# Math 387, Spring 2025, Class Notes

Randall Holmes

February 16, 2025

## Contents

# 1 Jan 15 2025:

We did administrative stuff then read problems 1-7 in the Bogart book, section 1.2.

I'm going to write out my official definition of what a function is. We will talk about motivation for this later.

Let $S$ and $T$ be sets.

We say that $R$ is a relation from $S$ to $T$ iff $R$ is a triple $(S, T, G)$, where $G \subseteq S \times T$. $G$ is called the graph of $R$, and we say that $x\,R\,y$ is true iff $(x, y) \in G$.

We say that $f$ is a function from $S$ to $T$ (written $f : S \to T$) just in case $f$ is a relation $(S, T, G)$ from $S$ to $T$ and for each $x \in S$ there is exactly one $y$ in $T$ such that $(x, y) \in G$. We define $f(x)$, for each $x \in S$, aas the unique $y$ such that $(x, y) \in G$.

An alternative approach is to identify relations and functions with their graphs (so they are just subsets of $S \times T$), but this requires care in expression which most undergraduate textbooks don't bother with. We will discuss in detail what the problems are with the approach the book takes.

# 2 Jan 31, 2025

I gave a lecture on proofs by math induction relevant to our material

**Theorem:** Im going to use the notation ${}_nC_r$ instead of $\left( \begin{array}{c} n \\ r \end{array} \right)$ because it is easier to typset.

If ${}_nC_r$ is recursively defined for $0 \leq r \leq n$ with base cases ${}_nC_0 =_n C_n = 1$ and recurrence relation ${}_nC_{r+1} =_n C_r +_n C_{r-1}$ when $0 < r < n$, then ${}_nC_r = \frac{n!}{r!(n-r)!}$.

We prove this by induction on $n$.

**Basis step:** We need to prove the claim where $n = 0$. The only thing to show is that ${}_0C_0 = \frac{0!}{(0-0)!}$. The left side is defined as 1, and the right side readily computes to 1, so this is direct. (recall throughout this proof the recursive definition of the factorial: 0!=1, $(n+1)! = n!(n+1)$.

**Induction hypothesis:** Fix an arbitrary $k$ and assume that for $0 \leq r \leq k$, ${}_kC_r = \frac{k!}{r!(k-r)!}$.

**Induction goal:** Show that ${}_{k+1}C_r = \frac{(k+1)!}{r!((k+1)-r)!}$.

**Induction step of the proof:** The cases $r = 0$ and $r = k+1$ are direct from the recurive definition of binomial coefficients and direct factorial calculations.

${}_{k+1}C_0 = 1 = \frac{(k+1)!}{(k+1)!} = \frac{(k+1)!}{0!((k+1)-0)!}$

${}_{k+1}C_{k+1} = \frac{(k+1)!}{(k+1)!} = \frac{(k+1)!}{(k+1)!((k+1)-(k+1))!}$

Now suppose that $0 < r < k$.

${}_{k+1}C_r$ =[rec def]${}_kC_r + {}_kC_{r-1}$ =[ind hyp] $\frac{k!}{r!(k-r)!} + \frac{k!}{(r-1)!(k-(r-1))!}$ [algebra] $= \frac{k!}{r!(k-r)!} + \frac{k!}{(r-1)!((k-r)+1)!}$ =[algebra, aiming for a common denominator]$\frac{k!(k-r)}{r!(k-r)!(k-r)} + \frac{k!r}{((r-1)!r)(k-(r-1))!}$

= [rec def of factorial]$\frac{k!(k-r)}{r!((k-r)+1)!} + \frac{k!r}{r!(k-(r-1))!} = \frac{k!(k-r)}{r!((k-r)+1)!} + \frac{k!r}{r!)(k-(r-1))!} = \frac{k!(k-r)}{r!((k+1)-r)!} + \frac{k!r}{r!)((k+1)-r))!} = \frac{k!k}{r!((k+1)-r)!} = \frac{(k+1)!}{r!((k+1)-r)!}$

which completes the proof.

It is worth noting that this is neither the way we defined ${}_nC_r$ nor the way we proved this theorem. The definition and argument above are not combinatorial (they are not about counting). Nonetheless this definition and proof are useful.

Our official definition is that ${}_nC_r$ is the number of $r$ element subsets in an $n$ element set.

