

A Theorem Proving Assistant

Joe Duffin

School of Computer Science
University College Dublin

20th March 2017



- What is Theorem Proving
- What I Built
- How does it work

What is a Theorem?

A Theorem is a proposition which is not necessarily self-evident but can be proved with a chain of reasoning.

Theorem (\vee zero)

$$P \vee \text{true} \equiv \text{true}$$

What is Theorem Proving?

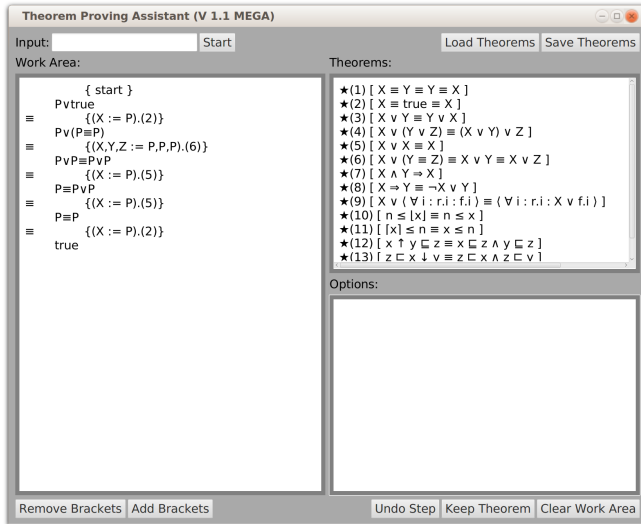
Proof of \vee zero

$$\begin{aligned} & P \vee \text{true} \\ \equiv & \{(X := P).(0)\} \\ & P \vee (P \equiv P) \\ \equiv & \{(X, Y, Z := P, P, P).(1)\} \\ & P \vee P \equiv P \vee P \\ \equiv & \{(X := P).(2)\} \\ & P \equiv P \\ \equiv & \{(X := P).(0)\} \\ & \text{true} \end{aligned}$$

Theorems

$$\begin{aligned} (0) & [X \equiv X \equiv \text{true}] \\ (1) & [X \vee (Y \equiv Z) \\ & \quad \equiv X \vee Y \equiv X \vee Z] \\ (2) & [X \vee X \equiv X] \end{aligned}$$

What I Built

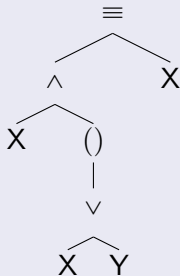


How it Works - Expression Representation

String Representation (*Absorb0*)

$$X \wedge (X \vee Y) \equiv X$$

Tree Representation (*Absorb0*)

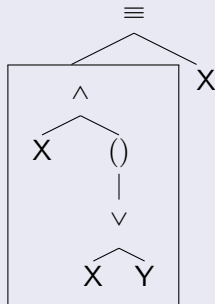


- Syntax trees are used to represent expressions.

How it Works - Pattern Matching

Rule:

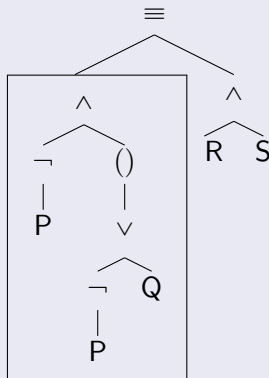
$$X \wedge (X \vee Y) \equiv X$$



Look Up Table

User Expression:

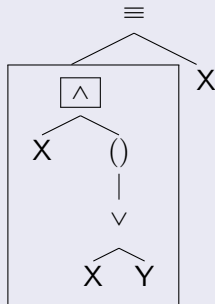
$$\neg P \wedge (\neg P \vee Q) \equiv R \wedge S$$



How it Works - Pattern Matching

Rule:

