Simplify: ① $\neg(\forall a:\mathbb{N}.\ (\exists b:\mathbb{N}.\ ((a=0)\vee(a+b=0))))$

$\equiv \exists a:\mathbb{N}.\ \neg(\exists b:\mathbb{N}.\ (a=0)\vee(a+b=0))$

$\equiv \exists a:\mathbb{N}.\ \forall b:\mathbb{N}.\ \neg((a=0)\vee(a+b=0))$

$\equiv \exists a:\mathbb{N}.\ \forall b:\mathbb{N}.\ (a\neq 0)\wedge(a+b\neq 0)$

Quantifier Restriction

Consider "every even integer is equal to 2".

How to encode formally?

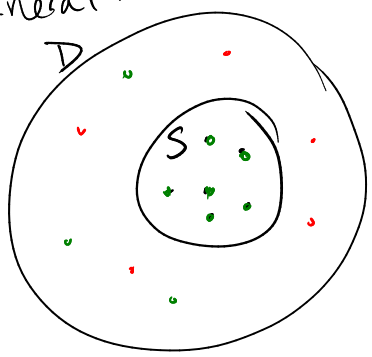
(domain of even integers)

① $\forall n:\mathrm{Even}.\ n=2.$

Alternatively:

② $\forall n:\mathbb{Z}.\ \mathrm{Even}(n)\longrightarrow(n=2).$

In general:



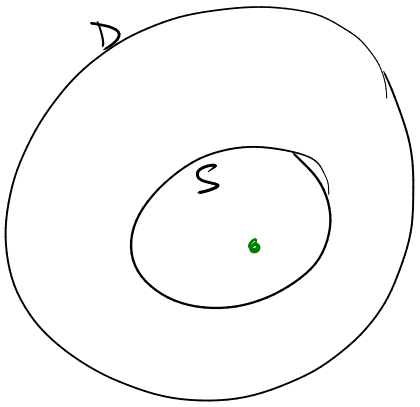
$\forall s:S.\ P(s)$

$\equiv \forall d:D.\ S(d)\longrightarrow P(d).$

Likewise

$\exists s:S.\ P(s)$

$\equiv \exists d:D.\ S(d)\wedge P(d).$



eg. "Every even integer greater than 2 can be written as the sum of two prime numbers".

$$\forall n : (\text{Even ints.} > 2) . \exists p : \text{Prime} . \exists q : \text{Prime} . n = p + q .$$

$$\equiv [\forall n : \mathbb{Z} . (\text{Even}(n) \wedge (n > 2)) \rightarrow] [(\exists p : \mathbb{N} . \text{Prime}(p) \wedge ([\exists q : \mathbb{N} . \text{Prime}(q) \wedge] (n = p + q)))]$$

Proofs!

Proof = formal way to establish the truth of a proposition.

Proofs can be written in many (more or less formal) styles, but the underlying structure is always the same.

For each propositional logic connective, we will see

1. How to prove a proposition of that form
2. How to use a proposition of that form if you already know it.

(Introduction / elimination rules)

---

1. True.

- To prove True, do nothing.
- If you know True, you know nothing.

	Prove / want	Use / know
T	—	—
F		Anything!
$P \wedge Q$	Prove P Prove Q	Know P Know Q.
$P \to Q$	Suppose P, prove Q.	If we know $P \to Q$ and we know P, then conclude Q.
$P \vee Q$	Prove P, OR prove Q. (your choice)	To show R if you know $P \vee Q$, show $(P \to R)$ and show $(Q \to R)$.
$\forall x : D . P(x)$	Let y be arbitrary Prove $P(y)$	Pick specific d Know $P(d)$
$\exists x : D . P(x)$	Pick specific d Prove $P(d)$	Let y be arbitrary Know $P(y)$.

② False

- There is no way to prove False.

  (Note: you may be able to prove False given specific assumptions. There is no way to prove it "from scratch".)

- If you know False, you can conclude anything you want.

  ("ex falso quodlibet" — "from false, anything you want")

③ $P \wedge Q$

- To prove $P \wedge Q$,
  - prove P
  - prove Q.
- If you know $P \wedge Q$, then you know P, and you know Q.

④ $P \to Q$

- To prove $P \to Q$, (temporarily) suppose P is true, and prove Q in that hypothetical world.
- If you know $P \to Q$, and you know P, then Q is true.

Ex. Prove: if $n > 2$ and $r > 10$, then $n > 2$.

Formally, $((n > 2) \wedge (r > 10)) \longrightarrow (n > 2)$.

To prove this, suppose $(n > 2) \wedge (r > 10)$; we must show $(n > 2)$.

| Since we know $(n > 2) \wedge (r > 10)$, we know $(n > 2)$.

Since we showed $(n > 2)$ under the assumption $(n > 2) \wedge (r > 10)$, therefore $(n > 2) \wedge (r > 10) \longrightarrow (n > 2)$.

(could omit.)

Ex. Write an outline for a proof of $P \to (Q \wedge R)$.

Proof. We must show $P \to (Q \wedge R)$. So suppose P; we must show $Q \wedge R$.

> To show $Q \wedge R$, we will show each seperately.
>
> | Proof of Q (using P).
>
> | Proof of R (using P).
>
> [Since we showed each of Q and R, therefor $Q \wedge R$.]

[Since we showed $Q \wedge R$ under the supposition P, therefor $P \to (Q \wedge R)$.] ∎

Ex. Prove that $(2n+1 > 6) \to (n > 2)$.

Proof. Suppose $(2n+1 > 6)$; we must show $n > 2$.

> $2n+1 > 6$
>
> $\to$ { subtract 1 from both sides }
>
> $2n > 5$
>
> $\to$ { divide both sides by 2 }
>
> $n > 5/2$
>
> $\to$ { $n > 5/2 > 2$ }.
>
> $n > 2$

∎

(QED = "quod erat demonstrandum" that which was to be demonstrated)

- $P \vee Q$.
  - To prove $P \vee Q$, prove P, OR prove Q (your choice).
  - If you know $P \vee Q$, and want to prove R, prove $(P \to R)$ and prove $(Q \to R)$. Then no matter which of P or Q is true, R will follow.

- $\forall x : D.\ P(x)$
  - To prove this, suppose y is an arbitrary element of the domain D, and prove $P(y)$.
  - If you know $\forall x : D.\ P(x)$, then you know $P(d)$ is true for any specific d in D of your choice.

assume nothing about y other than being in D.

technically, pick a new variable; can also reuse x.

- $\exists x : D.\ P(x)$
  - To prove $\exists x : D.\ P(x)$, pick a specific d in D of your choice and prove $P(d)$.
  - If you know $\exists x : D.\ P(x)$, let y represent an arbitrary element of D, then you know $P(y)$.

pick new variable!

Ex. Prove: if n is an odd integer, then n^2 is also odd.

$$\forall n : \mathbb{Z}.\ \text{Odd}(n) \rightarrow \text{Odd}(n^2).$$

$$\left[\ \text{Odd}(n) \equiv \exists k : \mathbb{Z}.\ n = 2k + 1\ \right].$$