Our proof of the identity (already familiar but we review it) by combinatorial methods is via the counting of $r$-element ordered lists. By the general product principle, there are $n(n-1) \cdot (n-(r-1) = \prod i = 0^{r-1}(n-i) = n_r$ ordered lists of length $r$ of distinct elements taken from an $n$-element set.

Now partition the collection of ordered lists into blocks determined by their range (a list is a function with domain an initial segment of the natural natural numbers, so it has a range...): the possible ranges are exactly the $r$ elements subsets of the $n$ element set. So there are ${}_nC_r$ blocks in the partition by the set based official definition of this notation.

Each of the blocks of the partition has $r!$ elements (the different orders in which the $r$ elements of the range can appear).

The Quotient Principle is a backward version of the product principle: if we have a set $A$ of size $x$ with a partition $P$ each of whose blocks is of size $y$, then the size of $P$ must be $\frac{x}{y}$.

It follows that the partition is of size $\frac{n_r}{r!} = \frac{n!}{r!(n-r)!}$, the same result as above but as the result of a counting argument.

**Theorem (the binomial theorem):** $(x+y)^n = \sum_{i=0}^{n} {}_nC_i x^{n-i} y^i$

We prove this by induction on $n$.

**Basis step:** $(x+y)^0 = 1 = ({}_0C_0)x^{0-0}y^0 = \sum_{i=0}^{0}({}_0C_i)x^{0-i}y^i$

**Induction hypothesis:** For an arbitrary $k$, assume that $(x+y)^k = \sum_{i=0}^{k}({}_kC_i)x^{k-i}y^i$.

**Induction goal:** Prove that $(x+y)^k = \sum_{i=0}^{k+1}({}_{k+1}C_i)x^{(k+1)-i}y^i$.

**Induction step of the proof:**

$$(x+y)^{k+1} = (x+y)^k(x+y)$$

$$= (x+y)^k(x+y) = (x+y)^k x + (x+y)^k y$$

Now apply the induction hypothesis
$= x(\sum_{i=0}^{k}({}_kC_i)x^{k-i}y^i) + y(\sum_{i=0}^{k}({}_kC_i)x^{k-i}y^i)$
apply properties of summations which should not be mysterious
$= \sum_{i=0}^{k}({}_kC_i)x^{(k+1)-i}y^i + \sum_{i=0}^{k}({}_kC_i)x^{k-i}y^{i+1}$
Notice that on the left (the term where we added an $x$ factor) we have the powers of $x$ and $y$ that we want in the goal, but on the right we do not. We start to fix this by renaming the dummy variable in the right hand term to $j$.
$= \sum_{i=0}^{k}({}_kC_i)x^{(k+1)-i}y^i + \sum_{j=0}^{k}({}_kC_j)x^{k-j}y^{j+1}$
We want the power of $y$ in the right term to be $i$. We can do this by setting $j = i-1$, with the following result.
$= \sum_{i=0}^{k}({}_kC_i)x^{(k+1)-i}y^i + \sum_{i=1}^{k+1}({}_kC_{i-1})x^{k-(i-1)}y^i$
and further
$= \sum_{i=0}^{k}({}_kC_i)x^{(k+1)-i}y^i + \sum_{i=1}^{k+1}({}_kC_{i-1})x^{(k+1)-i}y^i$

We now have similar terms to add on both sides but we need to pull ou the first term of the left hand sum and the last term of the right hand sum, so that they are summed over the same indices.
$= ({}_kC_0)x^{(k+1)-0}y^0 + \sum_{i=1}^{k}({}_kC_i)x^{(k+1)-i}y^i + \sum_{i=1}^{k}({}_kC_{i-1})x^{(k+1)-i}y^i + ({}_kC_k)x^{(k+1)-(k+1)}y^{k+1}$
further
$= x^{k+1} + \sum_{i=1}^{k}({}_kC_i + {}_k\,C_{i-1})x^{(k+1)-i}y^i + y^{k+1}$
and by the recurrence relation on binomial coefficients, and the fact that the first and last terms are correct,
$= x^{k+1} + \sum_{i=1}^{k}({}_{k+1}C_i)x^{(k+1)-i}y^i + y^{k+1} = \sum_{i=0}^{k+1}({}_{k+1}C_i)x^{(k+1)-i}y^i$
This is not really a combinatorial proof, but it is very relevant to combinatorics (the theorem is useful) and the ability to manipulation indexed sum and product notation is useful in combinatorics (and in other areas of math).