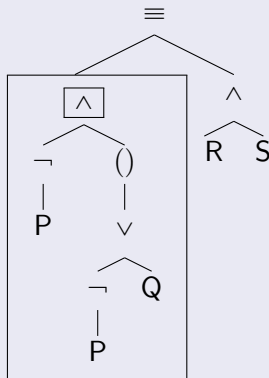
$$X \wedge (X \vee Y) \equiv X$$



Look Up Table

User Expression:

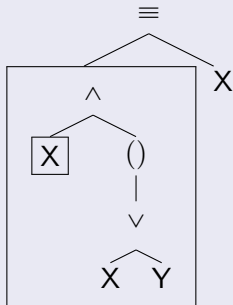
$$\neg P \wedge (\neg P \vee Q) \equiv R \wedge S$$



How it Works - Pattern Matching

Rule:

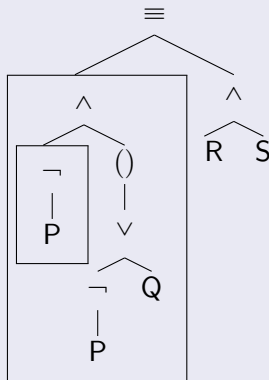
$$X \wedge (X \vee Y) \equiv X$$



Look Up Table

User Expression:

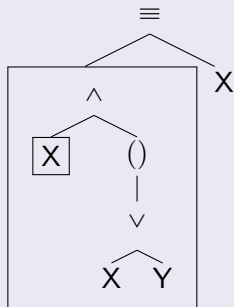
$$\neg P \wedge (\neg P \vee Q) \equiv R \wedge S$$



How it Works - Pattern Matching

Rule:

$$X \wedge (X \vee Y) \equiv X$$

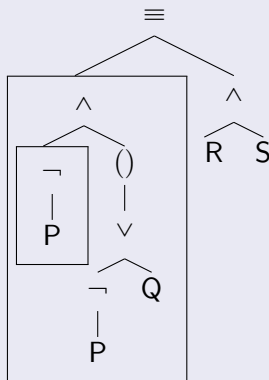


Look Up Table

$$X := \neg P$$

User Expression:

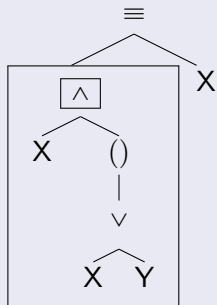
$$\neg P \wedge (\neg P \vee Q) \equiv R \wedge S$$



How it Works - Pattern Matching

Rule:

$$X \wedge (X \vee Y) \equiv X$$

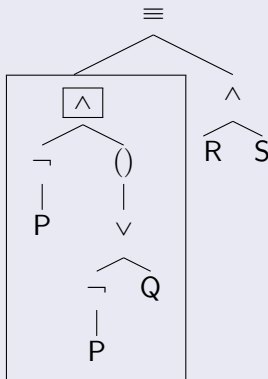


Look Up Table

$$X := \neg P$$

User Expression:

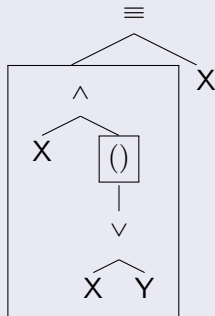
$$\neg P \wedge (\neg P \vee Q) \equiv R \wedge S$$



How it Works - Pattern Matching

Rule:

$$X \wedge (X \vee Y) \equiv X$$

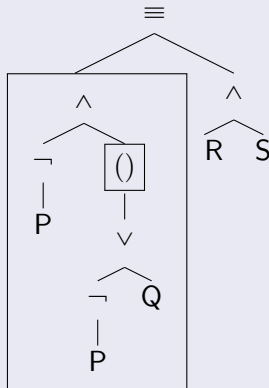


Look Up Table

$$X := \neg P$$

User Expression:

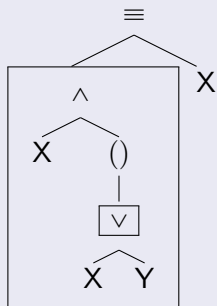
$$\neg P \wedge (\neg P \vee Q) \equiv R \wedge S$$



How it Works - Pattern Matching

Rule:

$$X \wedge (X \vee Y) \equiv X$$

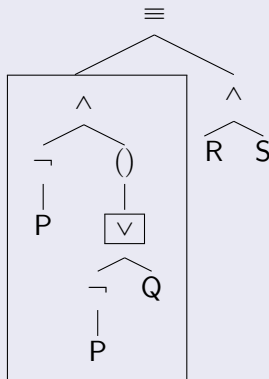


Look Up Table

$$X := \neg P$$

User Expression:

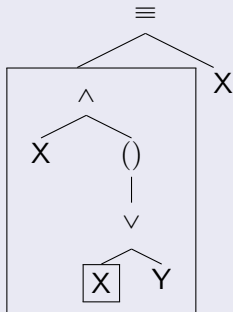
$$\neg P \wedge (\neg P \vee Q) \equiv R \wedge S$$



How it Works - Pattern Matching

Rule:

$$X \wedge (X \vee Y) \equiv X$$

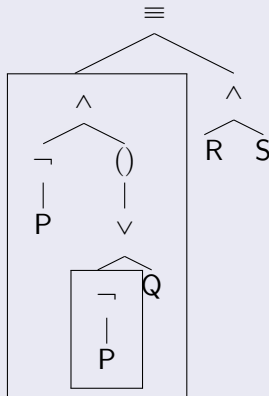


Look Up Table

$$X := \neg P$$

User Expression:

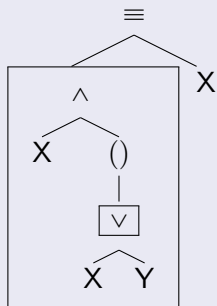
$$\neg P \wedge (\neg P \vee Q) \equiv R \wedge S$$



How it Works - Pattern Matching

Rule:

$$X \wedge (X \vee Y) \equiv X$$

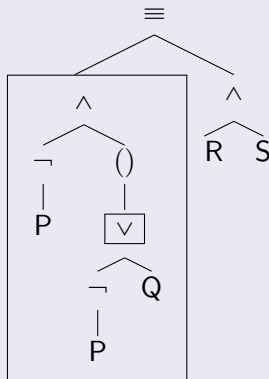


Look Up Table

$$X := \neg P$$

User Expression:

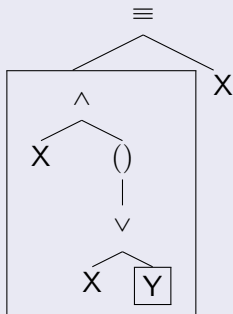
$$\neg P \wedge (\neg P \vee Q) \equiv R \wedge S$$



How it Works - Pattern Matching

Rule:

$$X \wedge (X \vee Y) \equiv X$$

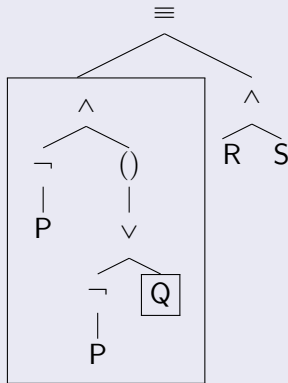


Look Up Table

$$X := \neg P$$

User Expression:

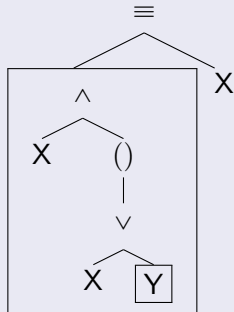
$$\neg P \wedge (\neg P \vee Q) \equiv R \wedge S$$



