Overview: Proof techniques

Direct proof

You go in logical steps from the assumption to the conclusion.

Counter-examples

To disprove a "for all" statement, you provide a single instance for which the property is not true.

Proof by contradiction

You assume that the negation is true, and come to a contradiction.

Contrapositive proof

Instead of p->q, you prove (not q)->(not p)

Biconditional proof

To prove a p<->q statement, you need to prove p->q AND q->p

TODAY: Proof by induction

Book: Chapter 1, section 1.6

Q: Can you calculate the sum 1+2+3+....+(n-1)+n (with n a natural number)?

- sum = 0

  for (i=1, i++ , i=n)

  (sum = sum+i)

- $\sum_{i=1}^{n} i = 1 + 2 + \dots + n$

  $= \frac{n}{2}(n+1)$

Mathematical induction

- proof technique for statements of the form $(\forall n \geq N, n \in \mathbb{Z}) P(n)$

Two steps:

1. Base case: proof of P(N)

(the statement holds for the first number, the first domino falls)

2. Induction step: proof of (for all n≥N) (P(n)->P(n+1))

(If the n-th domino falls, so does the (n+1)-th)

- $P(N)$ is true : Base case
- $p(n) \to p(n+1)$ $\forall n$ (induction step)

$p(N), \; p(N) \to p(N+1) \implies p(N+1)$

$p(2) \to p(3)$

$p(3) \to p(4)$

$\vdots$

$$(\forall n \in \mathbb{N}) \left(\sum_{k=1}^{n} k = \frac{n(n+1)}{2} \right)$$

- Base case. Proof of $P(1)$ ✓ statement is true for n=1

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

- Induction step. Proof of $\forall m \geq 1,\ P(m) \to P(m+1)$

$$P(m) : \sum_{k=1}^{m} k = \frac{m(m+1)}{2} \quad \text{(assumption)}$$

$$P(m+1) : \sum_{k=1}^{m+1} k = \frac{(m+1)(m+2)}{2} \quad \text{(to prove)}$$

$$\sum_{k=1}^{m+1} k = \underbrace{(1+2+\ldots+m)}_{\sum_{k=1}^{m} k} + m+1 = \frac{m(m+1)}{2} + (m+1)$$

$$= (m+1)\left(\frac{m}{2}+1\right)$$

$$= (m+1)\frac{(m+2)}{2} \quad \blacksquare$$

$\forall n \in \mathbb{N} : 4^n - 1$ is divisible by 3

Proof by induction

- Base case : P(1) is true. $4^1 - 1 = 3$ 3 is divisible by 3 ✓
- Induction step $P(x) \to P(x+1)$ $\forall x \in \mathbb{N}$

  $P(x)$: $4^x - 1$ is divisible by 3 (induction hypothesis)

  $P(x+1)$: $4^{x+1} - 1$ is divisible by 3

$$4^{x+1} - 1 = 4 \cdot 4^x - 1 = 3 \cdot 4^x + \underbrace{4^x - 1}_{3k \text{ (assumption)}}$$

$$= 3(4^x + k) \longrightarrow \text{multiple of } 3$$ ✓

$$4 \cdot 4^x = (3+1) \cdot 4^x = 3 \cdot 4^x + 4^x$$

A country has two types of coins: 3 cent and 7 cent. Prove that you can make all sums of money starting from 12 cent (up to 1 cent accuracy) from these coins.

$12 = 3 + 3 + 3 + 3$

$13 = 3 + 3 + 7$

$14 = 7 + 7$

$15 = 3 + 3 + 3 + 3 + 3$

$16 = 3 + 3 + 3 + 7$

$17 = 7 + 7 + 3$

$18 = 6 \cdot 3$

$19 = 4 \cdot 3 + 7$

⋮

$3+3 \to 7$

$2 \cdot 7 \to 5 \cdot 3$

1) if we have 2x3 (at least), we can go 1c up

2) if we have 2x7, (at least), we can go 1c up

3) we always have 2x7 or 2x3

(negation: max 1x7, max 1x3, cannot add up to 12 or more

Proof by induction.

- Base case. P(12) holds. ✓

  $12 = 3+3+3+3$

- Induction step: $P(q) \to P(q+1)$

  1) q has 2 coins of 7 (r) or 2 coins of 3 atleast (s)

     ↳ $\neg(r \vee s) = \neg r \wedge \neg s$ is impossible, as $q \geq 12$

  2) if r is true, then we can replace 2×7 by 5×3
  3) if s is true, then we can replace 2×3 by 7

  ↳ in both cases, we can make $q+1$

$$\forall x \in \mathbb{N}, \exists y \in \mathbb{N} : x^y < y^x$$

negation.
$\exists x \, \forall y : x^y \geq y^x$

→ this statement is false, so we proove the negation.

→ how to start ?

try $x = 1$. Then $1^2 < 2^1$ → does not work.
$x = 2$. $2^3 < 3^2$ → does not work.
$x = 3$ ... $2^3 < 3^2$, $3^3 \leq 3^3$, $4^3 < 3^4$, $5^3 < 3^5$

↳ this might work!

→ so, we try to prove : $\forall y \in \mathbb{N} : y^3 \leq 3^y$

→ we already know : $1^3 \leq 3^1$ (ok for $y=1$)
$2^3 \leq 3^2$ (ok for $y=2$)
$3^3 \leq 3^3$ (ok for $y=3$)

↳ we use induction for $y \geq 3$

- Base case : $y = 3$. $3^3 \leq 3^3$ is true ✓
- Induction step : $P(y) \to P(y+1) \quad \forall y \geq 3$

$P(y)$: $y^3 \leq 3^y$ —— induction hypothesis

$P(y+1)$: $(y+1)^3 \leq 3^{y+1}$

(LHS: $(y+1)^3$; RHS: 3^{y+1})

strategy : we go from LHS to RHS using the induction hypothesis.

$$
\begin{aligned}
(y+1)^3 &= y^3 + 3y^2 + 3y + 1 \\
&\leq 3^y + 3y^2 + 3y + 1 && \text{(induction hypothesis)} \\
&\leq 3^y + y^3 + 3y + 1 && \text{(since } y \geq 3,\ y^3 \geq 3y^2\text{)} \\
&\leq 3^y + 3^y + 3y + 1 && \text{(induction hyp.)} \\
&\leq 3^y + 3^y + y^3 && (y^3 \geq 3y+1 \iff y^3 - 3y \geq 1 \iff y(y^2-3) \geq 1 \text{ since } y \geq 3) \\
&\leq 3^y + 3^y + 3^y \\
&\leq 3 \cdot 3^y \\
&\leq 3^{y+1}
\end{aligned}
$$

$\blacksquare$

End of chapter 1:
Logic and proofs.

We already completed 1/3 of the course.
Tomorrow: set theory