Discrete Algebraic Structures

WiSe 2025/2026

Prof. Dr. Antoine Wiehe
Research Group for Theoretical Computer Science

- Definition; be able to determine if a given set $f \subseteq A \times B$ is a function or not
- Properties of functions: injectivity, surjectivity, bijectivity
- Composition of functions
- Identity function
- Inverses

Question. Let $f\colon A \to B$ be a function. Can one "undo" f?
Given $b \in B$, is it possible to understand where b came from?

Need f to be both injective and surjective!

Theorem. If $f\colon A \to B$ is bijective, there exists $g\colon B \to A$ such that $g \circ f = \mathrm{Id}_A$ and $f \circ g = \mathrm{Id}_B$.
This g is unique, called the inverse of f, and written f^{-1}.

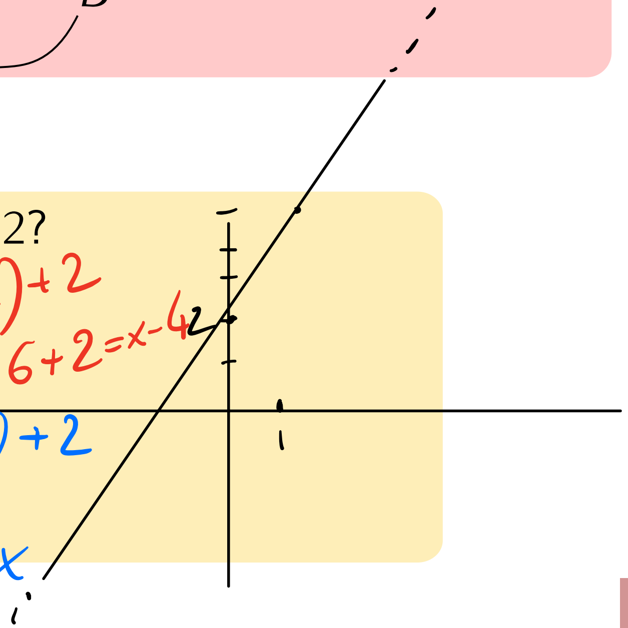
$$\begin{tikzcd} A \arrow[r, bend left, "f"] & B \arrow[l, bend left, "f^{-1}"] \end{tikzcd}$$

So $f^{-1}(f(a)) = a$ and $f(f^{-1}(b)) = b$ for all $a \in A, b \in B$.

What is the inverse of $f\colon \mathbb{Q} \to \mathbb{Q}$ defined by $f(x) = 3x + 2$?

- Trick question! f has no inverse ✗
- Trick question! f is not a function ✗
- $f^{-1}(x) = \frac{1}{3}x - 2$ × $f(f^{-1}(x)) = f(\frac{1}{3}x - 2) = 3(\frac{1}{3}x - 2) + 2 = x - 6 + 2 = x - 4$
- $f^{-1}(x) = \frac{1}{3}(x - 2)$ ✓ $f(f^{-1}(x)) = f(\frac{1}{3}(x-2)) = 3 \cdot \frac{1}{3}(x-2) + 2 = x$
- $f^{-1}(x) = \frac{3}{x-2}$ ✗

$f^{-1}(f(x)) = f^{-1}(3x+2) = \dots = x$



Introduction to Logic

- A language: a syntax (how to write things) and a semantics (what the things mean)

- A language: a syntax (how to write things) and a semantics (what the things mean)
- Propositional logic and Predicate logic

- A language: a syntax (how to write things) and a semantics (what the things mean)
- Propositional logic and Predicate logic

Propositional logic:

- the "mathematics of 0 and 1"

- A language: a syntax (how to write things) and a semantics (what the things mean)
- Propositional logic and Predicate logic

Propositional logic:

- the "mathematics of 0 and 1"
- Applications in CS engineering: down to the hardware side, everything is 0/1. Logic important for:
  - electronic circuit synthesis
  - minimization of circuits

- A language: a syntax (how to write things) and a semantics (what the things mean)
- Propositional logic and Predicate logic

Propositional logic:

- the “mathematics of 0 and 1”
- Applications in CS engineering: down to the hardware side, everything is 0/1. Logic important for:
  - electronic circuit synthesis
  - minimization of circuits
- Applications in math: how to prove things
  - 0=False,
  - 1=True
  - how to manipulate mathematical statements without making reasoning mistakes
  - how to recognize fallacies also in everyday life

- A language: a syntax (how to write things) and a semantics (what the things mean)
- Propositional logic and Predicate logic

Propositional logic:

- the "mathematics of 0 and 1"
- Applications in CS engineering: down to the hardware side, everything is 0/1. Logic important for:
  - electronic circuit synthesis
  - minimization of circuits
- Applications in math: how to prove things
  - 0=False,
  - 1=True
  - how to manipulate mathematical statements without making reasoning mistakes
  - how to recognize fallacies also in everyday life

Predicate logic:

- In CS: automated software verification
  (increasingly employed and demanded at tech giants like Microsoft and Amazon)
- In math: more powerful language using quantifiers

Syntax = what is legal to write

Syntax = what is legal to write

Definition (Propositional formulas)**.** The following are the only legal formulas:

1. every variable $p, q, r, \ldots$ is a formula value in $\{0,1\}$
2. $\top$ true and $\boxed{\bot}$ false are formulas, (TRUE and FALSE)
3. If ϕ and ψ are formulas, then $\phi \wedge \psi$ is a formula, (AND)
4. If ϕ and ψ are formulas, then $\phi \vee \psi$ is a formula, (OR)
5. If ϕ and ψ are formulas, then $\phi \Rightarrow \psi$ is a formula, (IMPLIES)
6. If ϕ is a formula, then $\neg\phi$ is a formula. (NOT)

Syntax = what is legal to write

Definition (Propositional formulas)**.** The following are the only legal formulas:

1. every variable $p, q, r, \ldots$ is a formula
2. $\top$ and $\bot$ are formulas, (TRUE and FALSE)
3. If ϕ and ψ are formulas, then $\phi \land \psi$ is a formula, (AND)
4. If If ϕ and ψ are formulas, then $\phi \lor \psi$ is a formula, (OR)
5. If ϕ and ψ are formulas, then $\phi \Rightarrow \psi$ is a formula, (IMPLIES)
6. If ϕ is a formula, then $\neg\phi$ is a formula. (NOT)

Example. $p \lor q$, $p \lor \top$, $p \land p$, $p \land \land p$, $\neg p \land \neg(\neg p)$, $(\neg p) \land ((\neg q) \Rightarrow r)$, $((p \Rightarrow q) \Rightarrow p) \Rightarrow p$

Syntax = what is legal to write

Definition (Propositional formulas)**.** The following are the only legal formulas:

1. every variable $p, q, r, \ldots$ is a formula
2. $\top$ and $\bot$ are formulas, (TRUE and FALSE)
3. If ϕ and ψ are formulas, then $\phi \wedge \psi$ is a formula, (AND)
4. If If ϕ and ψ are formulas, then $\phi \vee \psi$ is a formula, (OR)
5. If ϕ and ψ are formulas, then $\phi \Rightarrow \psi$ is a formula, (IMPLIES)
6. If ϕ is a formula, then $\neg\phi$ is a formula. (NOT)

Example. $p \vee q$, $p \vee \top$, $p \wedge p$, $p \wedge \wedge p$, $\neg p \wedge \neg(\neg p)$, $(\neg p) \wedge ((\neg q) \Rightarrow r)$, $((p \Rightarrow q) \Rightarrow p) \Rightarrow p$

formula (by 1.)

formula (by 1.)

Syntax = what is legal to write

Definition (Propositional formulas)**.** The following are the only legal formulas:

1. every variable $p, q, r, \ldots$ is a formula
2. $\top$ and $\bot$ are formulas, (TRUE and FALSE)
3. If ϕ and ψ are formulas, then $\phi \wedge \psi$ is a formula, (AND)
4. If If ϕ and ψ are formulas, then $\phi \vee \psi$ is a formula, (OR)
5. If ϕ and ψ are formulas, then $\phi \Rightarrow \psi$ is a formula, (IMPLIES)
6. If ϕ is a formula, then $\neg\phi$ is a formula. (NOT)

Example. $p \vee q$, $p \vee \top$, $p \wedge p$, $p \wedge \wedge p$, $\neg p \wedge \neg(\neg p)$, $(\neg p) \wedge ((\neg q) \Rightarrow r)$, $((p \Rightarrow q) \Rightarrow p) \Rightarrow p$

formula
(by 4.)

Syntax = what is legal to write

Definition (Propositional formulas)**.** The following are the only legal formulas:

1. every variable $p, q, r, \ldots$ is a formula
2. $\top$ and $\bot$ are formulas, (TRUE and FALSE)
3. If ϕ and ψ are formulas, then $\phi \wedge \psi$ is a formula, (AND)
4. If If ϕ and ψ are formulas, then $\phi \vee \psi$ is a formula, (OR)
5. If ϕ and ψ are formulas, then $\phi \Rightarrow \psi$ is a formula, (IMPLIES)
6. If ϕ is a formula, then $\neg\phi$ is a formula. (NOT)

Example. $p \vee q$, $p \vee \top$, $p \wedge p$, $p \wedge \wedge p$, $\neg p \wedge \neg(\neg p)$, $(\neg p) \wedge ((\neg q) \Rightarrow r)$, $((p \Rightarrow q) \Rightarrow p) \Rightarrow p$

formula (by 1.)

formula (by 2.)

