S. KIMMEL

Proof by Contradiction

Use: any statement P

Proof has two parts

① (Direct) $\neg P \to Q$

② (Direct) $\neg P \to \neg Q$

$\therefore P$

Most common

Structure

For contradiction assume $\neg P$

Explain explain... Q

Explain explain... $\neg Q$, a contradiction.

Thus, P is true

When start, don't know what Q is... you need to keep your eye out for what might be the contradiction.

S.KIMMEL

Q: Prove $\sqrt{2}$ is irrational

* Not of form $P \to Q$

A: For contradiction, suppose $\sqrt{2}$ is rational. Then $\exists\, a, b \in \mathbb{Z} : \frac{a}{b} = \sqrt{2}$ where the fraction is fully simplifed, so $\neg \exists\, c \in \mathbb{Z} : c|a \wedge c|b \wedge c > 2$
Squaring both sides, we have

$$a^2 = 2b^2.$$

Thus $2|a^2$. But this implies $2|a$. This means $\exists\, m \in \mathbb{Z} : 2m = a$. Plugging in, we have

$$4a^2 = 2b^2.$$

Dividing by 2, we get

$$2a^2 = b^2.$$

But this means $2|b^2$, and so $2|b$. But this means $2|a$ and $2|b$, which contradicts the fact that $\frac{a}{b}$ is fully simplifed. $\square$

Q: Prove: $\neg \exists\, x, y \in \mathbb{Z} : x^2 = 4 \quad + 2$

S.KIMMEL

Prove: $\neg \exists x, y \in \mathbb{Z}: x^2 = 4y + 2$

For contradiction, assume $\exists x, y \in \mathbb{Z}: x^2 = 4y+2$. Then x^2 is even, so x is even. Thus $\exists m \in \mathbb{Z}: x = 2m$. Plugging in and solving for y, we get

$$y = \frac{4m^2 - 2}{4} = m^2 - \frac{1}{2}$$

Since $m \in \mathbb{Z}$, this means $y \notin \mathbb{Z}$, a contradiction.

Using Contradictions to prove $P \to R$

$$\neg(P \to R) \to Q$$

$$\underbrace{\neg(P \to R)}_{\text{need to take negation of entire statement}} \to \neg Q$$

But $\neg(P \to R)$ is awkward. Instead use:

$$\neg(P \to R) \equiv P \wedge \neg R$$

Structure of Proof of $P \to R$ by contradiction

Assume $P \wedge \neg R$ ... Therefore Q. ... Therefore $\neg Q$

S.KIMMEL

Proof by Example:

Q: Which could be proved using an example?

A) $\forall x \in S, P(x)$

B): $\forall x \in S, \neg P(x)$

C): $\neg \exists x \in S : P(x)$

D) $\neg \forall x \in S, P(x)$

Structure:

- Prove there exists...

  We give an example

- Prove not all ....

  We give a counterexample

ex: Prove: not all students in this class were born in the same month

S.KIMMEL

Proof by Example:

Q: Which could be proved using an example?

A) $\forall x \in S, P(x)$

B) $\forall x \in S, \neg P(x)$

de Morgan

C) $\neg \exists x \in S : P(x) \equiv \forall x \in S, \neg P(x)$

To show its true for all of S, a single example is not enough

$\boxed{\text{D)}}$ $\neg \forall x \in S, P(x) \equiv \exists x \in S : \neg P(x) \Leftarrow$ To show there exists, a single example is enough

Structure:

- Prove there exists...

  We give an example

- Prove not all ....

  We give a counterexample

WARNING: If try to use proof by example to do a "for all" proof, you will be VERY wrong.

S.KIMMEL

When proving correctness of algorithm and see

if..

else..

use proof by cases to show

- cover all situations
- behaves correctly in all situations

Recursion?

Loops?

Proof by induction