# 3 Homework 3

This will be due on Friday the 7th, unless there are serious protests. I think you should have time; I'm sorry that I am only posting it on Monday.

1. Do problem 49 in Bogart. Write about your thinking as you work on it; this is perhaps an example of the proper use of the book for guided discovery (remember that we already talked about lattice paths in the other book).
2. Do problem 50 in Bogart. Write about your thinking as you work on it; this is perhaps an example of the proper use of the book for guided discovery (remember that we already talked about lattice paths in the other book).
3. Do problem 51 in Bogart (you may be saved on this one because we may do it in class: but I still want you to look at it beforehand, so approach it as an assigned problem).
4. Do problem 55 in Bogart
5. Do problem 56 in Bogart
6. Do problem 58 in Bogart

# 4 Induction proofs about sets: the pigeonhole principle and other obvious statements

The Pigeonhole Principle. stated informally in terms of pigeons, says that if you have $m$ pigeons to put in $n$ boxes, and $m > n$, then there must be two pigeons put in the same box. Pigeons are sociable and like to nest together, no animal cruelty here.

There is a function in this problem: the function $B$ which sends a pigeon $p$ to the box $B(p)$ in which it nests. What is claimed is that if the size $m$ of the domain of $B$ is greater than the size $n$ of the range of $B$ then $B$ is not an injection: there are pigeons $p$ and $q$ such that $B(p) = B(q)$.

**Theorem (Pigeonhole Principle):** If $A$ and $B$ are finite sets and $|A| > |B|$ then no function $f : A \to B$ is an injection.

We are going to prove this, but it will require a bit of work.

**Definition:** The relation $A \sim B$, read "$A$ is the same size as $B$" is defined as holding exactly if there is a bijection from $A$ to $B$. We state without proof that this is an equivalence relation: the reason for this is that the identity map from $A$ to $A$ witnesses reflexivity of $\sim$, the fact that the inverse of a bijection from $A$ to $B$ is a bijection from $B$ to $A$ witnesses symmetry of $\sim$, and the fact that if $f : A \to B$ and $g : B \to C$ are bijections then $g \circ f : A \to C$, their composition, witnesses transivity of $\sim$.

**Definition:** If there is a bijection from $\{1, \ldots, n\}$ to $A$, we say that $n$ is a size of $A$. In addition, the empty set has size 0. Clearly, this indicates that we can count the elements of $A$ in some order and get to $n$.

**Definition with justifying theorem:** We say a set $A$ is finite iff there is a natural number such that $n$ is a size of $A$. For finite sets $A$ we would like to define $|A|$ as the size of $A$, but we do need to prove a theorem to justify this: No set has more than one size.

**Proof of the theorem justifying the previous definition:** We prove by induction on $n$ that if $A$ has size $n$ and $m \neq n$, then $A$ does not have size $m$.

Basis: if $n = 0$, then $A$ is empty and $m > 0$, and there can be no bijection from $\{1, \ldots, m\}$ to the empty set, since there cannot even be a function like this (what is its value at 1?).

Induction step: suppose that we know that if any $A$ has size $k$ and $k \neq l$,, then $A$ does not have size $l$.

Let $A$ be a set of size $k+1$ and $l \neq k+1$. Our aim is to show that $A$ cannot be of size $l$. If $l = 0$, $A$ cannot be of size $l$ because $A$ is not empty. Otherwise, let $m = l - 1$, and notice that $m \neq k$. Let $f$ be a bijection from $\{1, \ldots, k+1\}$ to $A$. Let $g$ be a bijection from $\{1, \ldots, l\}$ to $A$. We define a map $g_1$: if $f(k+1) = g(l)$ then $g_1$ is defined as $g$. Otherwise, we define $g_1(i)$ as $g(l)$ if $g(i) = f(k+1)$, as $f(k+1)$ if $i = l$, and otherwise as $g(i)$. Clearly $g_i$ is a bijection from $\{1, \ldots, l\}$ to $A$, obtained by swapping at most one pair of values so that $g_1(l) = f(k+1)$. Now the map $f^-(i) = f(i)$ for $i \in \{1, \ldots, k\}$ and $g^-(i) = g_1(i)$ for $i \in \{0, \ldots, l-1\}$ witness the fact that $A \setminus \{f(k+1\}$ is of size $k$ and $A \setminus \{g_1(l)\}$ [the same set, because $g_1(l) = f(k+1)$!] is of size $l-1$. By ind hyp it follows that $k = l-1$, so $k+1 = l$, completing the proof.