Syntax = what is legal to write

Definition (Propositional formulas)**.** The following are the only legal formulas:

1. every variable $p, q, r, \ldots$ is a formula
2. $\top$ and $\bot$ are formulas, (TRUE and FALSE)
3. If ϕ and ψ are formulas, then $\phi \wedge \psi$ is a formula, (AND)
4. If If ϕ and ψ are formulas, then $\phi \vee \psi$ is a formula, (OR)
5. If ϕ and ψ are formulas, then $\phi \Rightarrow \psi$ is a formula, (IMPLIES)
6. If ϕ is a formula, then $\neg\phi$ is a formula. (NOT)

Example. $p \vee q$, $p \vee \top$, $p \wedge p$, $p \wedge \wedge p$, $\neg p \wedge \neg(\neg p)$, $(\neg p) \wedge ((\neg q) \Rightarrow r)$, $((p \Rightarrow q) \Rightarrow p) \Rightarrow p$

formula
(by 4.)

Syntax = what is legal to write

Definition (Propositional formulas)**.** The following are the only legal formulas:

1. every variable $p, q, r, \ldots$ is a formula
2. $\top$ and $\bot$ are formulas, (TRUE and FALSE)
3. If ϕ and ψ are formulas, then $\phi \land \psi$ is a formula, (AND)
4. If If ϕ and ψ are formulas, then $\phi \lor \psi$ is a formula, (OR)
5. If ϕ and ψ are formulas, then $\phi \Rightarrow \psi$ is a formula, (IMPLIES)
6. If ϕ is a formula, then $\neg\phi$ is a formula. (NOT)

Example. $p \lor q$, $p \lor \top$, $p \land p$, $p \land \land p$, $\neg p \land \neg(\neg p)$, $(\neg p) \land ((\neg q) \Rightarrow r)$, $((p \Rightarrow q) \Rightarrow p) \Rightarrow p$

formula
(by 1.)

Syntax = what is legal to write

Definition (Propositional formulas)**.** The following are the only legal formulas:

1. every variable $p, q, r, \ldots$ is a formula
2. $\top$ and $\bot$ are formulas, (TRUE and FALSE)
3. If ϕ and ψ are formulas, then $\phi \wedge \psi$ is a formula, (AND)
4. If If ϕ and ψ are formulas, then $\phi \vee \psi$ is a formula, (OR)
5. If ϕ and ψ are formulas, then $\phi \Rightarrow \psi$ is a formula, (IMPLIES)
6. If ϕ is a formula, then $\neg\phi$ is a formula. (NOT)

Example. $p \vee q$, $p \vee \top$, $p \wedge p$, $p \wedge \wedge p$, $\neg p \wedge \neg(\neg p)$, $(\neg p) \wedge ((\neg q) \Rightarrow r)$, $((p \Rightarrow q) \Rightarrow p) \Rightarrow p$

formula
(by 3.)

Syntax = what is legal to write

Definition (Propositional formulas)**.** The following are the only legal formulas:

1. every variable $p, q, r, \dots$ is a formula
2. $\top$ and $\bot$ are formulas, (TRUE and FALSE)
3. If ϕ and ψ are formulas, then $\phi \wedge \psi$ is a formula, (AND)
4. If If ϕ and ψ are formulas, then $\phi \vee \psi$ is a formula, (OR)
5. If ϕ and ψ are formulas, then $\phi \Rightarrow \psi$ is a formula, (IMPLIES)
6. If ϕ is a formula, then $\neg\phi$ is a formula. (NOT)

Example. $p \vee q$, $p \vee \top$, $p \wedge p$, $p \wedge \wedge p$, $\neg p \wedge \neg(\neg p)$, $(\neg p) \wedge ((\neg q) \Rightarrow r)$, $((p \Rightarrow q) \Rightarrow p) \Rightarrow p$

we are allowed to put parentheses/brackets around formulas,
like $3x + 1$ and $3x + (1)$
like $x + y \times z$ and $(x + y) \times z$

Syntax = what is legal to write

Definition (Propositional formulas)**.** The following are the only legal formulas:

1. every variable $p, q, r, \ldots$ is a formula
2. $\top$ and $\bot$ are formulas, (TRUE and FALSE)
3. If ϕ and ψ are formulas, then $\phi \land \psi$ is a formula, (AND)
4. If If ϕ and ψ are formulas, then $\phi \lor \psi$ is a formula, (OR)
5. If ϕ and ψ are formulas, then $\phi \Rightarrow \psi$ is a formula, (IMPLIES)
6. If ϕ is a formula, then $\neg\phi$ is a formula. (NOT)

Example. $p \lor q$, $p \lor \top$, $p \land p$, $p \cancel{\land \land} p$, $\neg p \land \neg(\neg p)$, $(\neg p) \land ((\neg q) \Rightarrow r)$, $((p \Rightarrow q) \Rightarrow p) \Rightarrow p$

$(p \land) \land p$

Which of the remaining examples is a legal formula?

$\neg p \land \neg(\neg p)$

$\neg p$

p

$p \Rightarrow q$ ✓ (S.)

$(p \Rightarrow q) \Rightarrow p$ ✓ (S.)

$((p \Rightarrow q) \Rightarrow p) \Rightarrow p$ ✓ (S.)

