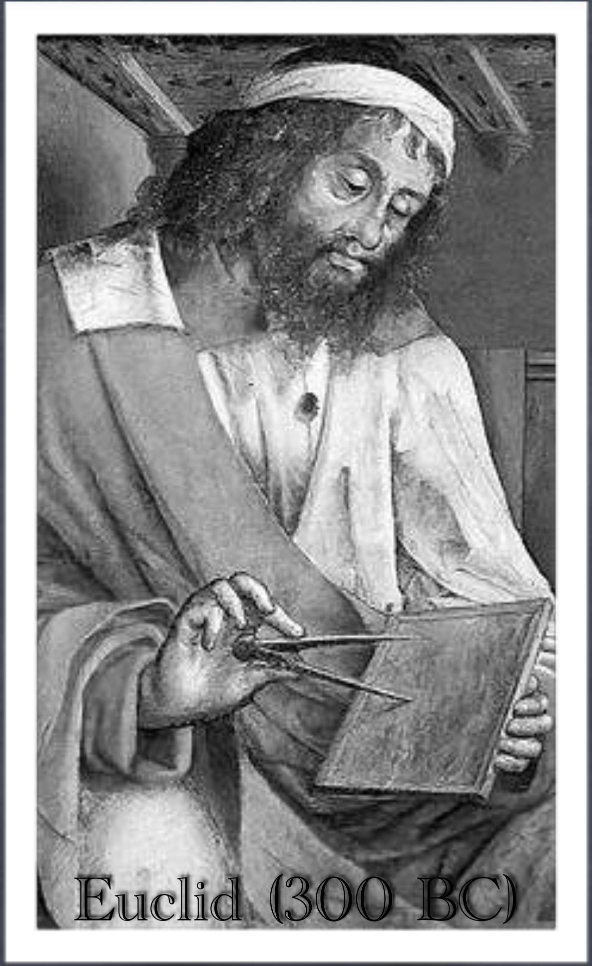


Proofs, Continued

Today

- Proofs : A style guide
  - Proofs should be easy to verify. All the cleverness goes into finding/writing the proof, not reading/verifying it!

P *vs.* **NP**" *(informally) :*
P = *class of problems for which <u>finding</u> a proof is computationally easy.*
NP = *class of problems for which <u>verifying</u> a proof is computationally easy.*
We believe that many problems in **NP** *are not in* **P**
(but we haven't been able to prove it yet!)

  - Multiple approaches: Direct deduction; Rewriting the proposition, e.g., as contrapositive; Proof by contradiction; Proof by giving a (counter)example, when applicable.
  - Today: Proof by case analysis; Mathematical induction

Cases

- Often it is helpful to break a proposition into various "cases" and prove them one by one
- e.g., To prove $p \rightarrow q$
  - $p \rightarrow p_1 \vee p_2 \vee p_3$
  - $p_1 \rightarrow q$
  - $p_2 \rightarrow q$
  - $p_3 \rightarrow q$
  - Hence $p \rightarrow q$

$$(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge (p_3 \rightarrow q) \equiv (p_1 \vee p_2 \vee p_3) \rightarrow q$$

$$((p \rightarrow r) \wedge (r \rightarrow q)) \rightarrow (p \rightarrow q)$$

Cases: Example

- Proving equivalences of logical formulas
- To prove: $p \lor (q \land r) \equiv (p \lor q) \land (p \lor r)$
  - $\forall p,q,r \in \{T,F\} \quad (p \lor (q \land r)) \longleftrightarrow ((p \lor q) \land (p \lor r))$
- Two cases: $p \lor \neg p$
- Case p: $p \lor (q \land r) \equiv T$

  $(p \lor q) \land (p \lor r) \equiv T$
- Case ¬p: $p \lor (q \land r) \equiv (q \land r)$

