

Today's topics

- Mathematical reasoning
 - More proof techniques
 - Sequences
 - Summations
- Reading: Sections 3.1-3.2
- Upcoming
 - Induction

Forward Reasoning

- Have premises p , and want to prove q .
 - Find a s_1 such that $p \rightarrow s_1$
 - Then, modus ponens gives you s_1 .
 - Then, find an $s_2 \ni$ (such that) $s_1 \rightarrow s_2$.
 - Then, modus ponens gives you s_2 .
 - And hope to eventually get to an $s_n \ni s_n \rightarrow q$.
- The problem with this method is...
 - It can be tough to see the path looking from p .

Backward Reasoning

- It can often be easier to see the *very same path* if you just start looking from the conclusion q instead...
 - That is, *first* find an s_{-1} such that $s_{-1} \rightarrow q$.
 - *Then*, find an $s_{-2} \ni s_{-2} \rightarrow s_{-1}$, and so on...
 - Working back to an $s_{-n} \ni p \rightarrow s_{-n}$.
- Note we *still* are using *modus ponens* to propagate truth *forwards* down the chain from p to s_{-n} to ... to s_1 to q !
 - We are *finding* the chain *backwards*, but *applying* it *forwards*.
 - This is not quite the same thing as an indirect proof...
 - In that, we would use *modus tollens* and $\neg q$ to prove $\neg s_{-1}$, etc.
 - However, it is similar.

Backward Reasoning Example

Example 1

- **Theorem:**

$$\forall a > 0, b > 0, a \neq b: (a+b)/2 > (ab)^{1/2}.$$

- **Proof:**

- Notice it is not obvious how to go from the premises $a > 0, b > 0, a \neq b$ directly forward to the conclusion $(a+b)/2 > (ab)^{1/2}$.
- So, let's work *backwards* from the conclusion, $(a+b)/2 > (ab)^{1/2}$!

Stone Game Example

Example 2

- Game rules:
 - There are 15 stones in a pile. Two players take turns removing either 1, 2, or 3 stones. Whoever takes the last stone wins.
- **Theorem:** There is a strategy for the first player that guarantees him a win.
- How do we prove this? Constructive proof...
 - Looks complicated... How do we pick out the winning strategy from among all possible strategies?
 - Work backwards from the endgame!

Working Backwards in the Game

- Player 1 wins if it is player 2's turn and there are no stones...
- P1 can arrange this if it is his turn, and there are 1, 2, or 3 stones...
- This will be true as long as player 2 had 4 stones on his turn...
- And so on...

<u>Player 1</u>	<u>Player 2</u>
	0
1, 2, 3	
	4
5, 6, 7	
	8
9, 10, 11	
	12
13, 14, 15	

“Forwardized” version

- **Theorem.** Whoever moves first can always force a win.
 - **Proof.** Player 1 can remove 3 stones, leaving 12. After player 2 moves, there will then be either 11, 10, or 9 stones left. In any of these cases, player 1 can then reduce the number of stones to 8. Then, player 2 will reduce the number to 7, 6, or 5. Then, player 1 can reduce the number to 4. Then, player 2 must reduce them to 3, 2, or 1. Player 1 then removes the remaining stones and wins.

Proof by Cases Example

Example 3

- **Theorem:** $\forall n \in \mathbf{Z} \neg(2|n \vee 3|n) \rightarrow 24|(n^2-1)$
 - **Proof:** Since $2 \cdot 3 = 6$, the value of $n \bmod 6$ is sufficient to tell us whether $2|n$ or $3|n$. If $(n \bmod 6) \in \{0, 3\}$ then $3|n$; if it is in $\{0, 2, 4\}$ then $2|n$. Thus $(n \bmod 6) \in \{1, 5\}$.
 - **Case #1:** If $n \bmod 6 = 1$, then $(\exists k) n = 6k + 1$.
 $n^2 = 36k^2 + 12k + 1$, so $n^2 - 1 = 36k^2 + 12k = 12(3k + 1)k$. Note $2|(3k + 1)k$ since either k or $3k + 1$ is even. Thus $24|(n^2 - 1)$.
 - **Case #2:** If $n \bmod 6 = 5$, then $n = 6k + 5$. $n^2 - 1 = (n - 1) \cdot (n + 1) = (6k + 4) \cdot (6k + 6) = 12 \cdot (3k + 2) \cdot (k + 1)$. Either $k + 1$ or $3k + 2$ is even. Thus, $24|(n^2 - 1)$.