Now we can prove the pigeonhole principle. We use the convenient notation $[n]$ for $\{1, \ldots, n\}$ (and $[0]$ for the empty set).

**Proof of the pigeonhole principle:** It is enough to prove that for $m > n$, there is no injection from $\{1, \ldots, m\}$ to $\{1, \ldots, n\}$. If we have $|A| = m > n = |B|$ and we have an injection from $A$ to $B$, and a bijection $g : [m] \to A$ and a bijection $h : [n] \to B$, then $h^{-1} \circ f \circ g$ would be a bijection from $[m]$ to $[n]$. This uses the fairly obvious fact that the composition of a bijection with an injection is an injection, twice.

We prove the claim above by induction on $n$.

The basis step is evident: there cannot be an injection from $[m]$ with $m > 0$ to $[0]$, the empty set, since there cannot even be such a function.

Suppose it has been shown that for no $m > k$ can there be an injection from $[m]$ to $[k]$.

Suppose for the sake of a contradiction that we have $m > k+1$ and an injection $g$ from $[m]$ to $[k+1]$. By ind hyp we can suppose that $k+1$ is in the range of $g$: otherwise, by restricting the codomain of

$g$ to exclude $k+1$, we get an injection from $[m]$ to $[k]$ immediately, contradicting ind hyp.

Define a possibly different injection $g_1$: if $g(m) = k+1$, $g = g_1$: otherwise define $g_1(i)$ as $g(m)$ if $g(i) = k+1$, as $m$ if $i = k+1$, and otherwise as $g(i)$.

Now the map $g^-$ defined as $g_1(i)$ for $i < m$ is an injection from $[m-1]$ to $[k]$, contradicting the induction hypothesis.

We used the same value-swapping maneuver in the two previous arguments, but not in exactly the same way. I do note that the pigeonhole principle does have the theorem justifying the definition of $|A|$ as a special case: you might want to think out why this is true.

Now there is a similar result about surjections.

**Theorem:** If $A$ and $B$ are finite sets with $|A| < |B|$, there is no surjection from $A$ to $B$,

**Proof of theorem:** For reasons similar to those given in the argument about injections, it is enough to show that if $m < n$, there is no surjection from $[m]$ to $[n]$: if we had general sets with $|A| = m < n = |B|$ and a surjection from $A$ to $B$, we could use counting maps to build a surjection from $[m]$ to $[n]$.

**Theorem:** If $A, B$ are finite sets and $|A| < |B|$, there is no surjection from $A$ to $B$.

**Proof:** It is enough to prove that there is no surjection from $[m]$ to $[n]$ where $m < n$.

Suppose that $m < n$ and there is a surjection $f : [m] \to [n]$. Define $f^*(i)$ for each $i \in [n]$ as the smallest $j \in [m]$ such that $f(j) = i$. There is such a $j$ because $f$ is a surjection. It is obvious that $f^*$ is an injection. But there cannot be an injection from $[n]$ to $[m]$, because $m < n$, by the pigeonhole principle. So we are done.

**Theorem:** If $A$ and $B$ are finite sets of the same size and $f : A \to B$, then $f$ is an injection if and only if $f$ is a surjection.

**Lemma:** Any proper subset $B$ of a finite set $A$ is finite and has $|B| < |A|$.

**Proof:** We prove this by induction on the size of $A$.

The basis is trivially true because a set of size 0 has no proper subsets at all.

Suppose that every proper subset $B$ of any set $A$ of size $k$ has $B$ finite and $|B| < k$.

Let $B$ be a proper subset of a set $A$ of size $k+1$: our aim is to show that $B$ is finite and $|B| < k+1$.

Let $f : [k+1] \to A$ be a bijection. If $f(k+1) \notin B$ we are done, because then $B$ is a subset of the range of the restriction of $f$ to $[k]$, which is a set of size $k$, so $B$ has size less or equal to $k$ (it is either a proper subset of the image or the entire image) and so less than $k+1$.