  $(p \lor q) \land (p \lor r) \equiv (q \land r)$

Cases: Example

- $\forall a,b,c,d \in \mathbb{Z}^+$ If $a^2+b^2+c^2 = d^2$, then d is even iff a,b,c are all even.
- Suppose $a,b,c,d \in \mathbb{Z}^+$ s.t. $a^2+b^2+c^2 = d^2$. Will show d is even iff a,b,c are all even.
- 4 cases based on number of a,b,c which are even.
- Case 1: a,b,c all even $\Rightarrow d^2 = a^2+b^2+c^2$ even $\Rightarrow$ d even.
- Case 2: Of a,b,c, 2 even, 1 odd. Without loss of generality, let a be odd and b, c even. i.e., $a=2x+1$, $b=2y$, $c=2z$ for some x,y,z. Then, $d^2 = a^2+b^2+c^2 = 2(2x^2+2x+2y^2+2z^2) + 1 \Rightarrow d^2$ odd $\Rightarrow$ d odd.
- Case 3: Of a,b,c, 1 even, 2 odd. W.l.o.g, $a=2x+1, b=2y+1, c=2z$. Then, $d^2=a^2+b^2+c^2 = 4(x^2+x+y^2+y+4z^2) + 2$. Contradiction! (why?)
- Case 4: a,b,c all odd $\Rightarrow d^2 = a^2+b^2+c^2 = 4w+3 \Rightarrow$ d odd.

Mathematical Induction

Proof by Programming

The Fable of the Proof Deity!

(OK, I made it up :))

- You have been imprisoned in a dungeon. The guard gives you a predicate P and tells you that the next day you will be asked to produce the proof for P(n) for some $n \in \mathbb{Z}^+$. If you can, you'll be let free!
- You pray to Seshat, the deity of wisdom.
- You tell her what P is. She thinks for a bit and says, indeed, $\forall n \in \mathbb{Z}^+ \; P(n)$. But she wouldn't give you a proof.
- You plead with her. She relents a bit and tells you. If you give me the proof for P(k) for any k, and give me a gold coin, I will give you the proof for P(k+1).
- You are hopeful, because you have worked out the proof for P(1) (and you're very rich) ...

The Fable of the Proof Deity!

(OK, I made it up :))

- After getting out of the dungeon, you have an envelope with the proof of P(207) with you. You open it.
  - The first page is the proof of P(1) you gave.
  - The second page has the proof for a Lemma: $\forall k \in \mathbb{Z}^+ \;\; P(k) \longrightarrow P(k+1)$.
  - The third page has:
    Since P(1) and, by Lemma, $P(1) \longrightarrow P(2)$, we have P(2).
    Since P(2) and, by Lemma, $P(2) \longrightarrow P(3)$, we have P(3).
    $\vdots$
    Since P(206) and, by Lemma, $P(206) \longrightarrow P(207)$, we have P(207).
    QED
- You feel a bit silly for having paid 206 gold coins. But at least, you learned something...

Programming a Proof

- Let $f(n) = \Sigma_{(i=1 \text{ to } n)}\ i^2$ and $g(n) = n(n+1)(2n+1)/6$
- $\forall n \in \mathbb{Z}^+,\ \ f(n) = g(n)$
    - $f(1) = 1,\quad g(1) = 1$ ✔
    - $f(2) = 5,\quad g(2) = 5$ ✔
    - $f(3) = 14,\quad g(3) = 14$ ✔
    - But we need to check this for all n...
- To the rescue: mathematical induction
    - No need to explicitly write down such a proof. Enough to prove that an explicit proof exists!
        - Describe a procedure that can generate the proof for each n

Proof by Induction

- To prove $\forall n \in \mathbb{Z}^+ \; P(n)$:
- First, we prove $P(1)$ and $\forall k \in \mathbb{Z}^+ \; P(k) \rightarrow P(k+1)$

An axiom in our system for $\mathbb{Z}^+$

Weak

The Principle of Mathematical Induction

For any n, we can run this procedure to generate a proof for P(n), and hence for any n, P(n) holds.

