Induction

Lectures 11–12 (Chapter 19)

What is a proof?

A proof of a statement is a complete and convincing argument that the statement is true.

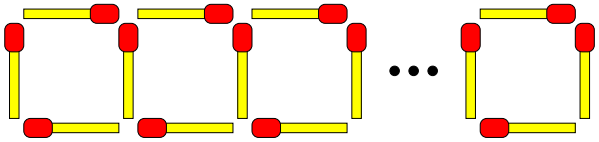
A proof is a means of communication.

The desired form of the proof and the required amount of detail will depend on who you should convince.

A clear exposition of the logical reasoning involved is (also) an important part of the argument.

Read handout “What is (in) a proof?”, available from the website.

Matches



Question

How many matches do we need to make a sequence of $n \geq 1$ squares?

Conjecture

For all $n \geq 1$: with $3n + 1$ matches we can make a sequence of n squares.

How can we prove this conjecture?

Proving a universal statement

General strategy for proving universal quantification $\forall_x[P(x) : Q(x)]$:

Declare an arbitrary element x satisfying the predicate P and establish that it also satisfies the predicate Q.

Assume:
(k) **var** $x; P(x)$
⋮
$(\ell - 1)$ $Q(x)$
{∀-intro on (k) and $(\ell - 1)$:}
(ℓ) $\forall_x[P(x) : Q(x)]$

If the domain of quantification has structure, we can sometimes use a more sophisticated technique to prove a universal quantification.

Natural numbers have structure

On the natural numbers we can define the notion of successor, a mapping $s : \mathbb{N} \to \mathbb{N}$ that is defined, for all $n \in \mathbb{N}$, by

$$s(n) = n + 1 \ .$$

The *successor mapping* s imposes a structure on the set $\mathbb{N}$ that enables us to count:

1. there is a starting number 0; and
2. there is, for every number n, a next number $s(n) = n + 1$.

In fact, the set $\mathbb{N}$ can be defined as the least set of numbers such that $0 \in \mathbb{N}$ and if $n \in \mathbb{N}$, then also $s(n) \in \mathbb{N}$.

Induction (formalised)

Let P be a unary predicate on $\mathbb{N}$

Induction:

$\vdots$

(k) $P(0)$ ← Basis

var i; $i \in \mathbb{N}$

$P(i)$ ← Induction hypothesis

$\vdots$

$P(i+1)$

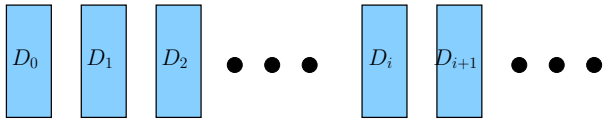
(l) $\forall_i[i \in \mathbb{N} : P(i) \Rightarrow P(i+1)]$ ← Step

{ Induction on (k) and (l): }

(m) $\forall_n[n \in \mathbb{N} : P(n)]$

Induction

Imagine an infinite sequence of dominoes:



If we know that

1. D_0 *falls*, and
2. the dominoes are close enough together to make sure that

   if D_i *falls, then also* D_{i+1} *falls (for all* $i \in \mathbb{N}$*),*

then we can conclude that every D_n $(n \geq 0)$ falls!

INDUCTION

Induction (correctness?)

Let P be a (unary) predicate on $\mathbb{N}$. Suppose:

1. $P(0)$ is true
2. $\underbrace{P(i) \Rightarrow P(i+1) \text{ is true } \textit{for all } i \in \mathbb{N}}_{\forall_i[i \in \mathbb{N} : P(i) \Rightarrow P(i+1)]}$ ← "PASS-ON-PROPERTY"

Then also:

2' $P(0) \Rightarrow P(1)$ ($\forall$-elim with 0), and hence ($\Rightarrow$-elim with $P(0)$): $P(1)$

2" $P(1) \Rightarrow P(2)$ ($\forall$-elim with 1), and hence ($\Rightarrow$-elim with $P(1)$): $P(2)$

2"' $\ldots$

There is a general method, independent of P, to establish $P(n)$ for every n from assumptions 1 and 2. This motivates (but does not prove!) the conclusion $\forall_n[n \in \mathbb{N} : P(n)]$.

