Mathematical Induction

Mingxun Zhou (mingxunz@ust.hk)

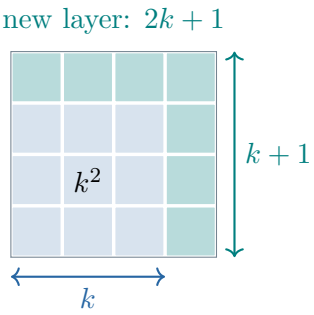
COMP2711 Discrete Mathematical Tools

Learning objectives

- Write an induction proof with a precise claim, base case, hypothesis, and target.
- Choose a hypothesis that covers the smaller objects used in the proof.
- Use strong induction and well-ordering to prove claims about integers.

1 Ordinary induction

The identity $1 + 3 + \cdots + (2n - 1) = n^2$ describes every positive integer n. Its recursive structure is visible: adding the next odd number extends a square by one layer.



MUST UNDERSTAND Mathematical induction

Theorem (Mathematical induction)**.** Let b be an integer. To prove $P(n)$ for every integer $n \geq b$, prove:

1. **Base case:** $P(b)$.
2. **Inductive step:** for every integer $k \geq b$, $P(k) \Rightarrow P(k + 1)$.

While proving the implication, assume $P(k)$ for an arbitrary $k \geq b$; this is the *inductive hypothesis*. The target is $P(k + 1)$. The assumption is local to the implication, so it does not assume the whole theorem.

1.1 Example: the odd-number sum

For all $n \geq 1$, prove

$$P(n): \quad \sum_{i=1}^{n}(2i-1) = n^2.$$

Base: at $n = 1$, both sides equal 1.

Step: fix $k \geq 1$ and assume $\sum_{i=1}^{k}(2i-1) = k^2$. The target is $\sum_{i=1}^{k+1}(2i-1) = (k+1)^2$. Then

$$\sum_{i=1}^{k+1}(2i-1) = \underbrace{\sum_{i=1}^{k}(2i-1)}_{k^2 \text{ by the hypothesis}} + (2k+1) = k^2 + 2k + 1 = (k+1)^2.$$

Induction proves the identity for every $n \geq 1$.

1.2 Example: choosing the starting value

Prove $2^n < n!$ for every integer $n \geq 4$. It is false at $n = 1, 2, 3$, so the starting value belongs in the statement.

Base: $2^4 = 16 < 24 = 4!$. For $k \geq 4$, assume $2^k < k!$. Then

$$2^{k+1} = 2 \times 2^k < 2k! < (k+1)k! = (k+1)!,$$

where the first inequality uses the hypothesis and the second uses $2 < k + 1$. Thus the result holds for all $n \geq 4$.

1.3 Example: divisibility

Prove $3 \mid (n^3 - n)$ for $n \geq 1$. The base is $1^3 - 1 = 0$. Assuming $3 \mid (k^3 - k)$,

$$(k+1)^3 - (k+1) = (k^3 - k) + 3k(k+1)$$

is divisible by 3. This proves the next case and hence the claim.

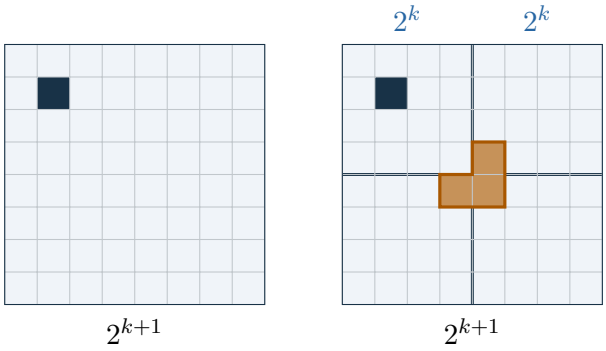
2 Choosing the induction hypothesis

The hypothesis must cover the smaller instances that appear in the step. For objects such as sets or boards, the claim usually quantifies over *every* object of the given size.

2.1 Example: a board with one missing square

Theorem. For every integer $k \geq 1$, every $2^k \times 2^k$ board with one square removed can be tiled by L-shaped trominoes (three connected squares forming an L).

The missing square may be anywhere. Rotations of a tromino are allowed.



Base: when $k = 1$, the remaining three squares of a 2×2 board form one tromino.

Step: assume the theorem for every deficient $2^k \times 2^k$ board. Divide a deficient $2^{k+1} \times 2^{k+1}$ board into four quadrants. One quadrant contains the missing square. Place one tromino at the center, covering one square in each of the other three quadrants. Each quadrant now has exactly one square unavailable: the original hole or a square covered by the central tromino. Apply the hypothesis to the four remaining regions. Their tilings and the central tromino tile the original board.

A hypothesis restricted to a corner hole would not suffice: the smaller boards may have holes in other positions. This is why the theorem allows *any* missing square.

