
\[ p^3 - n \text{ is divisible by } 3 \quad \forall n \in \mathbb{Z}^+ \]

**Basis step:** \( P(1) \) states \( 1^3 - 1 = 0 \) is divisible by 3 (which is true).

**Inductive step:** Suppose \( P(n) \)
\[ h^3 - n = 3m, \text{ where } m \in \mathbb{Z} \]
\[ (h+1)^3 - (n+1) = h^3 + 3h^2 + 3h + 1 - n - 1 \quad \text{(algebra)} \]
\[ = (h^3 - n) + 3(n^2 + n) \quad \text{(more algebra)} \]
\[ = 3(m + n^2 + n) \quad \text{(inductive hypothesis + algebra)} \]
which is divisible by 3 \( \square \)

4. Some important examples

a. Sums of a geometric series

[Note: We gave a direct proof earlier]

\[ \sum_{j=0}^{n} ar^j = \frac{ar^{n+1} - a}{r-1} \]

**Basis step:** Prove \( P(0) \). Note that since the sequence is over \( \mathbb{N} \), not \( \mathbb{Z}^+ \), we start from \( P(0) \), not \( P(1) \).

\( P(1) \) states
\[ \sum_{j=0}^{0} ar^j = ar^0 = a = \frac{ar^1 - a}{r-1} = a \frac{r-1}{r-1} \]

**Inductive step:** Suppose \( P(n) \)
\[ \sum_{j=0}^{n+1} ar^j = \sum_{j=0}^{n} ar^j + ar^{n+1} \]
\[ = \frac{ar^{n+1} - a}{r-1} + ar^{n+1} = \frac{ar^{n+1} - a}{r-1} + \frac{ar^{n+2} - ar^{n+1}}{r-1} \]
\[ = \frac{ar^{n+2} - a}{r-1} \quad \square \]
6. Inequality for harmonic numbers

Definition: The \( j \)-th harmonic number

is defined as \( H_j = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{j} \)

Proposition: \( H_{2^n} \geq 1 + \frac{n}{2} \) \( \forall n \in \mathbb{Z}^+ \)

Proof: Basis step: \( P(1) \) states \( 1 + \frac{1}{2} \geq 1 + \frac{1}{2} \)

which is true.

Inductive step:

\[
\begin{align*}
H_{2^{n+1}} &= \sum_{j=1}^{2^{n+1}} \frac{1}{j} = \sum_{j=1}^{2^n} \frac{1}{j} + \sum_{j=2^n+1}^{2^{n+1}} \frac{1}{j} = H_{2^n} + \sum_{j=2^n+1}^{2^{n+1}} \frac{1}{j} \\
H_{2^n} + \sum_{j=2^n+1}^{2^{n+1}} \frac{1}{j} &\geq H_{2^n} + 2^n \cdot \frac{1}{2^{n+1}}
\end{align*}
\]

where we note that there \( 2^n \) terms in the

sum, all of which are greater than or equal to \( \frac{1}{2^{n+1}} \)

\[
H_{2^{n+1}} \geq H_{2^n} + 2^n \cdot \frac{1}{2^{n+1}} \geq \left( 1 + \frac{n}{2} \right) + \frac{2^n}{2^{n+1}}
\]

(Inductive hypothesis)

\[
H_{2^{n+1}} \geq 1 + \frac{n}{2} + \frac{1}{2} = 1 + \frac{(n+1)}{2}
\]

Note: This proves that the harmonic series

diverges since as \( n \) increases,

it slowly becomes greater than any

number.

C. The power set \( \mathcal{P}(S) \) of a finite set

\( S \) has \( 2^n \) elements if \( |S| = n \)

Proof: We let \( P(n) \) be the proposition that

a set \( S \) with \( n \) elements has \( 2^n \) subsets
Basis step: $P(0)$ implies that the empty set $\emptyset$ has one subset since $2^0 = 1$, which is true since the only subset of the empty set is itself.

Inductive step: Suppose $S = \{a_1, a_2, \ldots, a_n\}$ has $n$ elements and consider the set $T = S \cup \{a_{n+1}\}$, which has $n+1$ elements. For every subset $B$, such that $B \subseteq S$, we can create two subsets of $T$, $B$ and $B \cup \{a_{n+1}\}$. Any subset of $T$ must be in one of these two sets of subsets.