Example

Prove by induction:

$$\forall_n[n \in \mathbb{N} : \sum_{k=0}^{n} k = \frac{1}{2}n(n+1)] \ .$$

Define the unary predicate P on $\mathbb{N}$ by

$$P(n) := [\sum_{k=0}^{n} k = \frac{1}{2}n(n+1)] \ .$$

Then we should prove that $\forall_n[n \in \mathbb{N} : P(n)]$. [Proof on next slide]

Example: $\forall_n[n \in \mathbb{N} : \sum_{k=0}^{n} k = \frac{1}{2}n(n+1)]$

$\sum_{k=0}^{0} k = 0 = \frac{1}{2} \cdot 0 \cdot (0+1)$

(1) $P(0)$ (Definition of P on previous slide)

(IH) **var** i; $i \in \mathbb{N}$

(IH) $P(i)$

$\sum_{k=0}^{i} k = \frac{1}{2}i(i+1)$ (Definition on P on previous slide)

$\sum_{k=0}^{i+1} k = \sum_{k=0}^{i} k + (i+1) \overset{\text{(IH)}}{=} \frac{1}{2}i(i+1) + (i+1)$

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

$\sum_{k=0}^{i+1} k = \frac{1}{2}(i+1)(i+2)$

$P(i+1)$ (Definition P on previous slide)

$P(i) \Rightarrow P(i+1)$

(2) $\forall_i[i \in \mathbb{N} : P(i) \Rightarrow P(i+1)]$

$\forall_n[n \in \mathbb{N} : P(n)]$ (Induction on (1) and (2))

Induction with different starting point (1)

Imagine again an infinite sequence of dominoes:

If we know that

1. D_{-3} *falls*, and
2. the dominoes are close enough together to make sure that:
   if D_i *falls, then* D_{i+1} *will fall too* (for all $i \in \mathbb{Z}$ with $i \geq -3$),

then we can conclude that every D_n $(n \geq -3)$ falls!

Induction with starting point other than 0

Let P be a unary predicate on $\mathbb{Z}$

Induction from $a \in \mathbb{Z}$:

$\vdots$

(k) $P(a)$

$\vdots$

(l) $\forall_i[i \in \mathbb{Z} \wedge i \geq a : P(i) \Rightarrow P(i+1)]$

{ Induction on (k) and (l): }

(m) $\forall_x[x \in \mathbb{Z} \wedge x \geq a : P(x)]$

Inductive definitions

Inductive proof: "*truth* is passed on"

Inductive definition: "*construction* is passed on"

Example:

Consider the sequence of numbers $a_0, a_1, a_2, \ldots$ defined by

$$\begin{array}{lcll} a_0 & := & 2 & \\ a_{i+1} & := & 2a_i - 1 & (\text{for all } i \in \mathbb{N}) \ . \end{array}$$

Then:

a_0	a_1	a_2	a_3	a_4	a_5	$\rightarrow$
2	3	5	9	17	33	$\rightarrow$

Conjecture: $\forall_n[n \in \mathbb{N} : a_n = 2^n + 1]$.[Proof on the next slide.]

Example

Define $a_0, a_1, a_2, \ldots$ by

$$\begin{array}{lcll} a_0 & := & 2 & \\ a_{i+1} & := & 2a_i - 1 & (i \in \mathbb{N}) \ . \end{array}$$

Define the unary predicate P on $\mathbb{N}$ by

$$P(n) := [a_n = 2^n + 1] \ .$$

We prove:

$$\forall_n[n \in \mathbb{N} : P(n)]$$

$a_0 = 2 = 2^0 + 1$

(1) $P(0)$ (Def. P)

var $i;\ i \in \mathbb{N}$

$P(i)$ (IH)