$P(1)$	$P(1) \rightarrow P(2)$
$P(2)$	$P(2) \rightarrow P(3)$
$P(3)$	$P(3) \rightarrow P(4)$
$P(4)$	$P(4) \rightarrow P(5)$
$P(5)$	$P(5) \rightarrow P(6)$
$\vdots$	$\vdots$

$\forall n \in \mathbb{Z}^+ \; P(n)$

Proof by Induction

- To prove $\forall n \in \mathbb{Z}^+ \; P(n)$:
  - First, we prove $P(1)$ and $\forall k \in \mathbb{Z}^+ \; P(k) \rightarrow P(k+1)$

    Base case

    Induction step

    Induction hypothesis
  - Then by (weak) mathematical induction, $\forall n \in \mathbb{Z}^+ \; P(n)$

$p|q$: p divides q
i.e., $\exists r$ s.t. $q=pr$

Example

- $\forall n \in \mathbb{N}$, $3 \mid n^3 - n$
  - Base case: $n=0$. $3|0$.
  - Induction step: For all integers $k \geq 0$
    Induction hypothesis: Suppose true for $n=k$. i.e., $k^3-k = 3m$
    To prove: Then, true for $n=k+1$. i.e., $3 \mid (k+1)^3-(k+1)$
    - $$\begin{aligned}(k+1)^3 - (k+1) &= k^3 + 3k^2 + 3k + 1 - k - 1 \\ &= (k^3 - k) + 3k^2+3k \\ &= 3m + 3k^2 + 3k \quad ✔\end{aligned}$$
- The non-inductive proof: $n^3-n = n(n^2-1) = (n-1)n(n+1)$.
  $3|n(n+1)(n+2)$ since one of n, $(n+1)$, $(n+2)$ is $\equiv 0 \pmod 3$

Proof by Induction

- To prove $\forall n \in \mathbb{Z}^+ \ P(n)$:
  - First, we prove $P(1)$ and $\forall k \in \mathbb{Z}^+ \ P(k) \rightarrow P(k+1)$
  - Then by (weak) mathematical induction, $\forall n \in \mathbb{Z}^+ \ P(n)$

In disguise

Well Ordering Principle

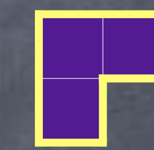
Every non-empty subset of $\mathbb{Z}^+$ has a minimum element.

(Can be used instead of Principle of Mathematical Induction)

- To prove $\forall n \in \mathbb{Z}^+ \ P(n)$:
  - Prove $P(1)$ and $\forall k \in \mathbb{Z}^+ \ \neg P(k+1) \rightarrow \neg P(k)$
  - For the sake of contradiction, suppose $\neg (\forall n \in \mathbb{Z}^+ \ P(n))$.
  - Let k' be the smallest $n \in \mathbb{Z}^+$ s.t. $\neg P(n)$. $k' \neq 1$ (since $P(1)$).
  - Let $k = k'-1$. Then, $k \in \mathbb{Z}^+$ and $\neg P(k+1)$. Then, $\neg P(k)$.
  - Contradicts the fact that k' is the smallest $n \in \mathbb{Z}^+$ s.t. $\neg P(n)$.

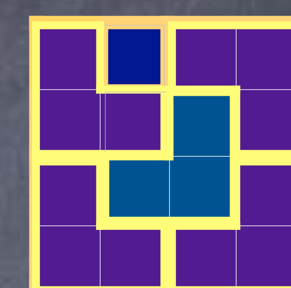
Tromino Tiling

- L-trominoes can be used to tile a "punctured" $2^n \times 2^n$ grid (punctured = one cell removed), for all positive integers n

