date: 2025-11-19

1 proof by induction

consider a recursive function to compute the factorial of a non-negative integer n.

```
function factorial(n) {
  if (n == 0) return 1
  return n * factorial(n - 1)
}
```

how can we be certain that this function is correct for *every* non-negative integer? this is where induction comes in.

1.1 steps

for example, we want to prove $\forall x \in \mathbb{N}\, P(x)$ by induction. there are steps in general:

1. prove $P(0)$.
2. show that $P(k) \to P(k+1)$ for any *arbitrary* k.
   - intuition: if $P(0)$ is true, then $P(1)$ is true, therefore $P(2)$ is true...
3. conclude that $P(x)$ is true $\forall x \in \mathbb{N}$.

we can use dominoes as an analogy: we first prove the first domino falls ($P(0)$); then, we prove that that any dominoes following it will fall ($P(k) \to P(k+1)$); and finally we conclude that all the dominoes will fall ($\forall x P(x)$).

1.2 structure

proving by induction usually have a similar structure.

$P(x) \equiv$ define the property that we are trying to solve
base case: prove the first domino will fall; usually it means proving $P(0)$ or $P(1)$.
inductive hypothesis: assume that $P(k)$ is true for an arbitrary k.
inductive step: show that $P(k) \to P(k+1)$. that is, prove that once the first domino falls, prove that the following will fall too. proofs will differ from one another in this step.
conclusion: conclude that all dominoes have fallen and the claim is true.

1.3 examples

in this section we provide examples for proving different topics.

1.3.1 summation

we want to prove that the sum $1 + 2 + 2^2 + ... + 2^n = 2^{n+1} - 1$ for all non-negative integers n.

$P(n) \equiv \sum_{i=0}^{n} 2^i = 2^{n+1} - 1$

base case: $P(0) : 2^0 = 1$ ✓

inductive hypothesis: assume that $P(k)$ holds for an arbitrary natural number k.

inductive step: we will now show that $P(k) \to P(k+1)$.

$$
\begin{aligned}
1 + 2 + ... + 2^k &= 2^{k+1} - 1 && \text{(by I.H)} \\
1 + 2 + ... + 2^k + 2^{k+1} &= 2^{k+1} - 1 + 2^{k+1} && \text{(add both sides)} \\
1 + 2 + ... + 2^k + 2^{k+1} &= 2^{k+1} + 2^{k+1} - 1 && \text{(associativity)} \\
1 + 2 + ... + 2^k + 2^{k+1} &= 2^1 \times 2^{k+1} - 1 && \text{(by definition)} \\
1 + 2 + ... + 2^k + 2^{k+1} &= 2^{k+2} - 1 && \text{(exponential definition)}
\end{aligned}
$$

conclusion: since we have proved the base case and the induction case, $\forall n \in \mathbb{N}\, P(n)$ by mathematical induction.

1.3.2 inequalities

we want to prove that $2^n < n!$ for every positive integer $n \geq 4$.

$P(n) \equiv 2^n < n!$

base case: $P(4) : 2^4 < 4!$ ✓

inductive hypothesis: assume that $P(k)$ holds for an arbitrary integer $k \geq 4$

inductive step: we will now show that $P(k) \to P(k+1)$.

$$
\begin{aligned}
2^k &< k! && \text{(by inductive hypothesis)} \\
2^1 \times 2^k &< 2 \times k! && \text{(multiply by 2)} \\
2^{k+1} &< 2 \times k! && \text{(definition of exp)} \\
2^{k+1} &< (k+1) \times k! && \text{(substitution since 2 < k + 1)} \\
2^{k+1} &< (k+1)! && \text{(definition of factorial)}
\end{aligned}
$$

conclusion: since we have proved the base case and the inductive case, $\forall n \geq 4(P(n))$ by induction.

1.3.3 divisibility

we want to prove that $n^3 - n$ is divisible by 3 whenever n is a positive integer.

$P(n) \equiv 3 \mid (n^3 - n)$
base case: $P(1) : 3 \mid 0$ ✓
inductive hypothesis: assume that $P(k)$ holds for an arbitrary positive integer k.
inductive step: we will now show that $P(k) \to P(k+1)$. $$\begin{aligned}(k+1)^3 - (k+1) &= k^3 + 3k^2 + 3k + 1 - (k+1) \\ &= k^3 + 3k^2 + 2k \\ &= (k^3 - k) + (3k^2 + 3k) \\ &= (k^3 - k) + 3(k^2 + k)\end{aligned}$$ we know that $3 \mid (k^3 - k)$ by inductive hypothesis, and $3 \mid 3(k^2 + k)$ by definition.
conclusion: since we have proved the base case and inductive case, $\forall n \in \mathbb{Z}^+(P(n))$ by induction.