$a_i = 2^i + 1$

$$\begin{array}{lcll} a_{i+1} & = & 2a_i - 1 & \\ & \overset{\text{(IH)}}{=} & 2(2^i + 1) - 1 & \\ & = & 2^{i+1} + 2 - 1 & \\ & = & 2^{i+1} + 1 & \end{array}$$

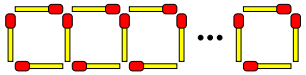
$P(i+1)$ (Def. $P(i+1)$)

$P(i) \Rightarrow P(i+1)$

(2) $\forall_i[i \in \mathbb{N} : P(i) \Rightarrow P(i+1)]$

$\forall_n[n \in \mathbb{N} : P(n)]$ (Ind. on (1) and (2))

Matches



Theorem

For all $n \geq 1$, we can make a sequence of n squares with $3n + 1$ matches.

Proof

Induction on n:

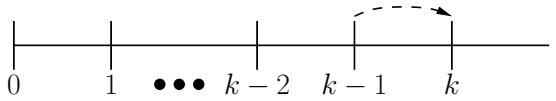
(BASIS) With $4 = 3 \cdot 1 + 1$ matches we can make a single square.

(STEP) Let $n \geq 1$, and suppose that we can make a sequence of n squares with $3n + 1$ matches (induction hypothesis). We use the right-most vertical match of the sequence as the left-most vertical match of the new square, and use 3 more matches to complete the new square. We have then used $(3n + 1) + 3 = 3(n + 1) + 1$ matches for $n + 1$ squares.

Strong induction

Induction: 'passing on *to successor*' $(\underline{i \rightarrow i{+}1})$

'receive *from predecessor*' $(\underline{k{-}1 \rightarrow k})$



When you arrive at $k{-}1$, you have already encountered 0 until $k{-}2$!

Wouldn't it be convenient if we could use the information obtained about the numbers 0 to $k{-}2$?

Super Pass-On Property

Suppose: $\forall_k[k \in \mathbb{N} : \forall_j[j \in \mathbb{N} \wedge j < k : P(j)] \Rightarrow P(k)]$

"If I know P for 0 until $k-1$, then also for k"

Then:

1. $\forall$-elim with $k := 0$: $P(0)$

$$
\begin{array}{ll}
 & \forall_j[j \in \mathbb{N} \wedge j < 0 : P(j)] \Rightarrow P(0) \\
\overset{val}{=\!=} & \{\ \text{Math: } j \in \mathbb{N} \wedge j < 0 \overset{val}{=\!=} \texttt{False}\ \} \\
 & \forall_j[\texttt{False} : P(j)] \Rightarrow P(0) \\
\overset{val}{=\!=} & \{\ \text{Empty Domain}\ \} \\
 & \texttt{True} \Rightarrow P(0) \\
\overset{val}{=\!=} & \{\ \text{Simple calculation: } \texttt{True} \Rightarrow P \overset{val}{=\!=} P\ \} \\
 & P(0)
\end{array}
$$

Strong induction (2)

Suppose: $\forall_k[k \in \mathbb{N} : \forall_j[j \in \mathbb{N} \wedge j < k : P(j)] \Rightarrow P(k)]$

"If we know P for 0 until $k-1$, then also for k"

Then:

1. $\forall$-elim with 0: $P(0)$
2. $\forall$-elim with 1: $P(0) \Rightarrow P(1)$, and hence ($\Rightarrow$-elim): $P(1)$

$$
\begin{array}{ll}
 & \forall_j[j \in \mathbb{N} \wedge j < 1 : P(j)] \Rightarrow P(1) \\
\overset{val}{=\!=} & \{\ \text{Math: } j \in \mathbb{N} \wedge j < 1 \overset{val}{=\!=} j = 0\ \} \\
 & \forall_j[j = 0 : P(j)] \Rightarrow P(1) \\
\overset{val}{=\!=} & \{\ \text{One-element}\ \} \\
 & P(0) \Rightarrow P(1)
\end{array}
$$

