Proof Techniques

I) Direct Proof

Goal: $P \to Q$

Structure :

Assume P

$\vdots$

Q

Therefore, $P \to Q$

II) Proof by Contraposition

Goal: $P \to Q$

Structure:

- Assume $\neg Q$

$\vdots$

- $\neg P$

Therefore, $P \to Q$

III) Proof by Contradiction:

Goal: P

Structure :

Assume $\neg P$

$\vdots$

$\therefore C$ ← some Contradiction

it could be a proposition like $(r \wedge \neg r)$

Goal: $P \to q \equiv \neg p \vee q$

Structure:

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

Assume P

Assume $\neg q$

$\vdots$

$\therefore C$ ← some Contradiction

III) Proof by Contradiction

Defn: A real number x is rational if $x = \frac{p}{q}$ for some integers $p, q \neq 0$.

$\forall x \; rational(x) \leftrightarrow \exists p \exists q \left(q \neq 0 \wedge x = \frac{p}{q}\right)$

Defn: A real number x is irrational if it's not rational

$\forall x \; irrational(x) \leftrightarrow \neg rational(x)$

$\forall x \; irrational(x) \leftrightarrow \forall p \forall q \left(\underbrace{q = 0 \vee x \neq \frac{p}{q}}_{\equiv \; q \neq 0 \rightarrow x \neq \frac{p}{q}}\right)$

Fact (we don't prove this fact. You learned this in Elementary School.):

If x is rational, then $x = \frac{p}{q}$ for some integers $p, q \neq 0$ where p and q have no common factors.

(reason: can simplify/cancel common factors in a fraction)

Prop. C: $\sqrt{2}$ is irrational.

$$\text{irrational}(\sqrt{2}) \equiv \forall p \forall q \left(q \neq 0 \rightarrow \sqrt{2} \neq \frac{p}{q} \right)$$

irrational($\sqrt{2}$)

Proof: Assume $\sqrt{2}$ is rational.

Choose $p, q \neq 0$ s.t. $\sqrt{2} = \frac{p}{q}$, and p and q do not have any common factors.

Observe that $(\sqrt{2})^2 = \left(\frac{p}{q}\right)^2$. Hence, $2 = \frac{p^2}{q^2}$.

Therefore $p^2 = 2q^2$.

Hence, p^2 is even. By prop. A (in fact by its contraposition), p is even.

Choose k s.t. $p = 2k$.

Notice that $q^2 = \frac{p^2}{2} = \frac{4k^2}{2} = 2k^2$.

Hence, q^2 is even, and by prop. A,

q is even. This is a contradiction ※

More Proof Methods

Proof by exhustion:

Prop. D: Prove that $(n+1)^3 \geq 3^n$ if n is a positive integer with $n \leq 4$.

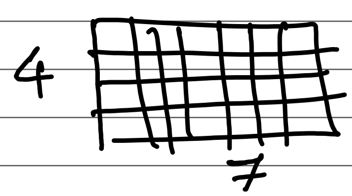
proof: We prove this by way of exhustion. We just need to verify the proposition for $n = 1, 2, 3, 4$.

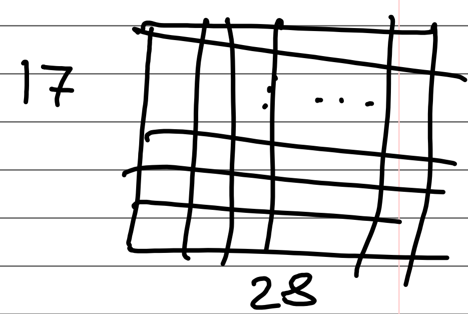
- $n=1$: $2^3 \geq 3^1$
- $n=2$: $3^3 \geq 3^2$
- $n=3$: $4^3 \geq 3^3$
- $n=4$: $5^3 \geq 3^4$. That concludes the proof.

---

prop.: Can you tile a 17×28 checkerboard using 4×7 tiles?

proof:





$17 = a \times 4 + b \times 7$

Any ordering of tiles that covers this checkerboard must cover the first column. Hence, there should exist a combination of vertical and horizontal 4×7 tiles that cover this column. Therefore, there should exist integers $0 \leq a \leq 5$ and $0 \leq b \leq 3$ s.t. $17 = a \times 4 + b \times 7$. However, this is impossible.

Proof by Cases:

A proof by cases must cover all possible cases that arise in a theorem.

Prop. E: Prove that $\max(x,y) = \frac{1}{2}(x+y+|x-y|)$ for all real numbers x and y.

Proof: We prove it case by case.

Case 1: Assume $x-y \leq 0$, or equivalenty $x \leq y$.
Observe that $\frac{1}{2}(x+y+|x-y|) = \frac{1}{2}(x+y-x+y)$
$= y$.

Moreover, notice that $\max(x,y) = y$ in this case.

Case 2: Assume $x-y > 0$, or equivalently $x > y$.
The proof in this case is similar to that of case 1.

$\square$

Existence Proofs:

A proof of a proposition of the form $\exists x P(x)$ is called existence proof.

+ A constructive existence proof works by constructing a "witness" a such that $P(a)$ is true.