$$(p \vee q) \wedge (\neg p \vee \neg q)$$

$$(p \lor q) \land (\neg p \lor \neg q)$$

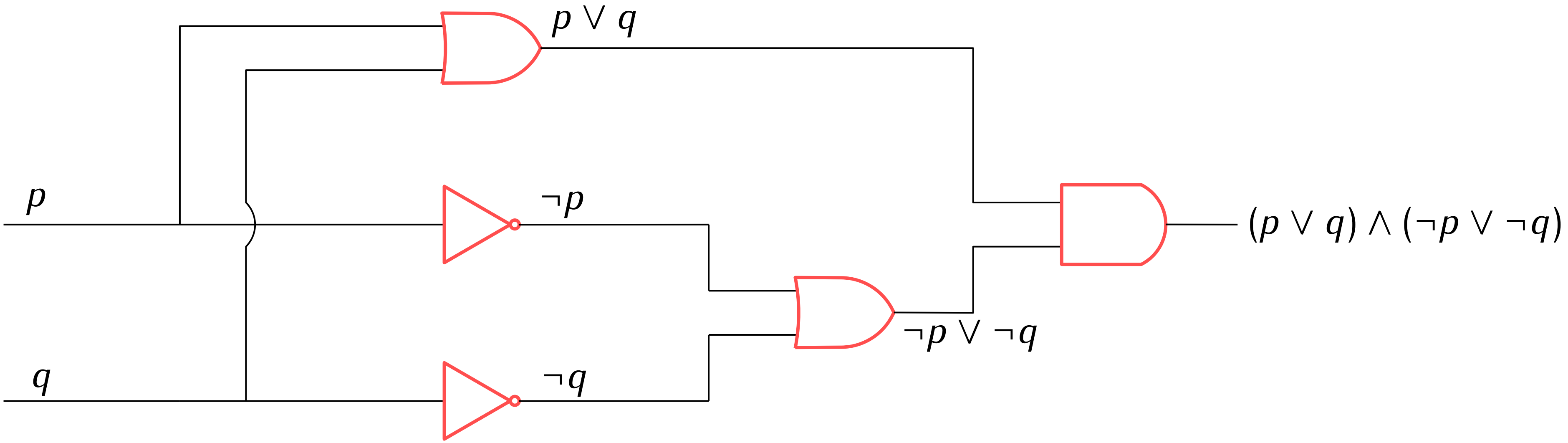
variables = 0/1 inputs

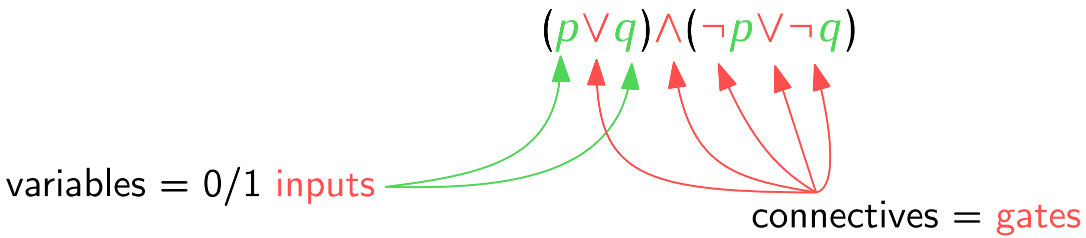
connectives = gates

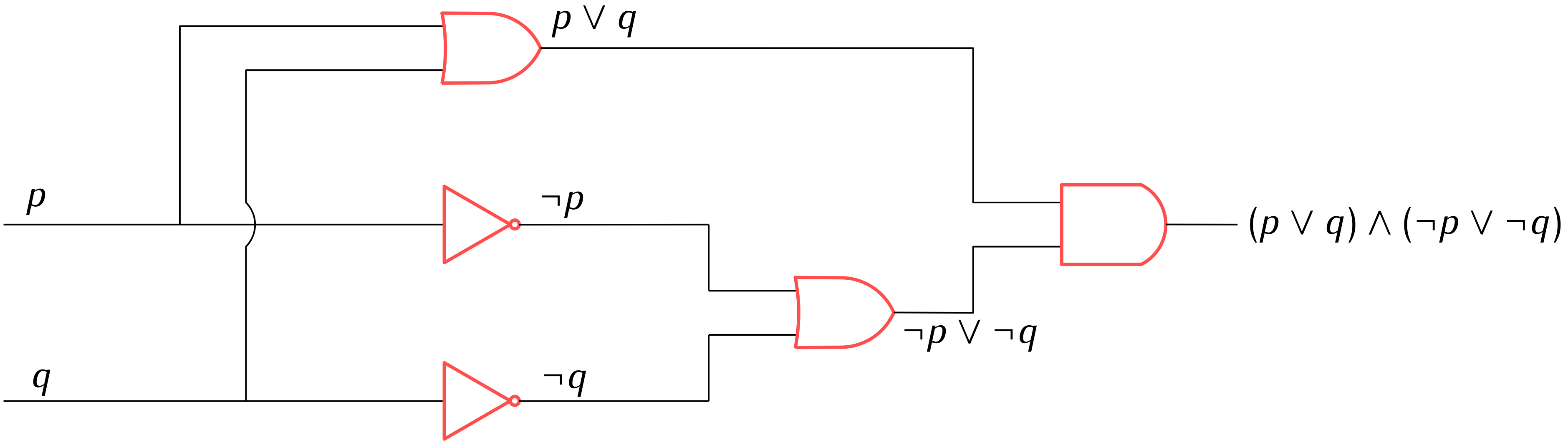
$(p \vee q) \wedge (\neg p \vee \neg q)$

variables = 0/1 inputs

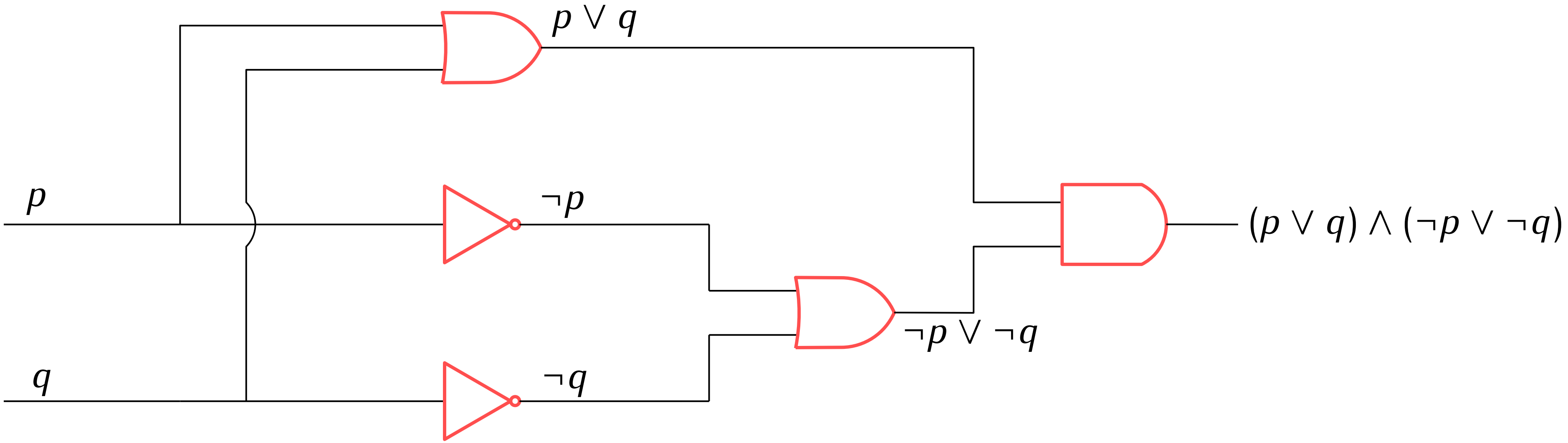
connectives = gates

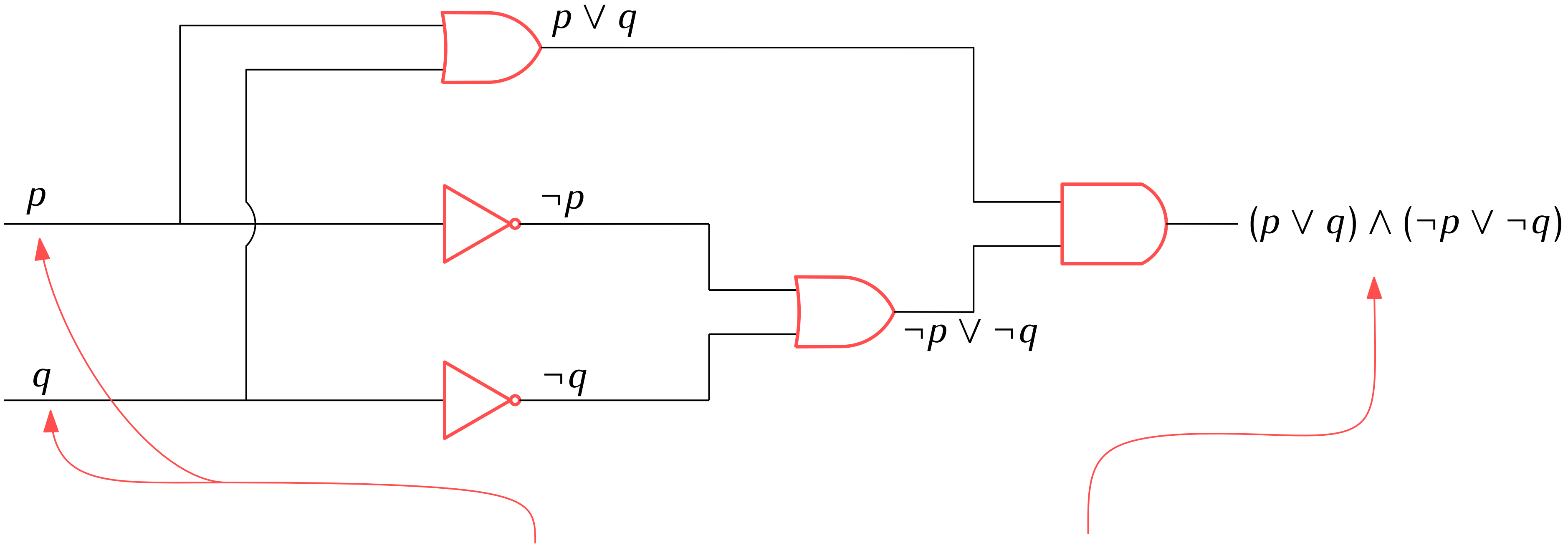




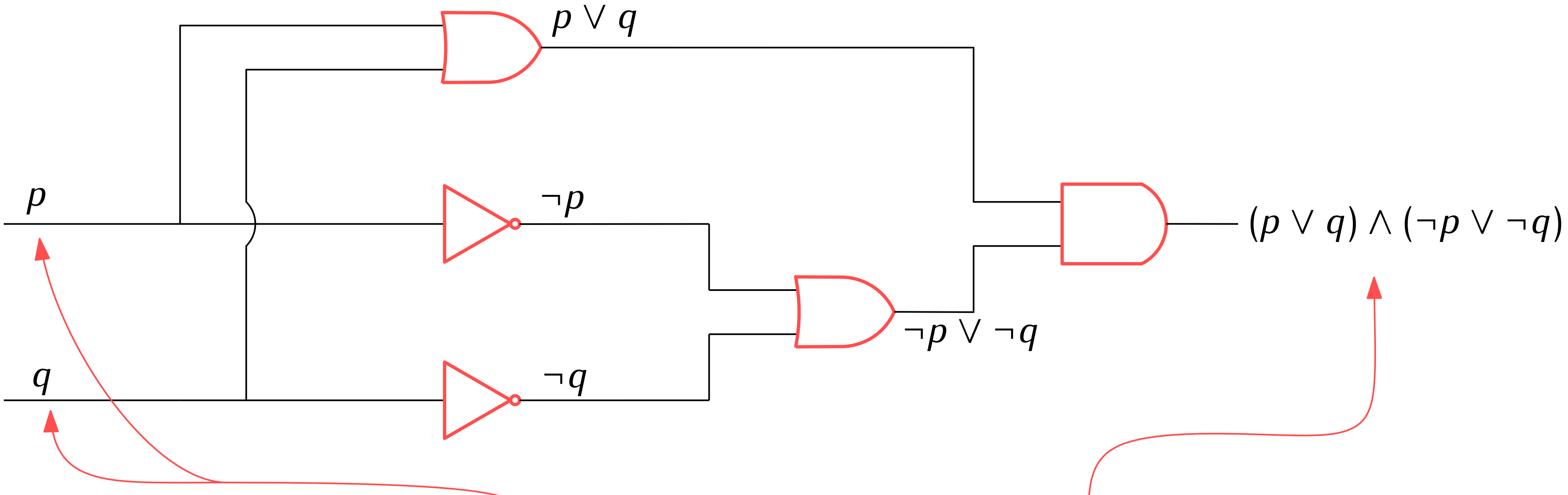


Question. For which values of the inputs (0/1) does the circuit output 1?