2.2 Example: counting subsets

Every n-element set has 2^n subsets. For $n = 0$, the only subset is the empty set. Assume the statement for every k-element set. Given a set T of size $k + 1$, remove one element a to obtain S. Subsets of T split into two disjoint groups:

$$\{X : X \subseteq S\}, \qquad \{X \cup \{a\} : X \subseteq S\}.$$

Each group has 2^k members, so there are 2^{k+1} subsets of T.

2.3 Checking the first transition

Consider the false claim that every collection of $n \geq 2$ distinct, pairwise nonparallel lines passes through one common point. The base $n = 2$ is true. A proposed step applies the hypothesis to the first k and last k lines, obtaining common points p and q. It then argues that the two overlapping lines force $p = q$.

There are $k - 1$ shared lines, so that argument needs $k \geq 3$. At $k = 2$ there is only one shared line, which can contain distinct points p and q. The proof never establishes the transition from two lines to three. Three sides of a triangle give a counterexample.

3 Strong induction

MUST UNDERSTAND Strong induction

Theorem (Strong induction)**.** To prove $P(n)$ for every integer $n \geq b$, prove $P(b)$ and, for every $k \geq b$, prove

$$\big(P(b) \wedge P(b+1) \wedge \cdots \wedge P(k)\big) \Rightarrow P(k+1).$$

We may use any earlier cases in the specified range. Several initial cases can be checked separately when the recursive step needs them.

3.1 Example: two-pile Nim

There are two piles of $a, b \geq 0$ stones. Players alternate removing any positive number of stones from one pile. Whoever takes the last stone wins; a player with no legal move loses.

The strategy is to *match your opponent's move*: leave equal piles for your opponent, then copy each removal in the other pile. For example, from $(5, 3)$ take two stones to leave $(3, 3)$.

Claim. (n, n) is losing for the first player, for every $n \geq 1$.

Proof by strong induction. The base is $(1, 1)$: the first player takes one stone, and the second takes the last.

Assume the claim holds for every $k = 1, \ldots, n$. Now consider $(n+1, n+1)$.

1. If the first player empties a pile, the second empties the other pile and wins.
2. If the first player takes $1 \leq m \leq n$ stones, the second matches the move. This leaves

$$(n+1-m, n+1-m), \qquad 1 \leq n+1-m \leq n.$$

   It is the first player's turn again. By the induction hypothesis, this is a losing position for that player. Thus the second player wins.

Matching without emptying a pile cannot continue forever: each round reduces the positive pile size. At $(1, 1)$, a pile must be emptied.

Thus equal piles are losing for the player to move. Unequal piles are winning: reduce the larger pile to match the smaller, then use the matching strategy. If one pile is already empty, simply take the other pile.

3.2 Example: sums of distinct Fibonacci numbers

Use the increasing Fibonacci sequence $F_1 = 1$, $F_2 = 2$, and $F_{k+1} = F_k + F_{k-1}$ for $k \geq 2$:

$$1, 2, 3, 5, 8, 13, 21, 34, 55, 89, \ldots.$$

Every positive integer can be expressed as a sum of distinct Fibonacci numbers.

Choose the largest Fibonacci number that fits, subtract it, and repeat. For 100, the successive remainders are 11, 3, and 0, giving

$$100 = 89 + 8 + 3.$$

Proof. Use strong induction on n. The cases $1 = F_1$ and $2 = F_2$ hold. For $n \geq 3$, assume every positive integer less than n has the required representation. Choose the largest $F_k \leq n$, so $k \geq 3$. Then

$$F_k \leq n < F_{k+1} = F_k + F_{k-1}, \qquad 0 \leq r := n - F_k < F_{k-1} < F_k.$$

If $r = 0$, the single term F_k is a representation. Otherwise $1 \leq r < n$, so the hypothesis supplies a representation of r with distinct Fibonacci numbers. Each summand is at most $r < F_k$, so adding F_k introduces no repeated term. This proves the claim. The same argument justifies the greedy procedure recursively.

Practice. Apply the procedure to 50 and 72. The answers are $50 = 34{+}13{+}3$ and $72 = 55{+}13{+}3{+}1$.

3.3 Example: several base cases

Every integer $n \geq 12$ can be written as $4a + 5b$ for nonnegative integers a, b.

$$12 = 4 + 4 + 4, \quad 13 = 4 + 4 + 5, \quad 14 = 4 + 5 + 5, \quad 15 = 5 + 5 + 5.$$

For a target $n \geq 16$, assume the claim for all integers from 12 to $n - 1$. Then $12 \leq n - 4 < n$, so write $n - 4 = 4a + 5b$ by the hypothesis. Adding 4 gives $n = 4(a + 1) + 5b$. The four bases start the four possible remainder classes modulo 4.

3.4 Why the two induction principles are equivalent

Strong induction allows the hypothesis of ordinary induction. Conversely, define

$$Q(k) = P(b) \wedge P(b + 1) \wedge \cdots \wedge P(k).$$

The base $P(b)$ establishes $Q(b)$. A strong-induction step proves $P(k + 1)$ from $Q(k)$, and hence proves $Q(k + 1)$. Ordinary induction on Q gives every $P(n)$.