Proof by Examples?

- A universal statement can never be proven by using examples, unless the universe can be validly reduced to only finitely many examples, and your proof covers all of them!
- **Theorem:** $\neg \exists x, y \in \mathbf{Z}: x^2 + 3y^2 = 8$. Example 4
 - **Proof:** If $|x| \geq 3$ or $|y| \geq 2$ then $x^2 + 3y^2 > 8$. This leaves $x^2 \in \{0, 1, 4\}$ and $3y^2 \in \{0, 3\}$. The largest pair sum to $4 + 3 = 7 < 8$.

A Constructive Existence Proof

Example 7

- **Theorem:** For any integer $n > 0$, there exists a sequence of n consecutive composite integers.
- Same statement in predicate logic:
 $\forall n > 0 \exists x \forall i (1 \leq i \leq n) \rightarrow (x+i \text{ is composite})$
- Proof follows on next slide...

The proof...

- Given $n > 0$, let $x = (n + 1)! + 1$.
- Let $i \geq 1$ and $i \leq n$, and consider $x+i$.
- Note $x+i = (n + 1)! + (i + 1)$.
- Note $(i+1)|(n+1)!$, since $2 \leq i+1 \leq n+1$.
- Also $(i+1)|(i+1)$. So, $(i+1)|(x+i)$.
- $\therefore x+i$ is composite.
- $\therefore \forall n \exists x \forall 1 \leq i \leq n : x+i$ is composite. Q.E.D.

Nonconstructive Existence Proof

- **Theorem:** There are infinitely many prime numbers.
 - Any finite set of numbers must contain a maximal element, so we can prove the theorem if we can just show that there is no *largest* prime number.
 - *I.e.*, show that for any prime number, there is a larger number that is *also* prime.
 - More generally: For *any* number, \exists a larger prime.
 - Formally: Show $\forall n \exists p > n : p \text{ is prime}$.

The proof, using *proof by cases*...

- Given $n > 0$, prove there is a prime $p > n$.
- Consider $x = n! + 1$. Since $x > 1$, we know that $(x \text{ is prime}) \vee (x \text{ is composite})$.
- **Case 1:** Suppose x is prime. Obviously $x > n$, so let $p = x$ and we're done.
- **Case 2:** x has a prime factor p . But if $p \leq n$, then $p \bmod x = 1$. So $p > n$, and we're done.

Adapting Existing Proofs

Example 5

- **Theorem:** There are infinitely many primes of the form $4k+3$, where $k \in \mathbb{N}$.
 - Recall we proved there are infinitely many primes because if p_1, \dots, p_n were all the primes, then $(\prod p_i)+1$ must be prime or have a prime factor greater than p_n , \Rightarrow contradiction!
 - **Proof:** Similarly, suppose q_1, \dots, q_n lists all primes of the form $4k+3$,
 - and analogously consider $Q = 4(\prod q_i)+3$.
 - Unfortunately, since $q_1 = 3$ is possible, $3|Q$ and so Q does have a prime factor among the q_i , so this doesn't work!
 - So instead, consider $Q = 4(\prod q_i)-1 = 4(\prod q_i-1)+3$. This has the right form, and has no q_i as a factor since $\forall i: Q \equiv -1 \pmod{q_i}$.