$p \lor q$
p
$\neg p$
$(p \lor q) \land (\neg p \lor \neg q)$
$\neg p \lor \neg q$
q
$\neg q$

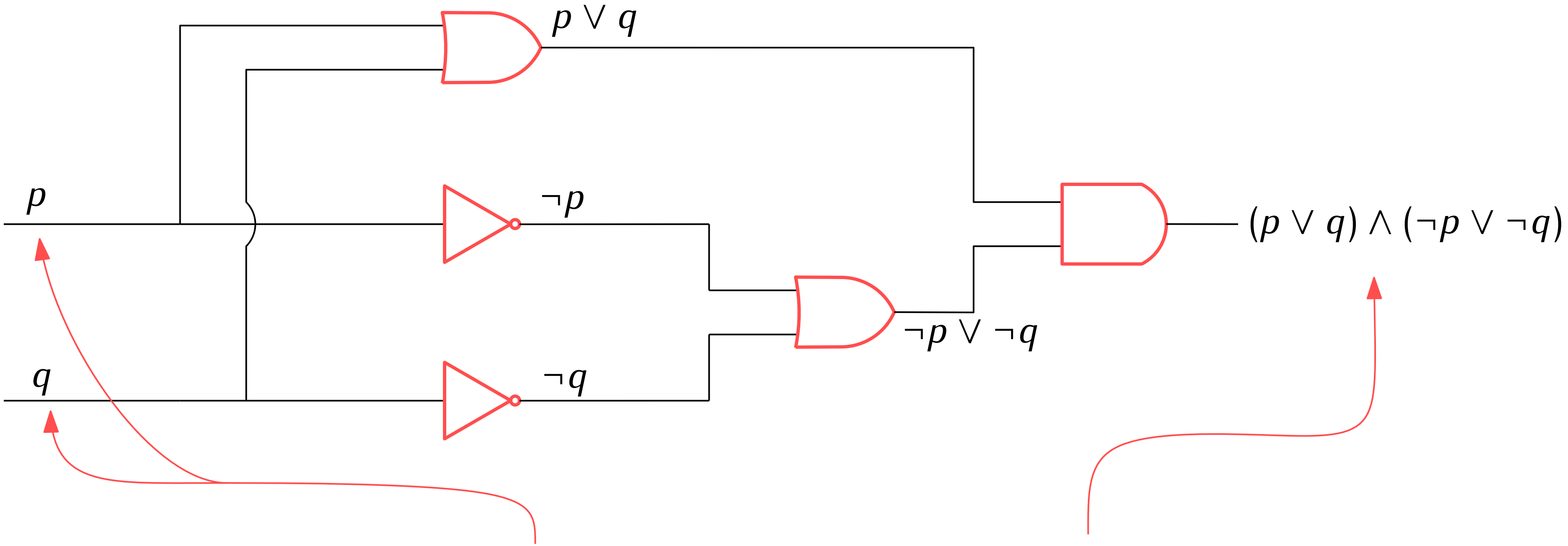


For each value of these in $\{0, 1\}$, we have a value of this in $\{0, 1\}$



For each value of these in $\{0, 1\}$, we have a value of this in $\{0, 1\}$

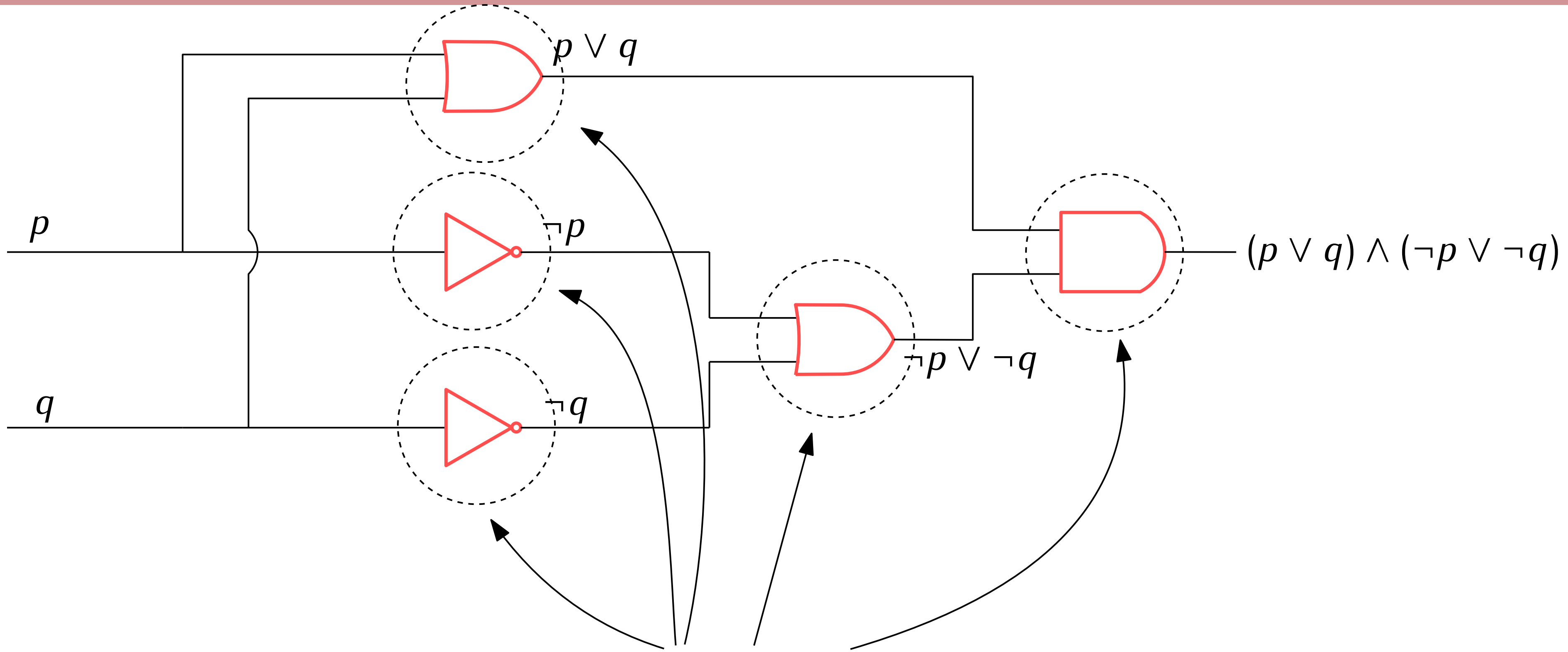
p	q	$(p \vee q) \wedge (\neg p \vee \neg q)$
0	0	
0	1	
1	0	
1	1	



For each value of these in $\{0, 1\}$, we have a value of this in $\{0, 1\}$

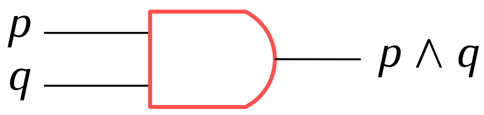
p	q	$(p \lor q) \land (\neg p \lor \neg q)$
0	0	
0	1	
1	0	
1	1	

truth table of $(p \lor q) \land (\neg p \lor \neg q)$



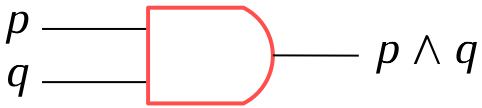
We start by defining the truth table for these