Strong induction (2)

Suppose: $\forall_k[k \in \mathbb{N} : \forall_j[j \in \mathbb{N} \wedge j < k : P(j)] \Rightarrow P(k)]$

"If we know P for 0 until $k-1$, then also for k"

Then:

1. $\forall$-elim with $k := 0$: $P(0)$
2. $\forall$-elim with $k := 1$: $P(0) \Rightarrow P(1)$, and hence ($\Rightarrow$-elim): $P(1)$
3. $\forall$-elim with $k := 2$: $P(0) \wedge P(1) \Rightarrow P(2)$, and hence ($\wedge$-intro + $\Rightarrow$-elim): $P(2)$

$$
\begin{array}{ll}
 & \forall_j[j \in \mathbb{N} \wedge j < 2 : P(j)] \Rightarrow P(2) \\
\overset{val}{=\!=} & \{\ \text{Math: } j \in \mathbb{N} \wedge j < 2 \overset{val}{=\!=} j = 0 \vee j = 1\ \} \\
 & \forall_j[j = 0 \vee j = 1 : P(j)] \Rightarrow P(2) \\
\overset{val}{=\!=} & \{\ \text{Domain Splitting + One-element } (2\times)\ \} \\
 & P(0) \wedge P(1) \Rightarrow P(2)
\end{array}
$$

Strong induction (2)

Suppose: $\forall_k[k \in \mathbb{N} : \forall_j[j \in \mathbb{N} \wedge j < k : P(j)] \Rightarrow P(k)]$

"If we know P for 0 until $k-1$, then also for k"

Then:

1. $\forall$-elim with 0: $P(0)$
2. $\forall$-elim with 1: $P(0) \Rightarrow P(1)$, and hence ($\Rightarrow$-elim): $P(1)$
3. $\forall$-elim with 2: $P(0) \wedge P(1) \Rightarrow P(2)$, and hence ($\wedge$-intro + $\Rightarrow$-elim): $P(2)$
4. ...

Strong induction (3)

Let P be a unary predicate on $\mathbb{N}$

Strong induction:

$\vdots$

(ℓ) $\quad \forall_k[k \in \mathbb{N} : \forall_j[j \in \mathbb{N} \wedge j < k : P(j)] \Rightarrow P(k)]$

{ Strong induction on (ℓ): }

(m) $\quad \forall_n[n \in \mathbb{N} : P(n)]$

NB: Follows from 'normal induction.'

What happened to the base case?

Example

Consider the sequence of numbers $a_0, a_1, a_2, \ldots$ defined by

$$\begin{array}{lcll} a_0 & := & 2 & \\ a_1 & := & 5 & \\ a_{i+2} & := & 3a_{i+1} - 2a_i & \text{(for all } i \in \mathbb{N}) \ . \end{array}$$

Then:

a_0	a_1	a_2	a_3	a_4	a_5	$\rightarrow$
2	5	11	23	47	95	$\rightarrow$

Prove that $\forall_n[n \in \mathbb{N} : a_n = 3 \cdot 2^n - 1]$.

Example

Define $a_0, a_1, a_2, \ldots$ by

$$\begin{array}{lcll} a_0 & := & 2 & \\ a_1 & := & 5 & \\ a_{i+2} & := & 3a_{i+1} - 2a_i & (i \in \mathbb{N}) \ . \end{array}$$

Define P on $\mathbb{N}$ by

$$P(n) := [a_n = 3 \cdot 2^n - 1] \ .$$

We prove that

$$\forall_n[n \in \mathbb{N} : P(n)]$$

var k; $k \in \mathbb{N}$

(IH) $\quad \forall_j[j \in \mathbb{N} \wedge j < k : P(j)]$

case $k = 0$: $a_0 = 2 = 3 \cdot 2^0 - 1$, so $P(0)$

case $k = 1$: $a_1 = 5 = 3 \cdot 2^1 - 1$, so $P(1)$

case $k \geq 2$:

$\forall$-elim with $k-1$: $P(k-1)$, so $a_{k-1} = 3 \cdot 2^{k-1} - 1$

$\forall$-elim with $k-2$: $P(k-2)$, so $a_{k-2} = 3 \cdot 2^{k-2} - 1$

Then:

$$\begin{array}{lcll} a_k & = & 3a_{k-1} - 2a_{k-2} & \\ & \overset{\text{(IH)}}{=} & 3(3 \cdot 2^{k-1} - 1) - 2(3 \cdot 2^{k-2} - 1) & \\ & = & 9 \cdot 2^{k-1} - 3 - 3 \cdot 2^{k-1} + 2 = 6 \cdot 2^{k-1} - 1 & \\ & = & 3 \cdot 2^k - 1, \text{ so } P(k) & \end{array}$$

{ Case distinction ($k = 0 \vee k = 1 \vee k \geq 2 \overset{val}{=\!=} k \in \mathbb{N}$!): }

$P(k)$

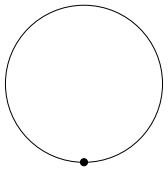
$\forall_j[j \in \mathbb{N} \wedge j < k : P(j)] \Rightarrow P(k)$

$\forall_k[k \in \mathbb{N} : \forall_j[j \in \mathbb{N} \wedge j < k : P(j)] \Rightarrow P(k)]$

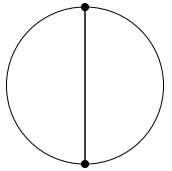
{ Strong induction: }

$\forall_n[n \in \mathbb{N} : P(n)]$

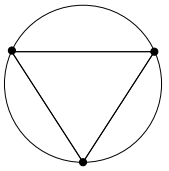
Cutting the cake (1)



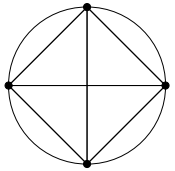
$1 = 2^{1-1}$ pieces



$2 = 2^{2-1}$ pieces



$4 = 2^{3-1}$ pieces

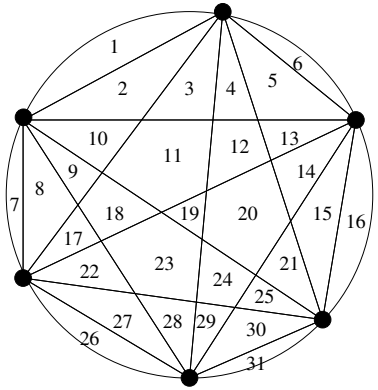


$8 = 2^{4-1}$ pieces

Conjecture

The number of pieces obtained by cutting the cake using n points on the edge of the cake is 2^{n-1}.

Cutting the cake (2)



The maximum number of portions we can get using 6 points on the edge of the cake is $31 \neq 32 = 2^{6-1}$.

Our conjecture fails for $n = 6$!

Example

Theorem:
Every postage greater than 7 cent can be formed with only 3-cent and 5-cent stamps.

Proof:
Define the unary predicate P on $\mathbb{N}$ by

$$P(p) := \exists_{k,\ell}[k, \ell \in \mathbb{N} : p = k \cdot 3 + \ell \cdot 5] \ .$$

To prove: $\forall_p[p \in \mathbb{N} \wedge p > 7 : P(p)]$.

[Proof on the next slide]

Example (cont.)

(1) **var** $p; p \in \mathbb{N} \wedge p > 7$

(2) $\forall_j[j \in \mathbb{N} \wedge 7 < j < p : P(j)]$

(3) Case $p = 8$: $p = 1 \cdot 3 + 1 \cdot 5$, so ($\exists^*$-intro) $P(p)$

(4) Case $p = 9$: $p = 3 \cdot 3 + 0 \cdot 5$, so ($\exists^*$-intro) $P(p)$

(5) Case $p = 10$: $p = 0 \cdot 3 + 2 \cdot 5$, so ($\exists^*$-intro) $P(p)$

(6) Case $p \geq 11$: $7 < p - 3 < p$, so ($\forall$-elim) $P(p-3)$.