If $f(k+1) \in B$ observe that $A \backslash f(k+1)$, a set of size $k$, has $B \backslash \{f(k+1)\}$ as a proper subset (if these two sets were equal, $A = B$ would follow) so $|B \backslash \{f(k+1)\}|$ exists (this set is finite) and $|B \backslash \{f(k+1)\}| = |B| - 1 < k$, so $|B| < k+1$ as desired.

**Proof of Theorem:** If $f : A \to B$ were an injection but not a surjection, then by modifying the codomain of $f$ you would get an injection from $A$ to a proper subset of $B$, which would be a smaller finite set by the Lemma, contradicting the pigeonhole principle.

If $f : A \to B$ were a surjection but not an injection, then $f^*$ defined just as in the proof of the previous Theorem would be an injection from $B$ to a proper subset of $A$, a finite set of smaller size, and this would contradict the pigeonhole principle. Alternatively, find $a_1$ and $a_2$ such that $f(a_1) = f(a_2)$ and $a_1 \neq a_2$. The restriction of $f$ to $A \backslash \{a_2\}$ is still a surjection to $B$, but $A \backslash \{a_2\}$ is a finite set smaller than $B$, contradicting the previous Theorem which asserts that there is no surjection from a smaller finite set to a larger finite set.

# 5 Induction proofs from recursive definitions: recursive definitions of exponentation and summation explored

This is a discussion of the same topic as problems 75-78 in Bogart, with some extra stuff.

**Problem 75:** We conjecture that the number of functions from $[m]$ to $[n]$ is $n^m$ (using the same handy abbreviation $[k]$ for $\{1, \ldots, k\}$)

We prove this by induction.

The basis case ($m = 0$): there is exactly one function from $[0] = \emptyset$ to $[n]$, and $n^0 = 1$. (in discrete mathematics, we define $0^0 = 1$, though it is an indeterminate form in calculus).

Let $k$ be arbitrary and suppose there are $n^k$ functions from $[k]$ to $[n]$.

Our goal is to show that there are $n^{k+1}$ functions from $[k+1]$ to $[n]$.

Each function $f$ from $[k+1]$ to $n$ determines an ordered pair $(f^-, y)$ uniquely where $f^- : [k] \to [n]$ is defined by $f^-(i) = f(i)$ for $i \in [k]$, and $y = f(k+1)$.

For any pair $(f^-, y)$ where $f^- : [k] \to [n]$ and $y \in [n]$ we can define a uniquely determined function $f$ defined by $f(i) = f^-(i)$ for $i \in [k]$ and $f(k+1) = y$ [we can explicitly write $f$ as

$$([k+1], [n], \texttt{graph}(f^-) \cup \{(k+1, y)\})$$

using our fancy definition of functions as ordered triples of domain, codomain, and graph).

In other words, there is a bijection between the set of functions $f$ from $[k+1]$ to $[n]$ and the Cartesian product of the set of functions from $[k] \to [n]$ and the set $[n]$. By inductive hypothesis and the simplest form of the product principle, the size of the cartesian product is $n^k \cdot n = n^{k+1}$, which establishes the expected value for the size of the set of functions from $[k+1]$ to $[n]$.

**Problem 76:** Define $a^n$ recursively: $a^0 = 1; a^{k+1} = a^k \cdot a$.

We prove that $a^{m+n} = a^m \cdot a^n$.

Of course there is the informal argument that $a^{m+n}$ is the product of $m+n$ copies of $a$, and $a^m \cdot a^n$ is the product of the product of $m$ copies of $a$ and the product of $n$ copies of $a$, which of course by regrouping (commutative and associative properties of addition) is the same thing.

This is awfully informal and generally written with dots, a sign of cheating. We prove it by induction on $n$.

The basis case, $n = 0$: $a^{m+0} = a^m = a^m \cdot 1 =^* a^m \cdot a^0$, starring the place where the recursive definition is used.

Suppose we have established that $a^{m+k} = a^m \cdot a^k$.

Then $a^{m+(k+1)} = a^{(m+k)+1} =^* a^{m+k} \cdot a = (!!!)(a^m \cdot a^k) \cdot a = a^m \cdot (a^k \cdot a) =^* a^m \cdot a^{k+1}$, starring application of the definition and !!! for use of ind hyp. I was very careful here about uses of the associative laws for addition and multiplication, because they are doing the real work and should not be hidden.