- Case of $\wedge$:



p	q	$p \wedge q$
0	0	0
0	1	0
1	0	0
1	1	1

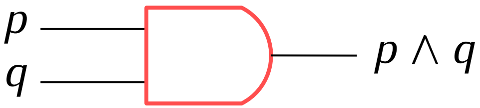
- Case of $\wedge$:



p	q	$p \wedge q$
0	0	0
0	1	0
1	0	0
1	1	1

both inputs must be 1

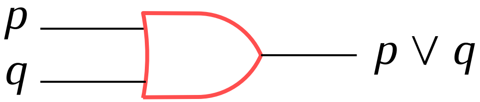
- Case of $\wedge$:



p	q	$p \wedge q$
0	0	0
0	1	0
1	0	0
1	1	1

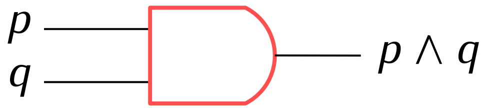
both inputs must be 1

- Case of $\vee$:



p	q	$p \vee q$
0	0	0
0	1	1
1	0	1
1	1	1

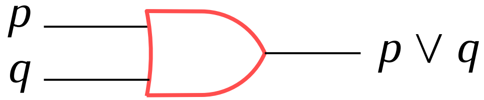
- Case of $\wedge$:



p	q	$p \wedge q$
0	0	0
0	1	0
1	0	0
1	1	1

both inputs must be 1

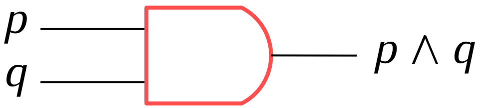
- Case of $\vee$:



p	q	$p \vee q$
0	0	0
0	1	1
1	0	1
1	1	1

it suffices that one of the inputs is 1

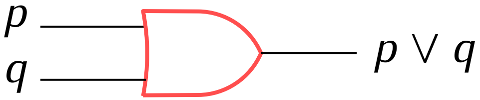
- Case of $\wedge$:



p	q	$p \wedge q$
0	0	0
0	1	0
1	0	0
1	1	1

both inputs must be 1

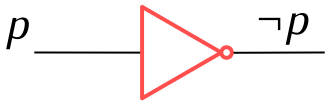
- Case of $\vee$:



p	q	$p \vee q$
0	0	0
0	1	1
1	0	1
1	1	1

it suffices that one of the inputs is 1

- Case of $\neg$:

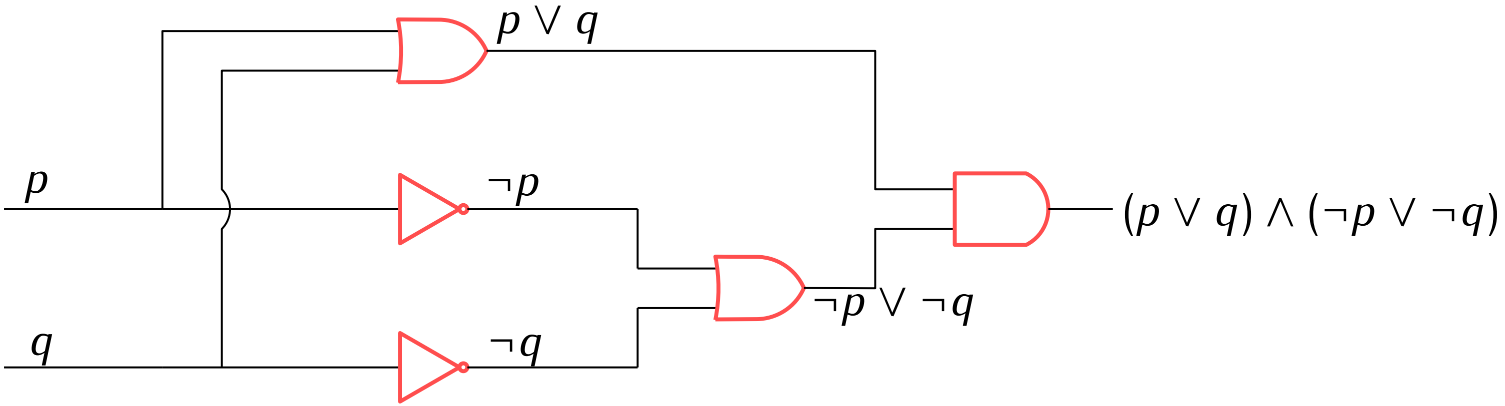


p	$\neg p$
0	1
1	0

p	q	$p \wedge q$
0	0	0
0	1	0
1	0	0
1	1	1

p	q	$p \vee q$
0	0	0
0	1	1
1	0	1
1	1	1

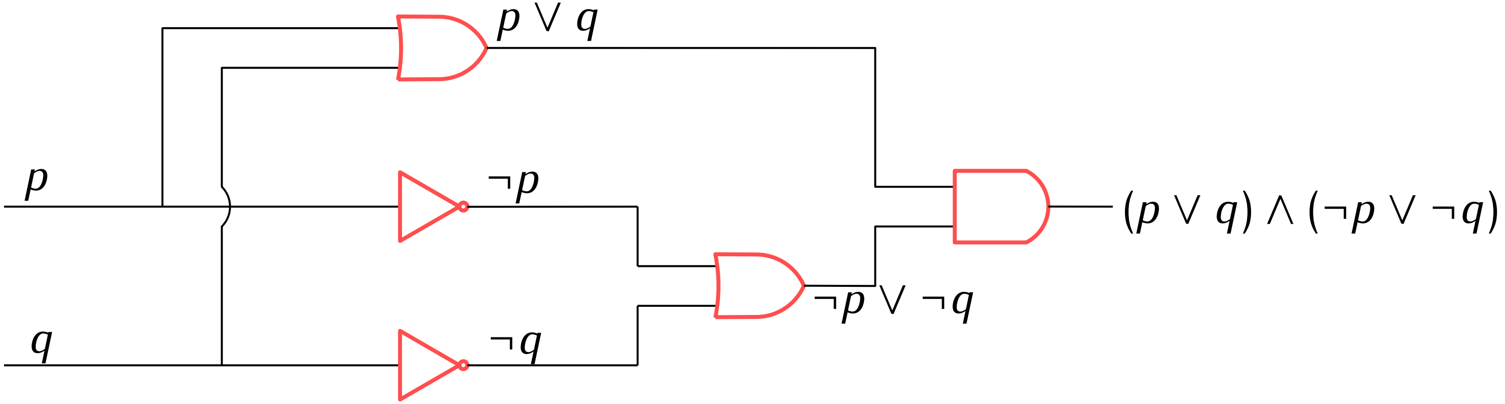
p	$\neg p$
0	1
1	0



p	q	$p \wedge q$
0	0	0
0	1	0
1	0	0
1	1	1

p	q	$p \vee q$
0	0	0
0	1	1
1	0	1
1	1	1

p	$\neg p$
0	1
1	0

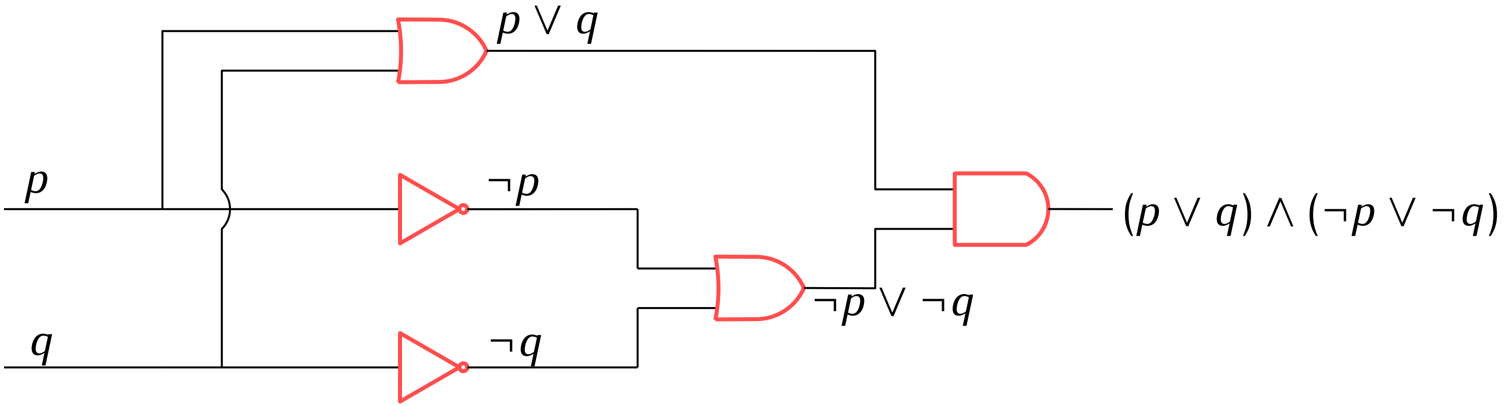


p	q	$\neg p$	$\neg q$	$p \vee q$	$\neg p \vee \neg q$	$(p \vee q) \wedge (\neg p \vee \neg q)$
0	0					
0	1					
1	0					
1	1					