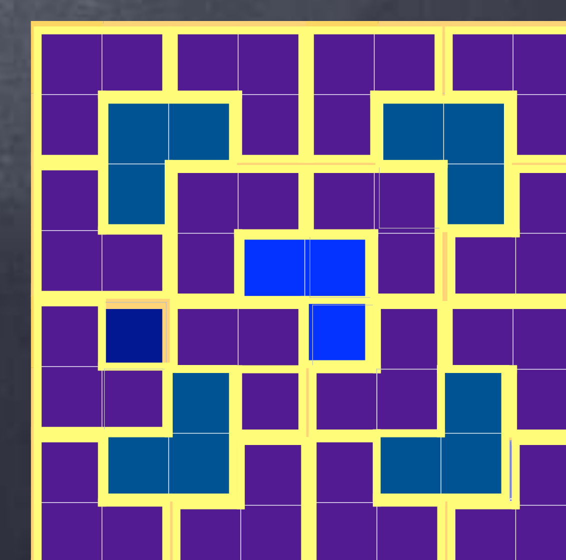


- Base case: n=1

- Inductive step: For all integers $k \geq 1$:
  Hypothesis: suppose, true for n=k
  To prove: then, true for n=k+1



  - Idea: can partition the $2^{k+1} \times 2^{k+1}$ punctured grid into four $2^k \times 2^k$ punctured grids, plus a tromino. Each of these can be tiled using trominoes (by inductive hypothesis).



- Actually gives a (recursive) algorithm for tiling

Structured Problems

- P(n) may refer to an object or structure of "size" n (e.g., a punctured grid of size $2^n \times 2^n$)
- To prove $P(k) \rightarrow P(k+1)$
  - Take the object of size k+1
  - Derive (one or more) objects of size k
  - Appeal to the induction hypothesis P(k), to draw conclusions about the smaller objects
  - Put them back together into the original object, and draw a conclusion about the original object, namely, P(k+1)

Common mistake:
Going in the opposite direction!
Not enough to reason about (k+1)-sized objects derived from k-sized objects

Strong Induction

Induction hypothesis: $\forall n \leq k\ P(n)$

- To prove $\forall n \in \mathbb{Z}^+\ \ P(n)$: we prove $P(1)$ (as before) and that

$$\forall k \in \mathbb{Z}^+\ \ (P(1) \land P(2) \land \ldots \land P(k)) \rightarrow P(k+1)$$

$P(1)$	$P(1) \rightarrow P(2)$
$P(2)$	$P(1) \land P(2) \rightarrow P(3)$
$P(3)$	$P(1) \land .. \land P(3) \rightarrow P(4)$
$P(4)$	$P(1) \land .. \land P(4) \rightarrow P(5)$
$P(5)$	$P(1) \land .. \land P(5) \rightarrow P(6)$
:	:

Mathematical Induction

The fact that for any n, we can run this procedure to generate a proof for P(n), and hence for any n, P(n) holds.

$\forall n \in \mathbb{Z}^+\ \ P(n)$

Same as weak induction for $\forall n\ Q(n)$, where $Q(n) \triangleq \forall m \in [1,n]\ \ P(m)$

Prime Factorization

- Every positive integer $n \geq 2$ has a prime factorization i.e, $n = p_1 \cdot \ldots \cdot p_t$ (for some $t \geq 1$) where all p_i are prime

Need some more work to show unique factorization.

$\underline{p \text{ prime} \wedge p|ab}$

$\rightarrow \underline{p|a \vee p|b}$

- Base case: $n=2$. ($t=1$, $p_1=2$).
- Induction step:

  (Strong) induction hypothesis: for all $n \leq k$, $\exists p_1,\ldots,p_t$, s.t. $n= p_1 \cdot \ldots \cdot p_t$

  To prove: $\exists q_1,\ldots,q_u$ (also primes) s.t. $k+1= q_1 \cdot \ldots \cdot q_u$