**Problem 78:** We give the recursive definition of summation notation: for $m \leq n$ and $\{x_i\}$ a sequence defined at least for $m \leq i \leq n$ (it might have a larger domain), define $\sum_{i=m}^{m} x_i$ as $x_m$ and define $\sum_{i=m}^{k+1} x_i$ as $(\sum_{i=m}^{k} x_i) + x_{k+1}$.

The author usually has $m = 1$ but this notation is used with other starting indices, so we might as well give a fully general definition. We will use the generality.

Prove that $b \cdot \sum_{i=1}^{n} a_i = \sum_{i=1}^{n} (b \cdot a_i)$.

Basis ($n = 1$): $b \cdot \sum_{i=1}^{1} a_i =^* b \cdot a_1 =^* \sum_{i=1}^{1} (b \cdot a_i)$. As before, a star indicates use of the definition.

Induction step: Suppose $b \cdot \sum_{i=1}^{k} a_i = \sum_{i=1}^{k} b \cdot a_i$.

Then $b \cdot \sum_{i=1}^{k+1} a_i =^* b \cdot ((\sum_{i=1}^{k} a_i) + a_{k+1}) = b \cdot (\sum_{i=1}^{k} a_i) + b \cdot a_{k+1} = (!!!)(\sum_{i=1}^{k} (b \cdot a_i)) + b \cdot a_{k+1} =^* \sum_{i=1}^{k+1} b \cdot a_i$

**The reverse and add proof of the formula for sums of arithmetic sequences:** This is an extended example, possibly beating something easy to death. But there really is something to see here about how informal manipulations of notation can be turned into something more precise.

An arithmetic sequence is a sequence $A_i$ defined by $A_0 = a; A_{n+1} = A_n + d$, where $a$ is the first term (cleverly indexed by 0 to simplify a formula) and $d$ is the common difference between successive terms.

The formula we want to prove is that $\sum_{i=0}^{n} a_i = \frac{A_0+A_n}{2} \cdot (n+1)$: the sum of a finite arithmetic sequence is the average of the first term and the last term of the sequence multiplied by the number of terms.

An informal argument, infected with dots:

$A_0 + A_1 + \ldots + A_{n-1} + A_n = x$ (the sum has a value $x$ of course), so

$A_n + A_{n-1} + \ldots + A_1 + A_0 = x$ so

$(A_0+A_n)+(A_1+A_{n-1})+\ldots(A_i+A_{n-i})+\ldots+(A_{n-1}+A_1)+(A_n+A_0) = 2x$

and each of these terms $A_i + A_{n-i}$ is equal to $(a+id)+(a+(n-i)d) = 2a+nd$ and there are $n+1$ terms so

$(2a+nd) \cdot (n+1) = 2x$

so $x = \frac{a+(a+nd)}{2} \cdot (n+1) = \frac{A_0+A_n}{2} \cdot (n+1)$

This of course is an informal argument.

We prove Lemmas needed to prove the same theorem formally but in fact in the same way.

**Lemma 1:** $\sum_{i=m}^{n} a = a(n-m+1)$ [adding terms which are all the same is multiplication]

**Proof:** By induction on $n$, starting at $m$.

basis ($n = m$): $\sum_{i=m}^{m} a = a = a(m-m+1)$

induction step: suppose $\sum_{i=m}^{k} a = a(k-m+1)$

Then $\sum_{i=m}^{k+1} a =^* (\sum_{i=1}^{k} a) + a = (!!!) = a(k-m+1) + a = a((k+1)-m+1)$

**Lemma 2:** $\sum_{i=m}^{n}(a_i + b_i) = \sum_{i=m}^{n} a_i + \sum_{i=1}^{n} b_i$

This will be assigned as homework.

**Lemma 3:** $\sum_{i=m}^{n} a_i = \sum_{i=m-j}^{n-j} a_{i+j}$ [change of variables: stating this a lot more generally than I did in class; it is worth noting that in the application of Lemma 3 that appears below, $j = -1$]

Prove by induction on $n$, starting at $m$

Basis ($n = m$): $\sum_{i=m}^{m} a_i =^* a_m = a_{(m-j)+j} =^* \sum_{i=m-j}^{m-j} a_{i+j}$

Induction step: Assume that $\sum_{i=m}^{k} a_i = \sum_{i=m-j}^{k-j} a_{i+j}$.

