Chapter 4: Proof by contradiction

Def'n: A contradiction is a statement of the form (P and (not P))

Example: For integers a, the statement:
(a is even and a is odd)
is a contradiction (why?)

Example of a proof by contradiction:

Proposition: There are no integer m, n such that $6m + 8n = 75$

Remark: A direct proof here is a bad idea, because we'd have to check all integers.

Idea of proof: $6m$ is even

$8n$ is even

so $6m+8n$ is even

If $6m+8n=75$, then 75 would be even. But 75 is odd (why?). So if $6m+8n=75$ 75 would be both even & odd, which is a contradiction.

Let's now write the proof:

Proof: We will prove the proposition by contradiction. Suppose m & n are integers that satisfy

$$6m+8n=75.$$

Since 6 & 8 are even, $75 = 6m+8n$

$= 2(3m+4n)$

is also even.

But this is not true since 75 is odd.

Thus such integers m & n do not exist

Justification for proof by contradiction:

Suppose we want to prove that P is true. Instead, we show that

$(\text{not } P) \Rightarrow Q$ where Q is false.

Why is this enough to prove P?

P	$\neg P$	Q	$(\neg P) \Rightarrow Q$	
T	F	T	T	Case I
T	F	F	T	Case II
F	T	T	T	Case III
F	T	F	F	Case IV

We can exclude Case IV bec we showed $\neg P \Rightarrow Q$

We can exclude Case III & Case I bec we know Q is false

Only case II remains possible so P is True.

Proving Implications by contradiction

Example: Prove by contradiction, the proposition:

For integers a & b

$$(a+b \geq 11) \Rightarrow [(a \geq 6) \text{ or } (b \geq 6)]$$

Idea **Step 1:** Observe the $\neg(P \Rightarrow Q) \Leftrightarrow (P \wedge \neg Q)$

P	Q	$P \Rightarrow Q$	$\neg(P \Rightarrow Q)$	$P \wedge \neg Q$
T	T	T	F	F
T	F	F	T	T
F	T	T	F	F
F	F	T	F	F

Same

Step 2: Recall that to prove $(P \Rightarrow Q)$ by contradiction, we show that

$(\neg(P \Rightarrow Q)) \Rightarrow R$ where R is false

So, putting step 1 & 2 together, we want to show $(P \wedge (\neg Q)) \Rightarrow R$ where R is false.

Back to our example:

Proof:

Suppose by way of contradiction that $\underbrace{(a+b \geq 11)}_{P}$ and $\underbrace{(a \leq 5) \wedge (b \leq 5)}_{\neg Q}$.

However $(a \leq 5) \wedge (b \leq 5) \Rightarrow \underbrace{(a+b \leq 10)}_{R}$ (why?),

and we assumed $(a+b) \geq 11$, so we have a contradiction. So

$$(a+b \geq 11) \Rightarrow (a \geq 6) \text{ or } (b \geq 6)$$

Proof by contrapositive

The contrapositive of $(P \Rightarrow Q)$

is $(\neg Q \Rightarrow \neg P)$.

Notice that they are equivalent:

P	Q	$\neg P$	$\neg Q$	$P \Rightarrow Q$	$(\neg Q \Rightarrow \neg P)$
T	T	F	F	T	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	T	T	T

So to prove $(P \Rightarrow Q)$ we can instead prove $(\neg Q \Rightarrow \neg P)$.

Example: If a, b, c are integers with $a > b$, then

$$ac \leq bc \Rightarrow c \leq 0$$

Proof: We will prove the contrapositive of $ac \leq bc \Rightarrow c \leq 0$.

That is, we will prove $(c > 0 \Rightarrow ac > bc)$.

that for integers a, b, c with $a > b$

Indeed, the contrapositive is true by the multiplicative law of inequalities, so we are done.

Chapter 5: The induction principle

Goal: We may want to prove that some property holds for all positive integer (or all integers $\geq n_0$).

Observation: The positive integers come in a sequence. The integer $n+1$ is the successor of the integer n.

Axiom (The Induction Principle)

Let $P(n)$ be a statement involving a general positive integer n. Then $P(n)$ is true for all $n \geq 1$ if

(i) $P(1)$ is true, and

(ii) $P(k) \Rightarrow P(k+1)$ for all positive int. k.

So, to prove $P(n)$ by induction, we have to do two things

(1) Prove that $P(1)$ is true (base case)

(2) Prove that $P(k) \Rightarrow P(k+1)$ (inductive step)

Inductive hypothesis

Template for proof by induction

Example:

Proposition: For all positive integers n, we have $n \leq n^3$.

Proof: We will prove this by induction.

(i) So, we start by checking the base case ($k=1$) which is clearly true as $1 \leq 1^3$.

(ii) We now proceed to the inductive step, so we assume $k \leq k^3$ and prove that $(k+1) \leq (k+1)^3$.

To that end, note that

$$k \leq k^3 \Rightarrow k+1 \leq k^3+1$$

and

$$k^3+1 \leq k^3+3k^2+3k+1 = (k+1)^3.$$

Hence, $k \leq k^3 \Rightarrow (k+1) \leq (k+1)^3$.

So, by induction we have $n \leq n^3$ for all positive int n.

Exercise: By observing that $n \leq n^3 \Leftrightarrow n^3 - n \geq 0$

can you prove the proposition without induction

Exercise: Prove that for all positive integers n

$$n \leq 2^n .$$

Changing the base case

Suppose we want to prove that the statement $P(n)$ is true for all positive integers $n \geq n_0$.