  - Case $k+1$ is prime: then $k+1=q_1$ for prime q_1
  - Case $k+1$ is not prime: $\exists a \in \mathbb{Z}^+$ s.t. $2 \leq a \leq k$ and $a|k+1$ (def. prime).
  - i.e., $\exists a,b \in \mathbb{Z}^+$ s.t. $2 \leq a,b \leq k$ and $k+1=a.b$ (def. divides; $a \geq 2 \rightarrow a.b > b$)
  - Now, by (strong) induction hypothesis, both a & b have prime factorizations: $a=p_1 \ldots p_s$, $b=r_1 \ldots r_t$.
  - Then $k+1=q_1 \ldots q_u$, where $u=s+t$, $q_i = p_i$ for $i=1$ to s and $q_i = r_{i-s}$, for $i=s+1$ to $s+t$.

Postage Stamps

- Claim: Every amount of postage that is at least ₹12 can be made from ₹4 and ₹5 stamps
  - i.e., $\forall n \in \mathbb{Z}^+ \quad n \geq 12 \rightarrow \exists a,b \in \mathbb{N} \quad n=4a+5b$
- Base cases: n=1,..,11 (vacuously true) and $n = 12 = 4\cdot3 + 5\cdot0$, $n = 13 = 4\cdot2 + 5\cdot1$, $n = 14 = 4\cdot1 + 5\cdot2$, $n = 15 = 4\cdot0 + 5\cdot3$.
- Induction step: For all integers $k \geq 16$:
  Strong induction hypothesis: Claim holds for all n s.t. $1 \leq n < k$
  To prove: Holds for n=k
  - $k \geq 16 \rightarrow k-4 \geq 12$.
  - So by induction hypothesis, $k-4=4a+5b$ for some $a,b \in \mathbb{N}$.
  - So $k = 4(a+1) + 5b$.

Be careful about ranges!

- Claim: Every non-empty set of integers has either all elements even or all elements odd. (Of course, false!)

- "Proof" (bogus): By induction on the size of the set.

- Base case: $|S|=1$. The only element in S is either even or odd, as claimed.

- Induction step: For all $k > 1$,

  Bug: Induction hypothesis cannot be bootstrapped from the base case

  Induction hypothesis: suppose all non-empty S with $|S| = k$, has either all elements even or all elements odd.
  To prove: then, it holds for all S with $|S|=k+1$.

  - Let $S = \{a,b\} \cup S'$, where $|S'|=k-1$.

  - $S' \cup \{a\}$ has all even or all odd. Say, all even. (The other case is analogous.) Then S' is all even, and $S' \cup \{b\}$ is also all even. Thus $S = S' \cup \{a,b\}$ is all even. QED.

Nim

- Alice and Bob take turns removing matchsticks from two piles
- Initially both piles have equal number of matchsticks
- At every turn, a player must choose one pile and remove <u>one or more</u> matchsticks from that pile
- Goal: be the person to remove the last matchstick

- Claim: In Nim, the second player has a <u>winning strategy</u>

  - (Aside: in <u>every</u> finitely-terminating two player game without draws, one of the players has a winning strategy)

- Claim: The following is a winning strategy for the second player: keep the piles matched at the end of your turn

Nim

- Claim: The following is a winning strategy for the second player: keep the piles matched at the end of your turn
- Rephrased: with this strategy for Bob (2nd player), at the end of each turn, either he has already won, or will win from there
- Induction variable: n = number of matchsticks on each pile at the beginning of the turn.
- Base case: n=1. Alice must remove one. Then Bob wins. ✔
- Induction step: for all integers $k \geq 1$

  Induction hypothesis: when starting with $n \leq k$, Bob always wins

  strong

  To prove: when starting with $n=k+1$, Bob always wins

  - Case 1: Alice removes all $k+1$ from one pile. Then Bob wins.
  - Case 2: Alice removes j, $1 \leq j \leq k$ from one pile. After Bob's move $k+1-j$ left in each pile. By induction hypothesis, Bob will always win from here.