Conjecture and Proof

Example 6

- We know that some numbers of the form $2^p - 1$ are prime when p is prime.
 - These are called the Mersenne primes.
- Can we prove the inverse, that $a^n - 1$ is composite whenever either $a > 2$, or ($a = 2$ but n is composite)?
 - All we need is to find a factor greater than 1.
- Note $a^n - 1$ factors into $(a - 1)(a^{n-1} + \dots + a + 1)$.
 - When $a > 2$, $(a - 1) > 1$, and so we have a factor.
 - When n is composite, $\exists r, s > 1: n = rs$. Thus, given $a = 2$, $a^n = 2^n = 2^{rs} = (2^r)^s$, and since $r > 1$, $2^r > 2$ so $2^n - 1 = b^s - 1$ with $b = 2^r > 2$, which now fits the first case.

Conjecture & Counterexamples

Example 8

- **Conjecture:** \forall integers $n > 0$, $n^2 - n + 41$ is prime.
 - Hm, let's see if we can find any counter-examples:
 - $1^2 - 1 + 41 = 41$ (prime)
 - $2^2 - 2 + 41 = 4 - 2 + 41 = 43$ (prime)
 - $3^2 - 3 + 41 = 9 - 3 + 41 = 47$ (prime) Looking good so far!!
 - Can we conclude after showing that it checks out in, say, 20 or 30 cases, that the conjecture must be true?
- **NEVER NEVER NEVER NEVER NEVER!**
 - Of course, $41^2 - 41 + 41$ is divisible by 41!!

Sequences

- A *sequence* or *series* $\{a_n\}$ is identified with a *generating function* $f:S \rightarrow A$ for some subset $S \subseteq \mathbf{N}$ and for some set A .
 - Often we have $S = \mathbf{N}$ or $S = \mathbf{Z}^+ = \mathbf{N} - \{0\}$.
 - Sequences may also be generalized to *indexed sets*, in which the set S does *not* have to be a subset of \mathbf{N} .
 - For general indexed sets, S may not even be a set of numbers at all.
- If f is a generating function for a series $\{a_n\}$, then for $n \in S$, the symbol a_n denotes $f(n)$, also called *term n* of the sequence.
 - The *index* of a_n is n . (Or, often i is used.)
- A series is sometimes denoted by listing its first and/or last few elements, and using ellipsis (...) notation.
 - E.g., “ $\{a_n\} = 0, 1, 4, 9, 16, 25, \dots$ ” is taken to mean $\forall n \in \mathbf{N}, a_n = n^2$.

Sequence Examples

- Some authors write “the sequence a_1, a_2, \dots ” instead of $\{a_n\}$, to ensure that the set of indices is clear.
 - Be careful: Our book often leaves the indices ambiguous.
- An example of an infinite series:
 - Consider the series $\{a_n\} = a_1, a_2, \dots$, where $(\forall n \geq 1) a_n = f(n) = 1/n$.
 - Then, we have $\{a_n\} = 1, 1/2, 1/3, \dots$

Example with Repetitions

- Like tuples, but unlike sets, a sequence may contain *repeated* instances of an element.
- Consider the sequence $\{b_n\} = b_0, b_1, \dots$ (note that 0 is an index) where $b_n = (-1)^n$.
 - Thus, $\{b_n\} = 1, -1, 1, -1, \dots$
 - Note repetitions!
 - This $\{b_n\}$ denotes an infinite sequence of 1's and -1 's, *not* the 2-element set $\{1, -1\}$.