Why? Suppose the contrary. Then, there is some $C = \{a_{i_1}, a_{i_2}, \ldots, a_{i_k}\}$ that is not in either group. Suppose $a_{i_k} \notin \{a_1, \ldots, a_{n}\}$, then $C$ is a perfectly good subset of $S$ and must be in a set of subsets $B$. Suppose $a_{i_k} \in \{a_1, \ldots, a_{n}\}$, then $C - \{a_{i_k}\}$ is a perfectly good subset of $S$ and hence $C$ must be in the set of subsets of $B \cup \{a_{i_k}\}$. Hence $C$ must be in one of two sets of subsets.

Each of these two sets of subsets has $2^n$ elements; so, the total number of subsets of $T$ is $2 \cdot 2^n = 2^{n+1}$.

d. Generalization of De Morgan's law

Prove \( \bigcap_{j=1}^{n} A_j = \bigcup_{j=1}^{n} \overline{A_j} \)

where \( A_j \subseteq U \), \( j = 1, \ldots, n \) and \( n \in \mathbb{Z}, \geq 2 \)

Basis step: Here we start at $n=2$

$P(2)$ asserts $A_1 \cap A_2 = A_1 \cup \overline{A_2}$

which is the usual De Morgan's law
Inductive step:

\[
\bigcap_{j=1}^{n+1} A_j = \left[ \bigcap_{j=1}^{n} A_j \right] \cap A_{n+1} \quad \text{(definition of intersection)}
\]

\[
= \left[ \bigcap_{j=1}^{n} A_j \right] \cup A_{n+1} \quad \text{(De Morgan's law)}
\]

\[
= \left[ \bigcup_{j=1}^{n} \bar{A_j} \right] \cup A_{n+1} \quad \text{(Inductive hypothesis)}
\]

\[
= \bigcup_{j=1}^{n+1} \bar{A_j} \quad \text{(definition)}
\]

5. These examples may convey the impression that when constructing an inductive proof, one just writes down immediately \(P(1)\) and \(P(n) \Rightarrow P(n+1)\). In fact, it is usually useful to look at several intermediate cases to get a feeling for what is going on.

Example: Suppose we want to find an expression for \(\sum_{j=1}^{n} j^2\). We might guess that it equals \(r(n+a)(n+b)(n+c)\), where \(r, a, b,\) and \(c\) are all real numbers, since we expect the power to increase by \(1\).

If so:

\[
\begin{align*}
 r(1+a)(1+b)(1+c) &= 1 \quad \text{(1.1)} \\
 r(2+a)(2+b)(2+c) &= 5 \quad \text{(1.2)} \\
 r(3+a)(3+b)(3+c) &= 14 \quad \text{(1.3)} \\
 r(4+a)(4+b)(4+c) &= 30 \quad \text{(1.4)}
\end{align*}
\]
First differences

\[ r \left[ a b + ac + bc + 3a + 3b + 3c + 7 \right] = 4 \]
\[ r \left[ a b + ac + bc + 5a + 5b + 5c + 19 \right] = 9 \]
\[ r \left[ ab + ac + bc + 7a + 7b + 7c + 37 \right] = 16 \]

Second differences

\[ r \left[ 2a + 2b + 2c + 12 \right] = 5 \]
\[ r \left[ 2a + 2b + 2c + 18 \right] = 7 \]

Third differences

\[ 6 r = 2 \quad \Rightarrow \quad r = \frac{1}{3} \]

Using 3.1
\[ \frac{2}{3} (a+b+c) = 1 \quad \Rightarrow \quad a+b+c = \frac{3}{2} \]

Using 2.1
\[ \frac{1}{3} (ab+ac+bc) + \frac{3}{2} + \frac{7}{3} = 4 \]

\[ (ab+ac+bc) = \frac{1}{2} \]

Using 1.1
\[ \frac{1}{3} \left[ abc + ab+ac+bc + a+b+c + 1 \right] = 1 \]
\[ abc = 0 \]

We choose \( a = 0 \)
\[ \Rightarrow b+c = \frac{3}{2} \quad , \quad bc = \frac{1}{2} \]
\[ \Rightarrow b = \frac{1}{2} \quad , \quad c = 1 \]

Hypothesis:
\[ \sum_{j=1}^{n} j^2 = \frac{1}{3} n \left( n + \frac{1}{2} \right) \left( n + 1 \right) \]
\[ = \frac{1}{6} n \left( 2n+1 \right) \left( n+1 \right) \]