+ A non constructive existence proof do not find an element a that $P(a)$ is true, but rather proves $\exists x P(x)$ in a different way (e.g., showing that the negation of $\exists x P(x)$ would esult in a contradiction)

Prop: prove that there exists a positive integer that can be written as sum of cubes of positive integers in two ways.

proof:

Consider 1729. It can be writen as 10^3+9^3 and 12^3+1^3. $\square$

was this existential proof constructive or non_constructive?

Prop.: prove that there exists irrational numbers x and y such that x^y is rational.

$\underbrace{(\sqrt{2})^{\sqrt{2}}}$ $\leftarrow$ if rational, we are done with the proof

if, $(\sqrt{2})^{\sqrt{2}}$ is irrational, then $\left((\sqrt{2})^{\sqrt{2}}\right)^{\sqrt{2}}$

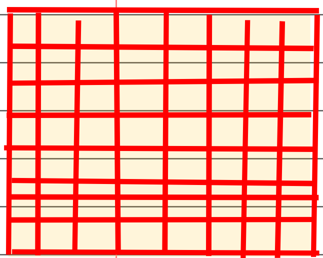
observe that $\left((\sqrt{2})^{\sqrt{2}}\right)^{\sqrt{2}} = (\sqrt{2})^{\sqrt{2}\times\sqrt{2}} = (\sqrt{2})^2 = 2$

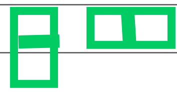
which is rational.

For another interesting non-constructive existential proof, see the chomp game example in the textbook (Example 12, Sec. 1.8)

More Examples

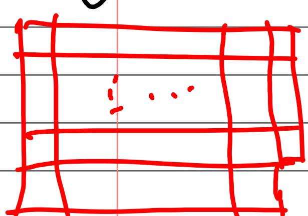
Ex: Can we tile the $\underbrace{\text{standard checkerboard}}_{8\times 8}$ with dominos?





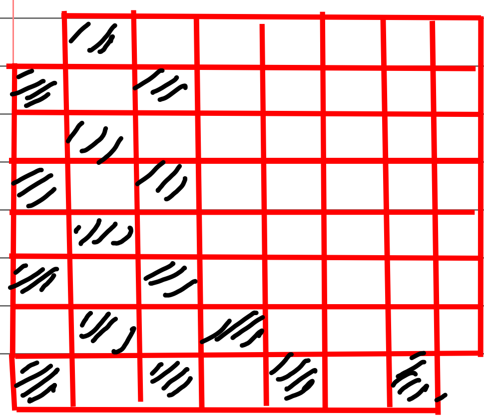
- yes. Start from the first row and first column and place all dominos vertically.

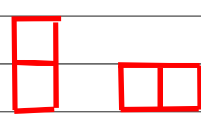
Ex: Can we tile a checkerboard obtained by removing one of the corners with dominos?



Assume that it is possible. Choose k to be the number of tiles that covers the map. observe that
$2 \times k = 63$ ⨳

Ex: Can we tile a checkerbard obtaind by removing the opposite corners by dominos?





Each tile covers 1 black and 1 white square.

Assume that it is possible to cover this map with K

dominos. Then, there should be k black squares, and k white squares. However, the number of white squares on the board is smaller than the number of black squares.

Advice for writing/reading Proofs

A good proof is clear and correct.

Clear: - Every statement has a clear meaning
- Every variable is bound

Correct: - every statement follows logically from the previous ones
- Calculations/other math is correct.

3 tips for writing a proof that is correct:

1) Be aware of the beginning (assumptions/hypothesis, defn)
middle (argument)
end (conclusion)

2) Use some keywords such as

+ Assume .... is arbitrary. ($\forall$)
+ Choose x such that ($\exists$)
+ Assume <hypothesis> ($\longrightarrow$)
+ We will show that <conclusion>
+ By the hypothesis/assumption/definition
+ It follows that ... / therefore ($\longrightarrow$)
+ You can use ($\rightarrow$) and ($\leftarrow$) two display splitting the biconditional.

+ Without Loss of Generality (WLOG) ...
(you are omitting some cases which can be proved exactly similarly by renaming, reordering variables)

+ observe that .. / Notice that ...

3) Be aware of quantifiers and bound variables.

Style: ① use complete English sentences.
② Try to be succint. But when in doubt, add more details.

Example of a bad proof:

prop.: $\sqrt{2}$ is irrational.

proof. $\sqrt{2} = 1.412\ldots$
This expansion never ends, so $\sqrt{2}$ is irrational. $\square$

Not clear

the logic is incorrect.

Very Very Very bad proof

How to find proofs

Problem: prove or disprove: $S = \forall x \; P(x) \to Q(x)$

Step 1: write down S and $\neg S =$

Step 2: write down all the definitions in the statements

Step 3: form a belief about S: True or false?
↳ try some small example
↳ either find a counterexample or a pattern

Step 4: Try to write a proof

Either find a proof or fail

revisit step 3.

A proof's structure:

Assumptions $\longrightarrow \longrightarrow \longrightarrow \longrightarrow \longrightarrow$ Conclusion

The process of finding a proof:

It's ok to fail and be stuck. I've been there more than you can imagine. But the joy of finally comming up with the proof!!