Recognizing Sequences

- Sometimes, you're given the first few terms of a sequence,
 - and you are asked to find the sequence's generating function,
 - or a procedure to enumerate the sequence.
- Examples: What's the next number?
 - 1,2,3,4,... 5 (the 5th smallest number >0)
 - 1,3,5,7,9,... 11 (the 6th smallest odd number >0)
 - 2,3,5,7,11,... 13 (the 6th smallest prime number)

The Trouble with Sequence Recognition

- As you know, these problems are popular on IQ tests, but...
- The problem of finding “the” generating function given just an initial subsequence is *not a mathematically well defined problem*.
 - This is because there are *infinitely* many computable functions that will generate *any* given initial subsequence.
- We implicitly are supposed to find the *simplest* such function (because this one is assumed to be most likely), but,
 - how are we to objectively define the *simplicity* of a function?
- We might define simplicity as the reciprocal of complexity, but...
 - There are *many* different plausible, competing definitions of complexity, and this is an active research area.
- So, these questions really have *no* objective right answer!
 - Still, we will ask you to answer them anyway... (Because others will too.)

What are Strings, Really?

- This book says “finite sequences of the form a_1, a_2, \dots, a_n are called *strings*”,
 - but *infinite* strings are also discussed sometimes.
- Strings are normally restricted to sequences composed of *symbols* drawn from a finite *alphabet*, and are often indexed from 0 or 1.
 - But these are really arbitrary restrictions also.
- Either way, the *length* of a (finite) string is just its number of terms (or of distinct indices).

Strings, more formally

- Let Σ be a finite set of *symbols*, *i.e.* an *alphabet*.
 - A *string* s over alphabet Σ is any sequence $\{s_i\}$ of symbols, $s_i \in \Sigma$, normally indexed by \mathbf{N} or $\mathbf{N} - \{0\}$.
- If a, b, c, \dots are symbols, the string $s = a, b, c, \dots$ can also be written $abc\dots$ (*i.e.*, without commas).
- If s is a finite string and t is any string, then the *concatenation of s with t* , written just st ,
 - is simply the string consisting of the symbols in s , in sequence, followed by the symbols in t , in sequence.

More Common String Notations

- The length $|s|$ of a finite string s is its number of *positions* (i.e., its number of index values i).
- If s is a finite string and $n \in \mathbf{N}$,
 - Then s^n denotes the concatenation of n copies of s .
- ε or “” denotes the empty string, the string of length 0.
 - This is fairly common, but the book uses λ instead.
- If Σ is an alphabet and $n \in \mathbf{N}$,
 - $\Sigma^n := \{s \mid s \text{ is a string over } \Sigma \text{ of length } n\}$, and
 - $\Sigma^* := \{s \mid s \text{ is a finite string over } \Sigma\}$.

Summation Notation

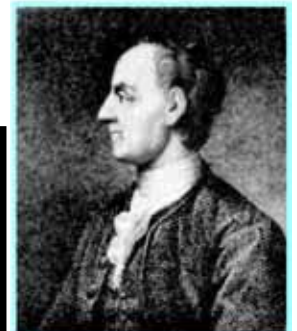
- Given a series $\{a_n\}$, an integer *lower bound* (or *limit*) $j \geq 0$, and an integer *upper bound* $k \geq j$, then the *summation of $\{a_n\}$ from j to k* is written and defined as follows:

$$\sum_{i=j}^k a_i \equiv a_j + a_{j+1} + \dots + a_k$$

- Here, i is called the *index of summation*.

Example: Impress Your Friends

- Boast, “I’m so smart; give me any 2-digit number n , and I’ll add all the numbers from 1 to n in my head in just a few seconds.”
- *I.e., Evaluate the summation:*
$$\sum_{i=1}^n i$$
- There is a simple closed-form formula for the result, discovered by Euler at age 12!
 - And frequently rediscovered by many...