Proof:
By construction \( P(1), P(2), P(3), P(4) \) are all true. Suppose \( P(n) \) is true

\[ \sum_{j=1}^{n} j^2 = \sum_{j=1}^{n} j^2 + (n+1)^2 = \frac{1}{3} n \left( n + \frac{1}{2} \right) (n+1) + (n+1)^2 \]
\[ = \frac{1}{3} (n+1) \left[ n \left( n + \frac{1}{2} \right) + 3(n+1) \right] = \frac{1}{3} (n+1) \left[ n^2 + \frac{7n}{2} + 3 \right] \]
\[
\frac{1}{3} (n+1)(n+\frac{3}{2})(n+2) = \frac{1}{3} \left[ (n+1) \left( \frac{n+3}{2} \right) \right] \left( n+1 \right) + 1
\]

5. Strong induction

a. In this case, we assume that \( P(j) \) is true for all \( j \leq n \) and we show that \( P(n+1) \) is true.

b. Our previous schematic was:
   
   \begin{align*}
   \text{Basis step: } & P(1) \\
   \text{Inductive step: } & P(n) \Rightarrow P(n+1) \ \forall \ n \in \mathbb{Z}^+
   \end{align*}

   Our new schematic is:

   \begin{align*}
   \text{Basis step: } & P(1) \\
   \text{Inductive step: } & (P(1) \land P(2) \land \ldots \land P(n)) \Rightarrow P(n+1)
   \end{align*}

   NOTE: While strong induction looks like it requires more, it is in fact equivalent to standard induction.
   
   It may, however, be easier to use.

c. Example: If \( n \in \mathbb{Z} \land n > 1 \), then \( n \) can be written as the product of primes.
   
   Basis step: \( P(2) \) is true since 2 is a prime.

   Inductive step: Assume \( P(j) \) is true for all \( j \leq n \).
   
   Case (i): \( n+1 \) is prime. In this case \( P(n+1) \) is immediately true.
Case (ii), \( n+1 \) is composite. Then, we may write \( n+1 = ab \), where \( 2 \leq a \leq b < n+1 \). Hence, both \( a \) and \( b \) can be decomposed into primes from our inductive assumption, and the result follows.

\[ a \quad \text{Example: Every amount of postage of 12 cents or more can be made up using 4-cent and 5-cent stamps.} \]

\begin{align*}
\text{ Basis step: } & \quad 12 \& = 3 \cdot 4 \& , \quad 13 \& = 2 \cdot 4 \& + 1 \cdot 5 \& \\
& \quad 14 \& = 1 \cdot 4 \& + 2 \cdot 5 \& , \quad 15 \& = 3 \cdot 5 \& \\
\text{ Inductive step: Suppose } n \geq 15 \text{ and we can form postage of } j \& \text{ where } 12 \leq j \leq n \text{ from 4-cent and 5-cent stamps. To form the postage for } n+1, \text{ we use the postage for } n-3 \text{ and add a 4-cent stamp.} \]

Note: In our basis step, we had to establish the result for steps, so that in the inductive step we could go back 3.

6. The well-ordering property
a. Axiom: Every non-empty set of non-negative integers has a least element. [We can use this to prove the validity of induction]
There must be a least \( N \) such that \( \sqrt{2} = M/N \).

Because \( M^2/N^2 = 2 \rightarrow M^2 = 2N^2 \).

We see, using this fact
\[
\frac{2N-M}{M-N} = \frac{(2N-M)N}{(M-N)N} = \frac{2N^2-MN}{(M-N)N} = \frac{M^2-MN}{(M-N)N} = \frac{(M-N)M}{(M-N)N} = \frac{M}{N}
\]

Since \( 1 < \sqrt{2} < 2 \), we have

\[
1 < M/N < 2 \quad \text{or} \quad N < M < 2N
\]

Subtracting \( N \), we find

\[
0 < M-N < N, \quad \text{which contradicts our hypothesis.}
\]

\( \Box \)

d. Mathematical Induction:
We can now prove the validity of mathematical deduction.

Given \( P(1) \) and \( P(k) \Rightarrow P(k+1) \), we also suppose \( \exists n \in \mathbb{Z}^+ \) such that \( \neg P(n) \). In this case, the set of integers for which \( P(n) \) is false is non-empty, and we denote its least element \( m \). We must have \( m \geq 1 \) since we are given \( P(1) \). In this case, \( P(m-1) \) must be true. \( P(m-1) \Rightarrow P(m) \) implies \( m \) is true, and we have a contradiction. \( \Box \)
C. Recursion and Structural Induction

1. In computer algorithms, one often defines functions and sets recursively.
   **Simple example:** \( a_n = 2^n \forall n \in \mathbb{N} \)

   We may also define \( a_0 = 1, a_{n+1} = 2a_n \forall n \in \mathbb{N} \)

Rosen pp. 177-179

2. Euclidean Algorithm

   a. This algorithm, known to the ancient Greeks, is a recursive algorithm for finding the greatest common divisor of two positive integers, written \( \gcd(a, b) \), \( a, b \in \mathbb{Z}^+ \).