p	q	$p \wedge q$
0	0	0
0	1	0
1	0	0
1	1	1

p	q	$p \vee q$
0	0	0
0	1	1
1	0	1
1	1	1

p	$\neg p$
0	1
1	0

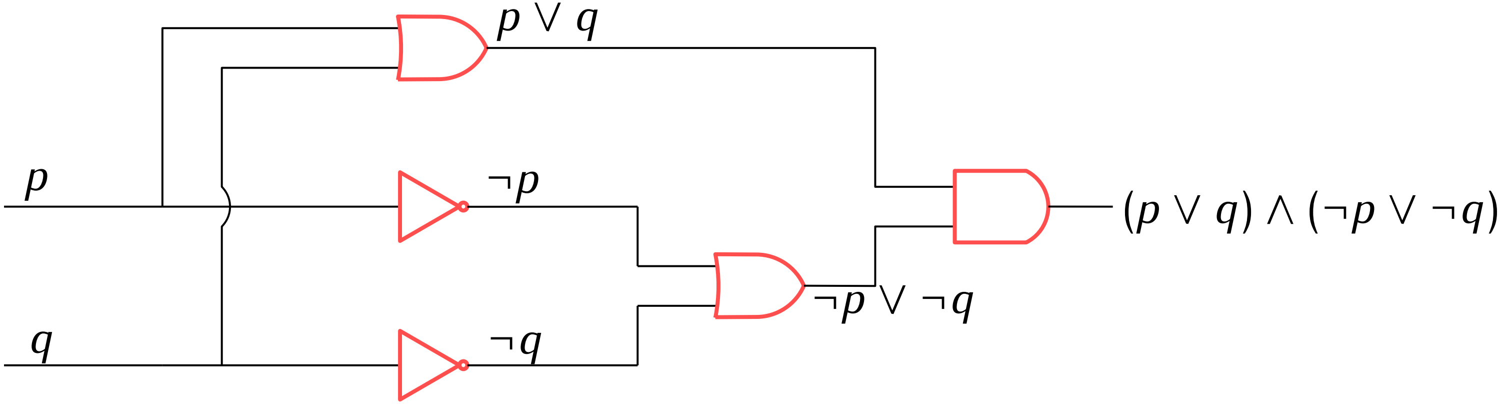


p	q	$\neg p$	$\neg q$	$p \vee q$	$\neg p \vee \neg q$	$(p \vee q) \wedge (\neg p \vee \neg q)$
0	0					
0	1					
1	0					
1	1					

p	q	$p \land q$
0	0	0
0	1	0
1	0	0
1	1	1

p	q	$p \lor q$
0	0	0
0	1	1
1	0	1
1	1	1

p	$\neg p$
0	1
1	0

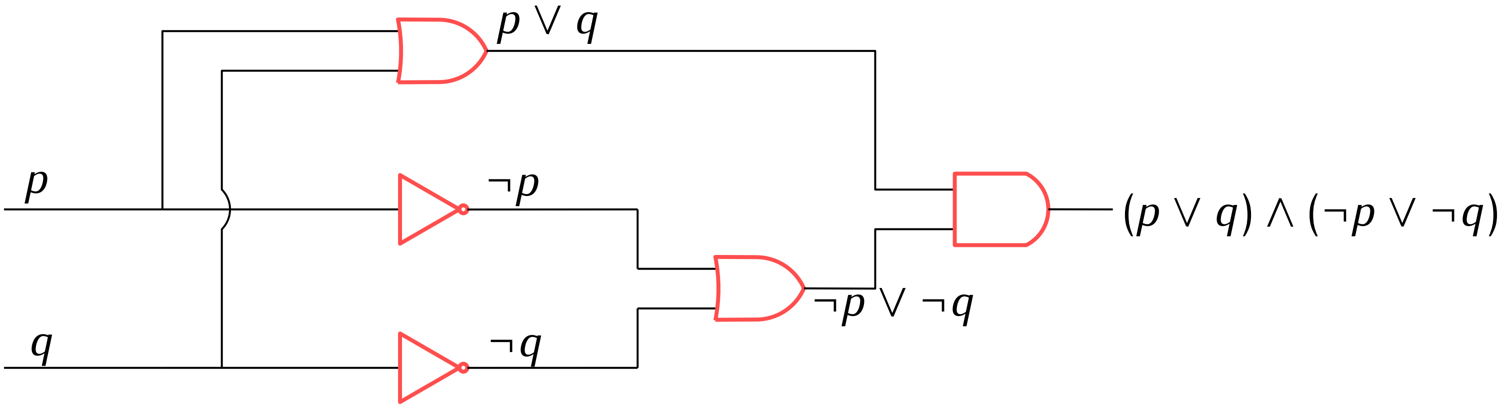


p	q	$\neg p$	$\neg q$	$p \lor q$	$\neg p \lor \neg q$	$(p \lor q) \land (\neg p \lor \neg q)$
0	0	1				
0	1	1				
1	0	0				
1	1	0				

p	q	$p \wedge q$
0	0	0
0	1	0
1	0	0
1	1	1

p	q	$p \vee q$
0	0	0
0	1	1
1	0	1
1	1	1

p	$\neg p$
0	1
1	0

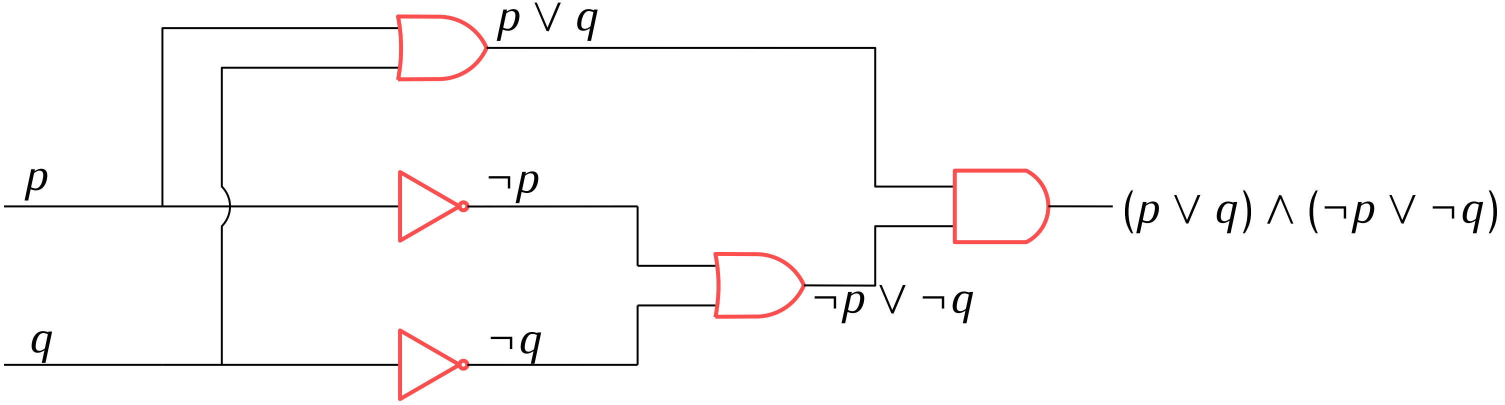


p	q	$\neg p$	$\neg q$	$p \vee q$	$\neg p \vee \neg q$	$(p \vee q) \wedge (\neg p \vee \neg q)$
0	0	1				
0	1	1				
1	0	0				
1	1	0				

p	q	$p \land q$
0	0	0
0	1	0
1	0	0
1	1	1

p	q	$p \lor q$
0	0	0
0	1	1
1	0	1
1	1	1

p	$\neg p$
0	1
1	0

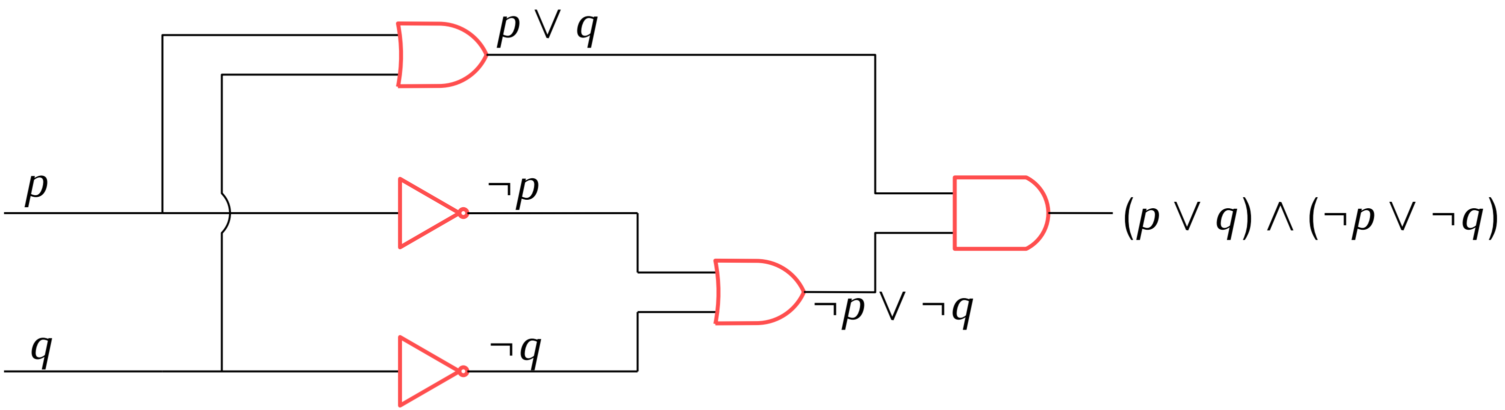


p	q	$\neg p$	$\neg q$	$p \lor q$	$\neg p \lor \neg q$	$(p \lor q) \land (\neg p \lor \neg q)$
0	0	1				
0	1	1				
1	0	0				
1	1	0				