Leonhard
Euler
(1707-1783)

Euler's Trick, Illustrated

- Consider the sum:

$$1 + 2 + \dots + (n/2) + ((n/2) + 1) + \dots + (n-1) + n$$

$n+1$
 \vdots
 $n+1$
 $n+1$

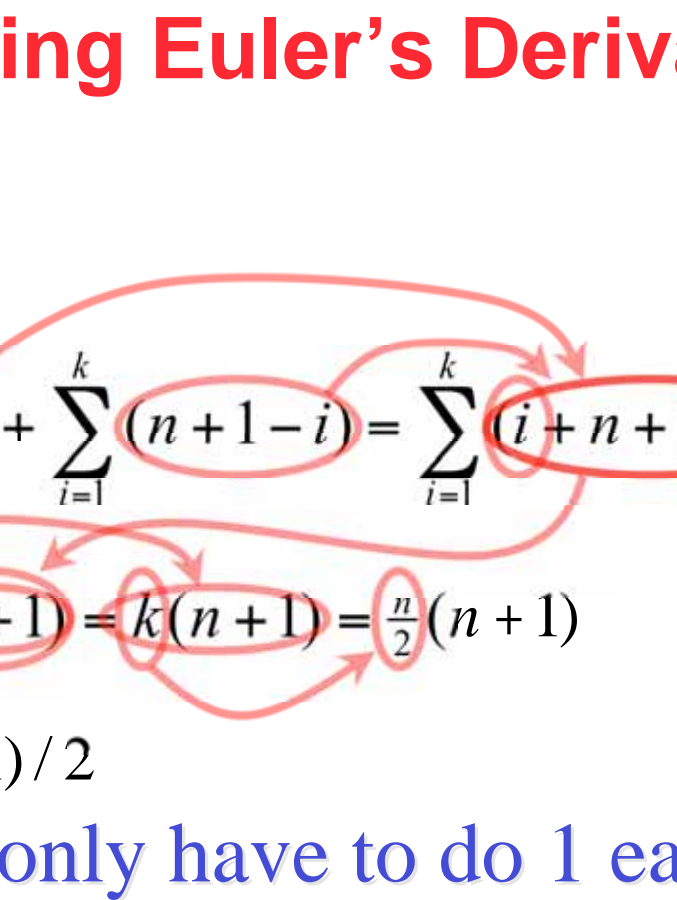
- We have $n/2$ pairs of elements, each pair summing to $n+1$, for a total of $(n/2)(n+1)$.

Symbolic Derivation of Trick

For case where n is even...

$$\begin{aligned}
 \sum_{i=1}^n i &= \sum_{i=1}^{2k} i = \left(\sum_{i=1}^k i \right) + \sum_{i=k+1}^n i = \left(\sum_{i=1}^k i \right) + \sum_{i=0}^{n-(k+1)} (i + (k+1)) \\
 &= \left(\sum_{i=1}^k i \right) + \sum_{i=0}^{n-(k+1)} ((n-(k+1)) - i) + (k+1) \\
 &= \left(\sum_{i=1}^k i \right) + \sum_{i=0}^{n-(k+1)} (n-i) = \left(\sum_{i=1}^k i \right) + \sum_{i=1}^{n-k} (n-(i-1)) \\
 &= \left(\sum_{i=1}^k i \right) + \sum_{i=1}^{n-k} (n+1-i) = \left(\sum_{i=1}^k i \right) + \sum_{i=1}^k (n+1-i) = \dots
 \end{aligned}$$

Concluding Euler's Derivation

$$\begin{aligned}\sum_{i=1}^n i &= \left(\sum_{i=1}^k i \right) + \sum_{i=1}^k (n+1-i) = \sum_{i=1}^k (i+n+1-i) \\ &= \sum_{i=1}^k (n+1) = k(n+1) = \frac{n}{2}(n+1) \\ &= n(n+1)/2\end{aligned}$$


- So, you only have to do 1 easy multiplication in your head, then cut in half.
- Also works for odd n (prove this at home).

Example: Geometric Progression

- A *geometric progression* is a series of the form $a, ar, ar^2, ar^3, \dots, ar^k$, where $a, r \in \mathbf{R}$.
- The sum of such a series is given by:

$$S = \sum_{i=0}^k ar^i$$

- We can reduce this to *closed form* via clever manipulation of summations...