   **Example:** Calculate \( \gcd(91, 287) \)

   1. Divide larger number by smaller
      \( 287 = 91 \cdot 3 + 14 \)
      \( \gcd(91, 287) = \gcd(14, 91) \)

   2. Divide larger number by smaller
      \( 91 = 14 \cdot 6 + 7 \)
      \( \gcd(14, 91) = \gcd(7, 14) \)

   3. Divide larger number by smaller
      \( 14 = 7 \cdot 2 \)
      \( \gcd(7, 14) = 7 \)
      \( \therefore \gcd(91, 287) = 7 \)

   Generally, to calculate \( \gcd(a, b) \), we proceed as follows.
Let \( r_0 = a \) and let \( r_1 = b \)  

We iterate recursively, writing  
\[
r_{j+1} = r_{j+1} g_{j+1} + r_{j+2} \quad 0 \leq r_{j+2} < r_{j+1}
\]

where \( j = 0 \) on the first iteration and proceeding through \( j = 1, 2, \ldots \), \( n-1 \)  

where \( n \) is the first \( j \)-value at which \( r_{j+2} = 0 \).  
\[
gcd(a, b) = r_n
\]

4.24

How do we know that this always terminates?

For definition of Rosen pseudo-code, see Appendix 2.

6. Pseudo-code (See Rosen 179)

\[
\text{procedure gcd}(a, b: \text{positive integers})
\]
\[
x_0 = a
\]
\[
y_0 = b
\]
\[
\text{while } y \neq 0
\]
\[
\text{begin}
\]
\[
r_i = x \mod y
\]
\[
x_i = y
\]
\[
y_i = r_i
\]
\[
\text{end} \{ gcd(a, b) = x_0 \}
\]

3. Recursively defined functions

a. Definition

Basis step: Specify the value of the function at 0

Recursive step: Give a rule for finding its value at any integer \( \geq 1 \) from small integers

b. Example: Recursive definition of \( F(n) = n! \)

Basis step: \( F(0) = 1 \)

Recursive step: \( F(n+1) = (n+1) F(n) \)
c. Fibonacci numbers, \( f_n, n \in \mathbb{N} \)
Basis step: \( f_0 = 0 \), \( f_1 = 1 \)
Recursive step: \( f_n = f_{n-1} + f_{n-2} \), \( n = 2, 3, 4, \ldots \)
\[
\begin{align*}
    f_2 &= 1+0 = 1, \quad f_3 = 1+1 = 2, \quad f_4 = 2+1 = 3, \\
    f_5 &= 3+2 = 5, \quad f_6 = 5+3 = 8, \quad f_7 = 8+5 = 13
\end{align*}
\]

\( \alpha \) is the "golden mean"

\[\alpha = \frac{\sqrt{5} - 1}{2}\]

\[\alpha^2 = \frac{3 + \sqrt{5}}{2} > 3 = f_4\]

**Lemma:** When \( n \in \mathbb{Z}, n \geq 3 \) then
\[
f_n > \alpha^{n-2}\]
where \( \alpha = \frac{\sqrt{5} - 1}{2} \)

**Proof:**

Basis step:
\[
\alpha < 2 = f_3
\]
\[
\alpha^2 = \frac{3 + \sqrt{5}}{2} > 3 = f_4
\]

Hence, \( P(3) \) and \( P(4) \) are true.

Inductive step: Assume \( P(j) \) is true for all \( j \geq 3 \), with \( k \geq 4 \). We must show that
\[
P(k+1) \text{ is true, or } f_{k+1} > \alpha^{k-1}
\]

We have \( \alpha^2 = \alpha + 1 \), which implies
\[
\alpha^{k-1} = \alpha^2 \cdot \alpha^{k-3} = (\alpha + 1) \alpha^{k-3} = \alpha^{k-2} + \alpha^{k-3}
\]

From the inductive hypothesis,
\[
f_{k+1} > \alpha^{k-2}, \quad f_k > \alpha^{k-1}
\]

Hence
\[
f_{k+1} = f_k + f_{k-1} > \alpha^{k-2} + \alpha^{k-3} = \alpha^{k-1}
\]

**Proof:**

\[\text{Lamé's Theorem: Let } a \text{ and } b \text{ be positive integers with } a > b. \text{ Then the number of divisions in the Euclidean algorithm to find } \text{gcd} (a, b) \text{ is less than or equal to five times the number of decimal digits in } b.\]