4 Well-ordering principle

MUST UNDERSTAND Well-ordering

Theorem (Well-ordering principle)**.** Every **nonempty** subset of $\mathbb{N} = \{0, 1, 2, \ldots\}$ has a least element.

A common use is to prove that a set $S \subseteq \mathbb{N}$ is empty:

1. Assume $S \neq \varnothing$ and choose its smallest element x.
2. Construct another element $x' \in S$ with $x' < x$.

This contradicts the choice of x. Therefore S must be empty. In particular, S can be the set of counterexamples to a claim; proving S empty proves the claim.

4.1 Example: an equation with no positive solutions

There are no positive integers x, y, z satisfying

$$x^2 + y^2 = 3z^2.$$

Proof. Assume the solution set $\mathcal{S}$ is nonempty. The set of third coordinates

$$\{z \in \mathbb{N} : (x, y, z) \in \mathcal{S} \text{ for some } x, y\}$$

is nonempty, so well-ordering gives a solution (x, y, z) with smallest z. We will construct another solution with a smaller third coordinate.

Dividing the equation by 9 gives

$$\left(\frac{x}{3}\right)^2 + \left(\frac{y}{3}\right)^2 = 3\left(\frac{z}{3}\right)^2.$$

We just need to show that $x/3$, $y/3$, and $z/3$ are integers.

Step 1: $3 \mid x$ and $3 \mid y$. Taking remainders modulo 3 on both sides gives $x^2 + y^2 \equiv 0 \pmod 3$. Check all pairs of remainders:

Remainder of $x^2 + y^2$ modulo 3

$x \backslash y$	0	1	2
0	**0**	1	1
1	1	2	2
2	1	2	2

Only $x \equiv y \equiv 0 \pmod 3$ works. Thus $3 \mid x$ and $3 \mid y$.

Step 2: $3 \mid z$. By Step 1, $9 \mid x^2$ and $9 \mid y^2$. Hence

$$3 \mid \frac{x^2 + y^2}{3} = z^2.$$

A square is 0 modulo 3 only when its base is 0 modulo 3, so $3 \mid z$.

Thus $(x/3, y/3, z/3)$ is a positive integer solution with $z/3 < z$, contradicting our choice of smallest z. Therefore the solution set is empty.

5 Practice

1. Prove $\sum_{i=0}^{n} r^i = (r^{n+1} - 1)/(r - 1)$ for every integer $n \geq 0$ and every fixed real $r \neq 1$.
2. Prove $7 \mid (8^n - 1)$ for every integer $n \geq 1$.
3. A proof checks $P(4)$ and shows $P(k) \Rightarrow P(k + 2)$ for all $k \geq 4$. Which cases follow? What additional base is sufficient for every $n \geq 4$?
4. For the board theorem, let t_k be the number of trominoes used. Give a recurrence and a formula for t_k.
5. Two players remove any positive number of matches from one of two piles. The last move wins. Prove that the second player can win when both piles initially have the same positive size.
6. Prove that every integer $n \geq 2$ has a prime divisor using a least counterexample.

Answers

1. Base $n = 0$: both sides equal 1. For the step, add r^{k+1} to the hypothesis:

$$\frac{r^{k+1} - 1}{r - 1} + r^{k+1} = \frac{r^{k+2} - 1}{r - 1}.$$

   This proves the identity by induction. If $r = 1$, the sum is $n + 1$ instead.

2. Base: $8 - 1 = 7$. If $8^k - 1 = 7q$, then $8^{k+1} - 1 = 8(8^k - 1) + 7 = 7(8q + 1)$.

3. Only even $n \geq 4$ follow. Add $P(5)$ to start the odd chain.

4. $t_1 = 1$ and $t_{k+1} = 4t_k + 1$. Also $t_k = (4^k - 1)/3$, since there are $4^k - 1$ uncovered cells and each tile covers three. The recurrence verifies the formula: $4(4^k - 1)/3 + 1 = (4^{k+1} - 1)/3$.

5. Induct strongly on the common pile size n. For $n = 1$, the second player takes the remaining match. For general n, mirror the first player's removal of r matches. If $r = n$, the second player wins immediately. Otherwise the piles both have size $n - r$, between 1 and $n - 1$, and it is again the first player's turn. Apply the hypothesis.

6. Let $m \geq 2$ be the least integer with no prime divisor. It is composite, so $m = ab$ with $2 \leq a, b < m$. By minimality, a has a prime divisor p. Then $p \mid m$, a contradiction.

Rosen, Sections 5.1–5.2 [1], provides further examples, including generalized De Morgan laws, greedy scheduling, the odd pie-fight problem, and polygon triangulation.

References

[1] Kenneth H. Rosen. *Discrete Mathematics and Its Applications.* McGraw-Hill Education, eighth edition, 2019.