Then $\sum_{i=m}^{k+1} a_i =^* (\sum_{i=m}^{k} a_i) + a_{k+1} = (!!!)(\sum_{i=m-j}^{k-j} a_{i+j}) + a_{k+1} = (\sum_{i=m-j}^{k-j} a_{i+j}) + a_{((k+1)-j)+j} =^* \sum_{i=m-j}^{(k+1)-j} a_{i+j}$ [using the fact that $(k+1)-j = (k-j)+1$ implicitly to save two extra steps].

**Lemma 4:** If $m < n$, $\sum_{i=m}^{n} a_i = \sum_{i=m+1}^{n} a_i + a_m$ [peel off the first term instead of the last term]

Prove by induction on $n$, starting at $m+1$

basis step ($n = m+1$): $\sum_{i=m}^{m+1} a_i = \sum_{i=m}^{m} a_i + a_{m+1} = a_m + a_{m+1} = a_{m+1} + a_m = \sum_{i=m+1}^{m+1} + a_m$

induction step: Suppose that $\sum_{i=m}^{k} a_i = \sum_{i=m+1}^{k} a_i + a_m$.

Then $\sum_{i=m}^{k+1} a_i =^* \sum_{i=m}^{k} + a_{k+1} = (!!!) \sum_{i=m+1}^{k} + a_m + a_{k+1} = \sum_{i=m+1}^{k} + a_{k+1} + a_m =^* \sum_{i=m+1}^{k+1} k + a_m$

**Lemma 5:** $\sum_{i=m}^{n} a_i = \sum_{i=m}^{n} a_{(m+n)-i}$ [reversing the indexing of a sum]

Prove by induction on $n$, starting at $m$

basis step ($n = m$): $\sum_{i=m}^{m} a_i = a_m = a_{(m+m)-m} = \sum_{i=m}^{m} a_{(m+m)-i}$

induction step: suppose $\sum_{i=m}^{k} a_i = \sum_{i=m}^{k} a_{(m+n)-i}$

$\sum_{i=m}^{k+1} a_i = (\sum_{i=m}^{k} a_i) + a_{k+1} = (\sum_{i=m}^{k} a_{(m+k)-i}) + a_{k+1} =$ [using Lemma 3] $(\sum_{i=m+1}^{k+1} a_{(m+k)-(i-1)}) + a_{(m+(k+1))-m} = (\sum_{i=m+1}^{k+1} a_{(m+(k+1))-i}) + a_{(m+(k+1))-m} = \sum_{i=m}^{k+1} a_{(m+(k+1))-i}$ [the last step used Lemma 4]

**The main result:** $\sum_{i=0}^{n} A_i = \frac{1}{2}(\sum_{i=0}^{n} A_i + \sum_{i=0}^{n} A_i) =$ [Lemma 5]
$\frac{1}{2}(\sum_{i=0}^{n} A_i + \sum_{i=0}^{n} A_{n-i}) =$[Lemma 2]$\frac{1}{2} \sum_{i=0}^{n}(A_i + A_{n-i}) =$
$\frac{1}{2} \sum_{i=0}^{n}((a + id) + (a + (n-i)d) =$[Lemma 1]$\frac{1}{2} \sum_{i=0}^{n}(2a + nd)$
$= \frac{1}{2}(2a + nd)(n+1) = \frac{1}{2}(A_0 + A_n)(n+1)$

The interesting thing is that the method we use for proving the main result is actually the same as the informal method we started with,,,with the fancy moves justified.

# 6 Homework 5, posted 2/16/2025, due 2/21/2025

A short assignment, since class was cancelled Friday. This took me quite a while to get to because type setting the notes on Wednesday's lecture was quite time consuming.

Prove the identities $(a^m)^n = a^{mn}$ and $(ab)^n = a^n b^n$ using the recursive definition of exponentiation and mathematical induction.

Prove Lemma 2 above, $\sum_{i=m}^{n}(a_i + b_i) = \sum_{i=m}^{n} a_i + \sum_{i=1}^{n} b_i$ using the recursive definition of summation and mathematical induction.