How it Works - Pattern Matching

Rule:

$$X \wedge (X \vee Y) \equiv X$$



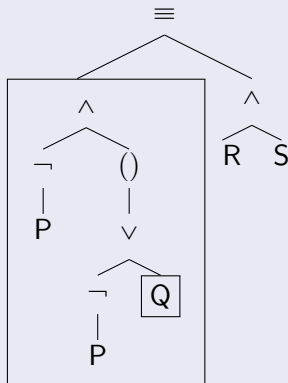
Look Up Table

$$X := \neg P$$

$$Y := Q$$

User Expression:

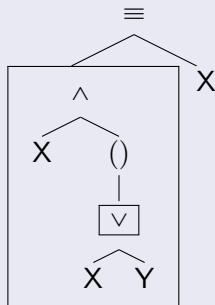
$$\neg P \wedge (\neg P \vee Q) \equiv R \wedge S$$



How it Works - Pattern Matching

Rule:

$$X \wedge (X \vee Y) \equiv X$$



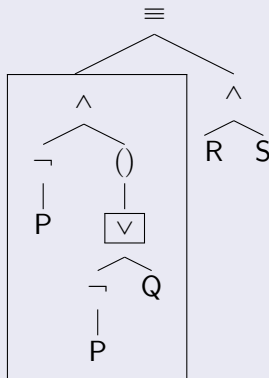
Look Up Table

$$X := \neg P$$

$$Y := Q$$

User Expression:

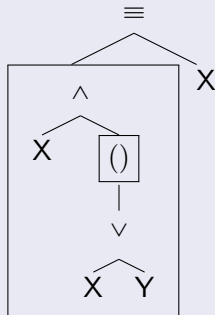
$$\neg P \wedge (\neg P \vee Q) \equiv R \wedge S$$



How it Works - Pattern Matching

Rule:

$$X \wedge (X \vee Y) \equiv X$$



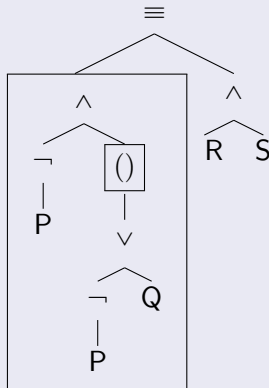
Look Up Table

$$X := \neg P$$

$$Y := Q$$

User Expression:

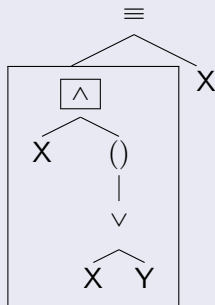
$$\neg P \wedge (\neg P \vee Q) \equiv R \wedge S$$



How it Works - Pattern Matching

Rule:

$$X \wedge (X \vee Y) \equiv X$$



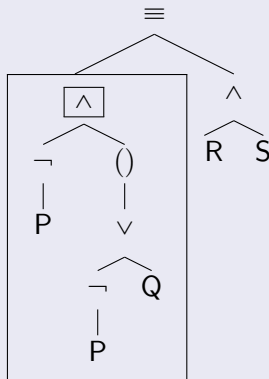
Look Up Table

$$X := \neg P$$

$$Y := Q$$

User Expression:

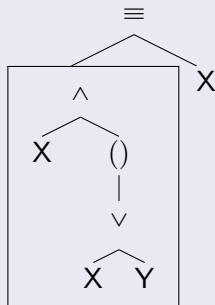
$$\neg P \wedge (\neg P \vee Q) \equiv R \wedge S$$



How it Works - Pattern Matching

Rule:

$$X \wedge (X \vee Y) \equiv X$$



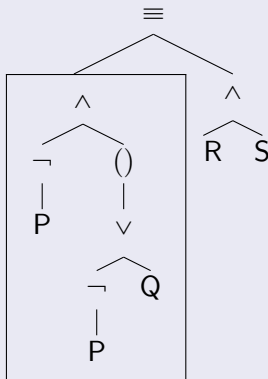
Look Up Table

$$X := \neg P$$

$$Y := Q$$

User Expression:

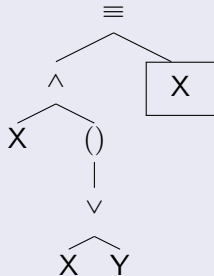
$$\neg P \wedge (\neg P \vee Q) \equiv R \wedge S$$



How it Works - Pattern Matching

Rule:

$$X \wedge (X \vee Y) \equiv X$$



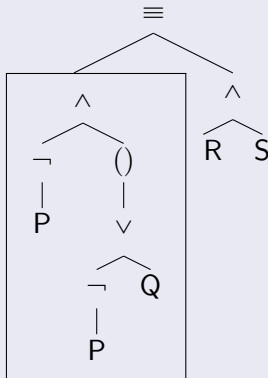
Look Up Table

$$X := \neg P$$

$$Y := Q$$

User Expression:

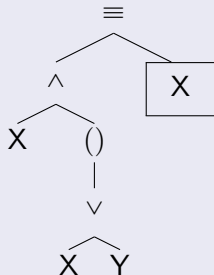
$$\neg P \wedge (\neg P \vee Q) \equiv R \wedge S$$



How it Works - Pattern Matching

Rule:

$$X \wedge (X \vee Y) \equiv X$$



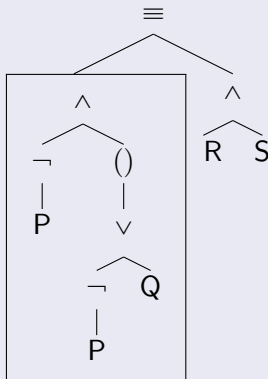
Look Up Table

$$X := \neg P$$

$$Y := Q$$

User Expression:

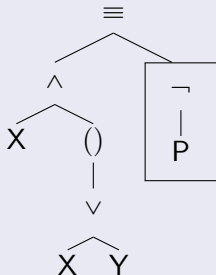
$$\neg P \wedge (\neg P \vee Q) \equiv R \wedge S$$



How it Works - Pattern Matching

Rule:

$$X \wedge (X \vee Y) \equiv X$$



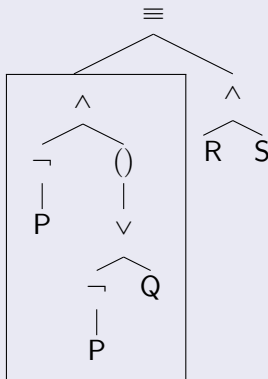
Look Up Table

$$X := \neg P$$

$$Y := Q$$

User Expression:

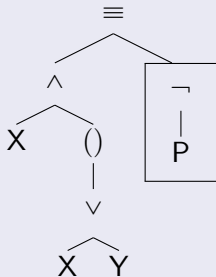
$$\neg P \wedge (\neg P \vee Q) \equiv R \wedge S$$



How it Works - Pattern Matching

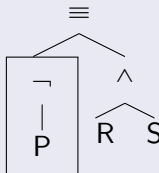
Rule:

$$X \wedge (X \vee Y) \equiv X$$



User Expression:

$$\neg P \equiv R \wedge S$$



Look Up Table

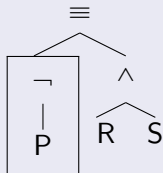
$$X := \neg P$$

$$Y := Q$$

How it Works - Pattern Matching

User Expression:

$$\neg P \equiv R \wedge S$$



Look Up Table

$$X := \neg P$$

$$Y := Q$$

- The new user expression and lookup table are used to generate the hint and next line of the proof.

The Step

$$\begin{aligned} & \neg P \wedge (\neg P \vee Q) \equiv R \wedge S \\ \equiv & \quad \{(X, Y ::= \neg P, Q).Abs0\} \\ & \neg P \equiv R \wedge S \end{aligned}$$

Conclusion

Questions...