To prove $P(n)$ by induction, we have to do two things:

(1) Prove that $P(n_0)$ is true (base case)

(2) Assume that for some $k \geq n_0$, $P(k)$ is true, prove $P(k) \Rightarrow P(k+1)$ (Inductive step)

→ Template for proof by induction

Example:

Proposition: For all integers $n \geq 4$, $n^2 \leq 2^n$.

Proof: We will proceed by induction.

(i) Base case ($n=4$): This is true because $16 = 4^2 \leq 2^4 = 16$.

(ii) Inductive step: Suppose that $k^2 \leq 2^k$.

We want to show that $(k+1)^2 \leq 2^{k+1}$.

By the inductive hypothesis, we have

$2k^2 \leq 2^{k+1}$. So, we will be done if we can show that $(k+1)^2 \leq 2k^2$... (why?)

However $(k+1)^2 \leq 2k^2 \Leftrightarrow 2k+1 \leq k^2$ and since $k \geq 4$, we have $k^2 \geq 4k = 2k + 2k \geq 2k+1$.

Hence $2k^2 \geq (k+1)^2$ and consequently $(k+1)^2 \leq 2^{k+1}$.

Thus, by induction $n^2 \leq 2^n$, for all $n \geq 4$.

Exercise: Prove that $n^2+n \leq 2^n$ for all integers $n \geq 5$.

Example: Prove that 3 divides n^3+2n whenever n is a positive integer

proof: We will proceed by induction

(i) Base case ($n=1$): Clearly 3 divides $1^3+2(1)$.

(ii) Inductive step: suppose 3 divides k^3+2k,

we would like to show that 3 divides $(k+1)^3+2(k+1)$.

Note that

$$(k+1)^3+2(k+1) = k^3+3k^2+3k+1+2k+2$$
$$= (k^3+2k)+3(k^2+k+1),$$

where $3 \mid (k^3+2k)$ by the inductive hyp. and $3 \mid 3(k^2+k+1)$. Hence $3 \mid \underbrace{(k^3+2k)+3(k^2+k+1)}_{=(k+1)^3+2(k+1)}$ as desired.

So we have that 3 divides n^3+2n. ▨

"Definition by induction" / recursion

Example: The sum of the first n positive integers

$1+2+\cdots+n$

define by induction

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

This is actually the same as the proposition

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

Exercise: prove this by induction.

Exercise: prove that for all positive integers n

$$\sum_{i=1}^{n} \frac{1}{i(i+1)} = \frac{n}{n+1}$$

5.4 Strong Induction

Axiom (The Strong Induction Principle)

Let $P(n)$ be a statement involving a general positive integer n. Then $P(n)$ is true for all $n \geq 1$ if

(i) $P(1)$ is true, and

(ii) [$P(n)$ holds for all positive int. $n \leq k$] $\Rightarrow P(k+1)$ for all positive int k.

So, to prove $P(n)$ by (strong) induction, we have to do two things

(1) Prove that $P(1)$ is true (base case)

(2) Suppose that (Inductive hypothesis)

[$P(n)$ holds for all positive int. $n \leq k$]

and deduce $P(k+1)$ is true (inductive step)

Template for proof by (strong) induction

Example (Fibonacci sequence)

Define the number u_n, for positive integers n as follows:

$$u_1 = 1$$
$$u_2 = 1$$
$$u_{k+1} = u_{k-1} + u_k \quad \text{for } k \geq 2$$

Proposition (Binet formula):

Define $\alpha = \frac{1+\sqrt{5}}{2}$, $\beta = \frac{1-\sqrt{5}}{2}$. Then

(this is the famous golden ratio)

$$u_n = \frac{\alpha^n - \beta^n}{\sqrt{5}}.$$

Proof: We proceed by strong induction.

(1) Base case ($n=1$): Note that $u_1 = 1$ by def'n, and $\frac{\alpha^1 - \beta^1}{\sqrt{5}} = \frac{1+\sqrt{5}-(1-\sqrt{5})}{2\sqrt{5}} = 1$

so $u_1 = \frac{\alpha^1 - \beta^1}{\sqrt{5}}$.

$(n=2)$: $u_2 = 1$, while $\dfrac{\alpha^2-\beta^2}{\sqrt{5}} = \dfrac{(\alpha-\beta)(\alpha+\beta)}{\sqrt{5}}$

$= \dfrac{1}{\sqrt{5}} = u_2$.

(2) Inductive step: Suppose the formula

$u_n = \dfrac{\alpha^n-\beta^n}{\sqrt{5}}$ is true for all $n \le k$

where $k \ge 2$. We have

$u_{k+1} = u_{k-1} + u_k$ (by def'n)

$= (\alpha^{k-1} - \beta^{k-1} + \alpha^k - \beta^k)/\sqrt{5}$

(by ind. hyp.)

$= [\alpha^{k-1}(1+\alpha) - \beta^k(1+\beta)]/\sqrt{5}$,

but $1+\alpha = \alpha^2$ & $1+\beta = \beta^2$ (check this).

So $u_{k+1} = [\alpha^{k-1}\cdot\alpha^2 - \beta^{k-1}\cdot\beta^2]/\sqrt{5} = \dfrac{\alpha^{k+1}-\beta^{k+1}}{\sqrt{5}}$

as required for our induction proof.

Hence $u^n = \dfrac{\alpha^n-\beta^n}{\sqrt{5}}$ for all positive int. n. ∎