p	q	$p \wedge q$
0	0	0
0	1	0
1	0	0
1	1	1

p	q	$p \vee q$
0	0	0
0	1	1
1	0	1
1	1	1

p	$\neg p$
0	1
1	0

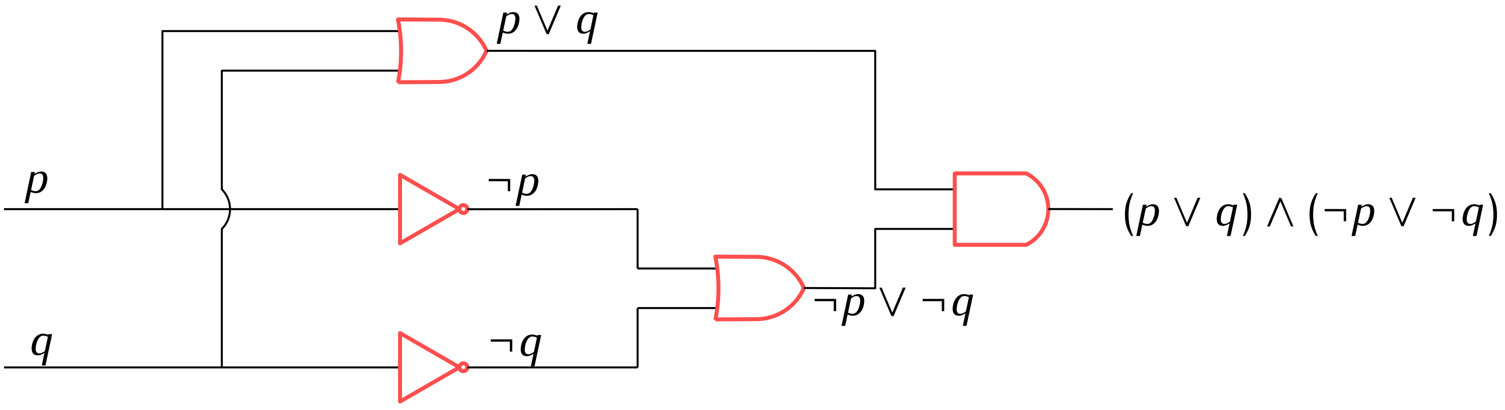


p	q	$\neg p$	$\neg q$	$p \vee q$	$\neg p \vee \neg q$	$(p \vee q) \wedge (\neg p \vee \neg q)$
0	0	1	1			
0	1	1	0			
1	0	0	1			
1	1	0	0			

p	q	$p \wedge q$
0	0	0
0	1	0
1	0	0
1	1	1

p	q	$p \vee q$
0	0	0
0	1	1
1	0	1
1	1	1

p	$\neg p$
0	1
1	0

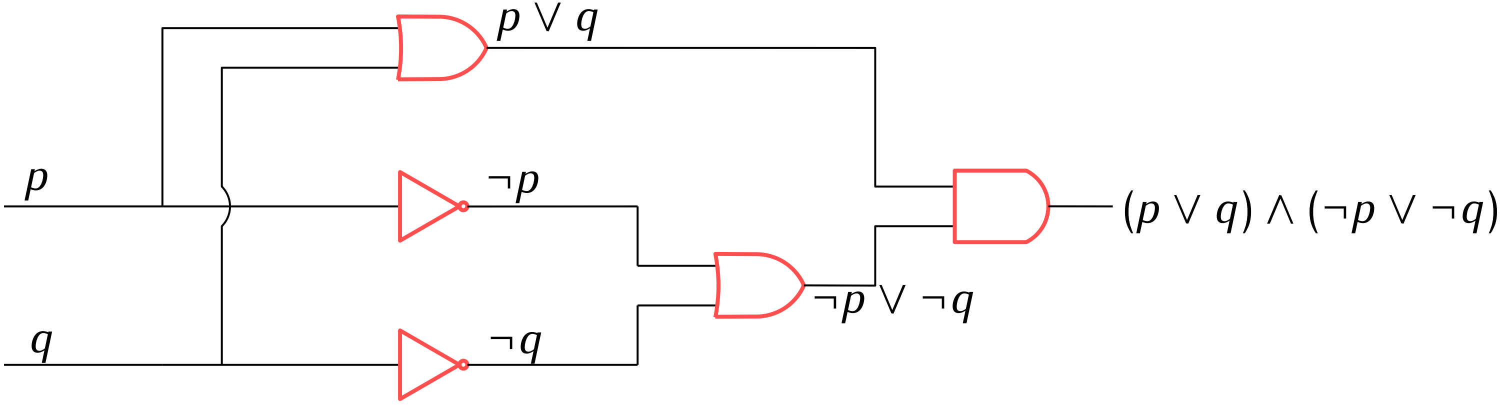


p	q	$\neg p$	$\neg q$	$p \vee q$	$\neg p \vee \neg q$	$(p \vee q) \wedge (\neg p \vee \neg q)$
0	0	1	1	0		
0	1	1	0	1		
1	0	0	1	1		
1	1	0	0	1		

p	q	$p \wedge q$
0	0	0
0	1	0
1	0	0
1	1	1

p	q	$p \vee q$
0	0	0
0	1	1
1	0	1
1	1	1

p	$\neg p$
0	1
1	0

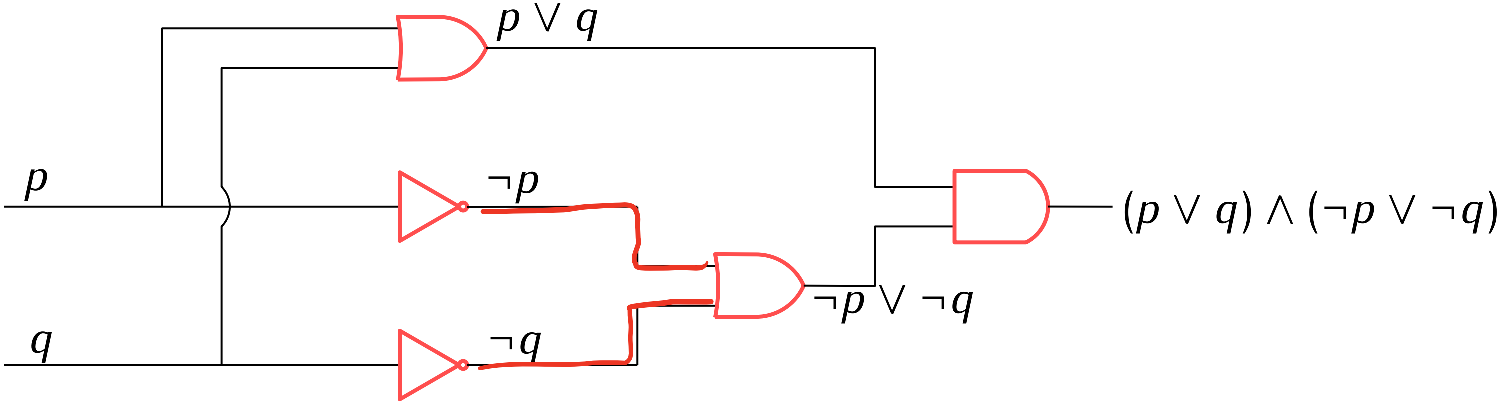


p	q	$\neg p$	$\neg q$	$p \vee q$	$\neg p \vee \neg q$	$(p \vee q) \wedge (\neg p \vee \neg q)$
0	0	1	1	0		
0	1	1	0	1		
1	0	0	1	1		
1	1	0	0	1		

p	q	$p \wedge q$
0	0	0
0	1	0
1	0	0
1	1	1

p	q	$p \vee q$
0	0	0
0	1	1
1	0	1
1	1	1

p	$\neg p$
0	1
1	0

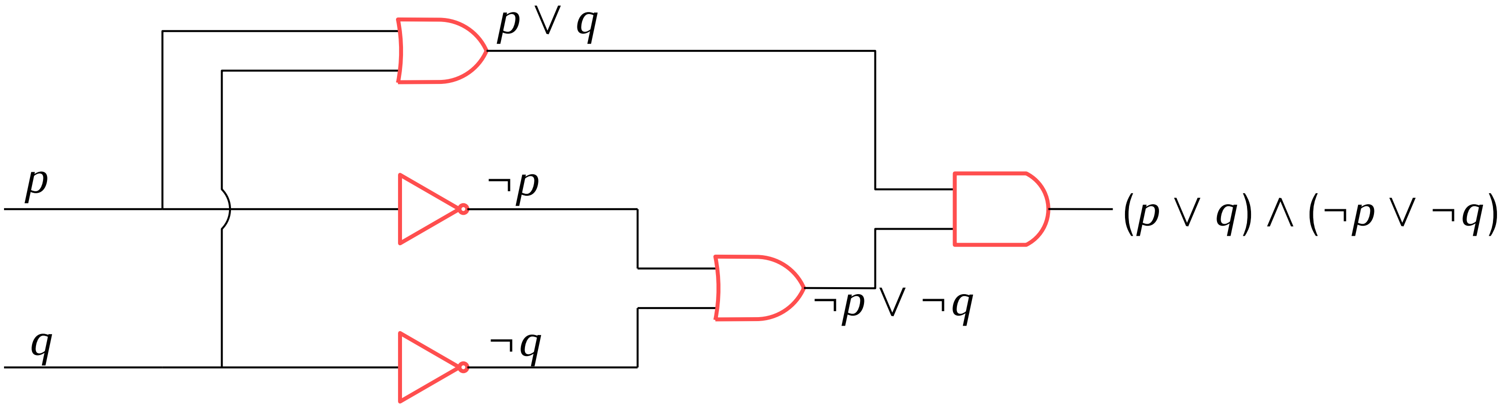


p	q	$\neg p$	$\neg q$	$p \vee q$	$\neg p \vee \neg q$	$(p \vee q) \wedge (\neg p \vee \neg q)$
0	0	1	1	0	1	
0	1	1	0	1	1	
1	0	0	1	1	1	
1	1	0	0	1	0	