(7) Pick k, ℓ with $k, \ell \in \mathbb{N}$ and $p - 3 = k \cdot 3 + \ell \cdot 5$
Then $p = (p-3) + 3 = (k \cdot 3 + \ell \cdot 5) + 3 = (k+1) \cdot 3 + \ell \cdot 5$
So ($\exists^*$-intro) $P(p)$

(8) { Case distinction: $p \in \mathbb{N} \wedge p > 7 \stackrel{val}{\Longrightarrow} p = 8 \vee p = 9 \vee p = 10 \vee p \geq 11$ }

(9) $P(p)$

(10) $\forall_j[j \in \mathbb{N} \wedge 7 < j < p : P(j)] \Rightarrow P(p)$

(11) $\forall_p[p \in \mathbb{N} \wedge p > 7 : \forall_j[j \in \mathbb{N} \wedge 7 < j < p : P(j)] \Rightarrow P(p)]$

(12) { Strong induction: }

(13) $\forall_p[p \in \mathbb{N} \wedge p > 7 : P(p)]$

Example (proof in textual form)

Proof:
We prove, with strong induction on p, that every postage p greater than 7 can be formed using only 3-cent and 5 cent stamps.
Let p be an arbitrary postage > 7.
Suppose: every postage p' with $7 < p' < p$ can be formed using 3-cent and 5-cent stamps (IH).
We now distinguish four cases:

- If $p = 8$, then p can be formed with one 3-cent stamp, and one 5-cent stamp.
- If $p = 9$, then p can be formed with three 3-cent stamps.
- If $p = 10$, then p can be formed with two 5-cent stamps.
- Suppose: $p \geq 11$. Then $7 < p - 3 < p$, so by (IH) $p - 3$ can be formed using k 3-cent stamps and ℓ 5-cent stamps ($k, \ell \in \mathbb{N}$).
  Hence, p can be formed with $k + 1$ 3-cent stamps and ℓ 5-cent stamps.

Thereby, the result is proved. □

Induction checklist

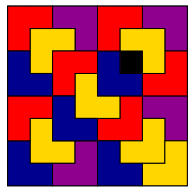
An inductive proof always includes the following ingredients:

1. one or more basis cases;
2. one or more step cases;
3. a clearly and explicitly stated induction hypothesis; and
4. one or more applications of the induction hypothesis.

Example: tromino puzzles

A tromino is a tile of the shape

An 8×8 board with an arbitrary 'unusable' field (coloured black) can be tiled with trominoes:



Example: tromino puzzles

Question: is it possible to tile every $n \times n$-board with a single 'unusable' field?

Answer: No! Obviously, tiling is, e.g., not possible if $n^2 - 1$ is not divisible by 3.

Theorem:

Every $2^n \times 2^n$ board with a single unusable field can be tiled with trominoes.

Proof:

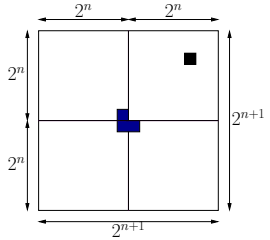
The proof is by induction on n.

- (BASIS) If $n = 0$, then the board entirely consists of the unusable field, and the rest of the board can be (trivially) tiled with zero trominoes.
- (STEP) [see next slide]

Example: tromino puzzles

Proof (cont.):

- (STEP) Suppose: every $2^n \times 2^n$ board with single unusable field can be tiled (induction hypothesis).



Consider arbitrary $2^{n+1} \times 2^{n+1}$ board with single unusable field.

It consists of four 'sub-boards' of $2^n \times 2^n$; unusable field is in one of the sub-boards.

Place tromino on inner corners of the other three sub-boards.

By the induction hypothesis, each of the four $2^n \times 2^n$ sub-boards can be tiled, and hence the $2^{n+1} \times 2^{n+1}$ board can be tiled. □