Geometric Sum Derivation

- Here we go...

$$\begin{aligned}
 S &= \sum_{i=0}^n ar^i \\
 rS &= r \sum_{i=0}^n ar^i = \sum_{i=0}^n rar^i = \sum_{i=0}^n arr^i = \sum_{i=0}^n ar^1 r^i \\
 &= \sum_{i=0}^n ar^{1+i} = \sum_{i=1}^{n+1} ar^{1+(i-1)} = \sum_{i=1}^{n+1} ar^i \\
 &= \left(\sum_{i=1}^n ar^i \right) + \sum_{i=n+1}^{n+1} ar^i = \left(\sum_{i=1}^n ar^i \right) + ar^{n+1} = \dots
 \end{aligned}$$

Derivation example cont...

$$\begin{aligned} rS &= \left(\sum_{i=1}^n ar^i \right) + ar^{n+1} = (ar^0 - ar^0) + \left(\sum_{i=1}^n ar^i \right) + ar^{n+1} \\ &= ar^0 + \left(\sum_{i=1}^n ar^i \right) + ar^{n+1} - ar^0 \\ &= \left(\sum_{i=0}^0 ar^i \right) + \left(\sum_{i=1}^n ar^i \right) + ar^{n+1} - a \\ &= \left(\sum_{i=0}^n ar^i \right) + a(r^{n+1} - 1) = S + a(r^{n+1} - 1) \end{aligned}$$

Concluding long derivation...

$$rS = S + a(r^{n+1} - 1)$$

$$rS - S = a(r^{n+1} - 1)$$

$$S(r - 1) = a(r^{n+1} - 1)$$

$$S = a \left(\frac{r^{n+1} - 1}{r - 1} \right) \quad \text{when } r \neq 1$$

$$\text{When } r = 1, S = \sum_{i=0}^n ar^i = \sum_{i=0}^n a1^i = \sum_{i=0}^n a \cdot 1 = (n + 1)a$$

Nested Summations

- These have the meaning you'd expect.

$$\begin{aligned}\sum_{i=1}^4 \sum_{j=1}^3 ij &= \sum_{i=1}^4 \left(\sum_{j=1}^3 ij \right) = \sum_{i=1}^4 i \left(\sum_{j=1}^3 j \right) = \sum_{i=1}^4 i(1 + 2 + 3) \\ &= \sum_{i=1}^4 6i = 6 \sum_{i=1}^4 i = 6(1 + 2 + 3 + 4) \\ &= 6 \cdot 10 = 60\end{aligned}$$

- Note issues of free vs. bound variables, just like in quantified expressions, integrals, etc.

Some Shortcut Expressions

$$\sum_{k=0}^n ar^k = a(r^{n+1} - 1) / (r - 1), r \neq 1$$
 Geometric series.

$$\sum_{k=1}^n k = n(n + 1) / 2$$
 Euler's trick.

$$\sum_{k=1}^n k^2 = n(n + 1)(2n + 1) / 6$$
 Quadratic series.

$$\sum_{k=1}^n k^3 = n^2(n + 1)^2 / 4$$
 Cubic series.

Using the Shortcuts

- Example: Evaluate $\sum_{k=50}^{100} k^2$.
 - Use series splitting.
 - Solve for desired summation.
 - Apply quadratic series rule.
 - Evaluate.
- $$\sum_{k=1}^{100} k^2 = \left(\sum_{k=1}^{49} k^2 \right) + \sum_{k=50}^{100} k^2$$
- $$\sum_{k=50}^{100} k^2 = \left(\sum_{k=1}^{100} k^2 \right) - \sum_{k=1}^{49} k^2$$
- $$= \frac{100 \cdot 101 \cdot 201}{6} - \frac{49 \cdot 50 \cdot 99}{6}$$
- $$= 338,350 - 40,425$$
- $$= 297,925.$$