p	q	$p \wedge q$
0	0	0
0	1	0
1	0	0
1	1	1

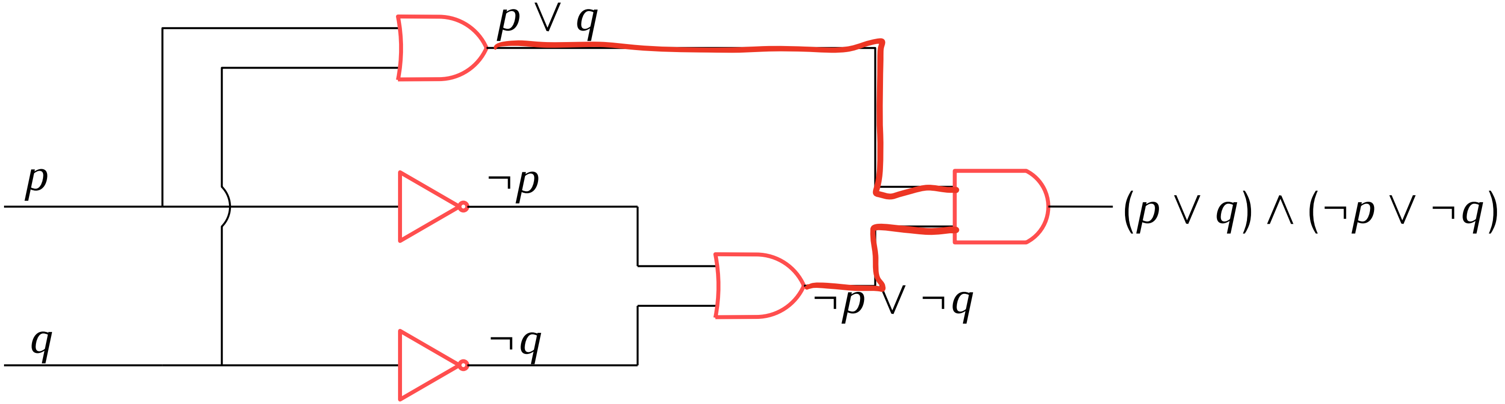
p	q	$p \vee q$
0	0	0
0	1	1
1	0	1
1	1	1

p	$\neg p$
0	1
1	0



p	q	$\neg p$	$\neg q$	$p \vee q$	$\neg p \vee \neg q$	$(p \vee q) \wedge (\neg p \vee \neg q)$
0	0	1	1	0	1	
0	1	1	0	1	1	
1	0	0	1	1	1	
1	1	0	0	1	0	

p	q	$p \wedge q$
0	0	0
0	1	0
1	0	0
1	1	1



p	q	$p \vee q$
0	0	0
0	1	1
1	0	1
1	1	1

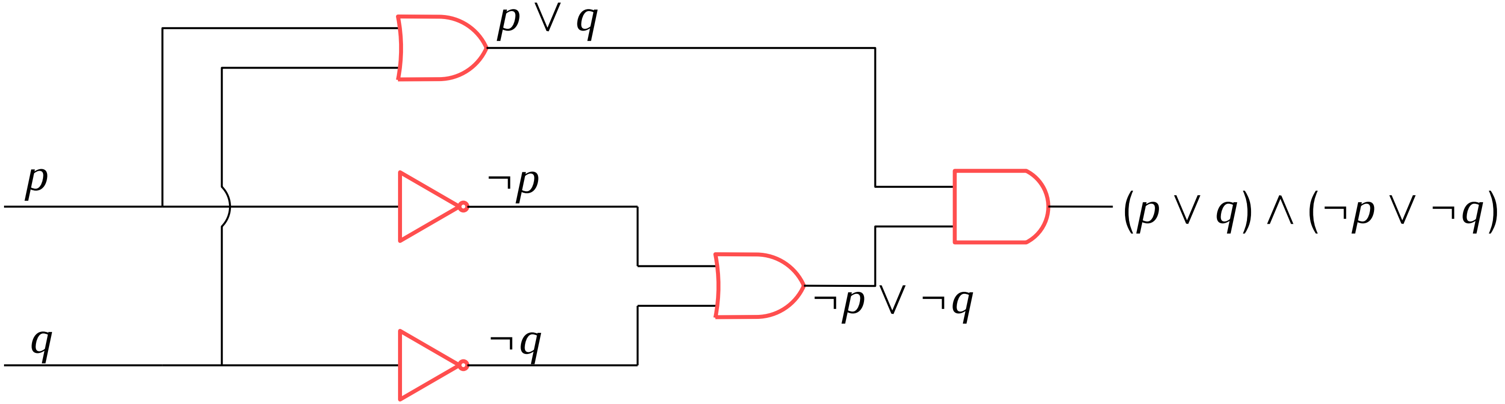
p	$\neg p$
0	1
1	0

p	q	$\neg p$	$\neg q$	$p \vee q$	$\neg p \vee \neg q$	$(p \vee q) \wedge (\neg p \vee \neg q)$
0	0	1	1	0	1	0
0	1	1	0	1	1	1
1	0	0	1	1	1	1
1	1	0	0	1	0	0

p	q	$p \land q$
0	0	0
0	1	0
1	0	0
1	1	1

p	q	$p \lor q$
0	0	0
0	1	1
1	0	1
1	1	1

p	$\neg p$
0	1
1	0

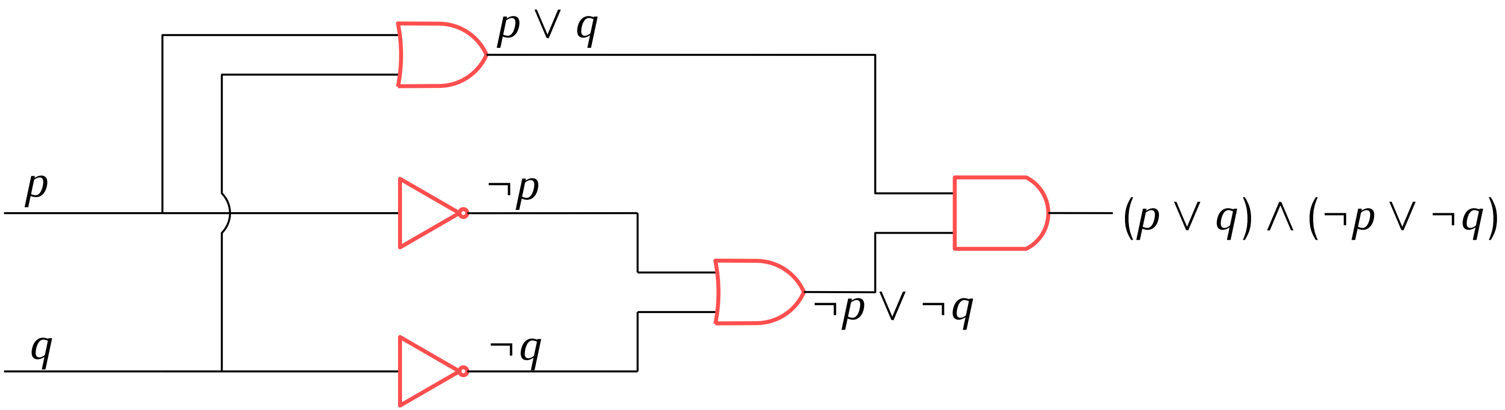


p	q	$\neg p$	$\neg q$	$p \lor q$	$\neg p \lor \neg q$	$(p \lor q) \land (\neg p \lor \neg q)$
0	0	1	1	0	1	0
0	1	1	0	1	1	1
1	0	0	1	1	1	1
1	1	0	0	1	0	0

p	q	$p \wedge q$
0	0	0
0	1	0
1	0	0
1	1	1

p	q	$p \vee q$
0	0	0
0	1	1
1	0	1
1	1	1

p	$\neg p$
0	1
1	0



p	q	$\neg p$	$\neg q$	$p \vee q$	$\neg p \vee \neg q$	$(p \vee q) \wedge (\neg p \vee \neg q)$
0	0	1	1	0	1	0
0	1	1	0	1	1	1
1	0	0	1	1	1	1
1	1	0	0	1	0	0

$\top$ $\boxed{1}$ $\bot$ $\boxed{0}$

Definition (Propositional formulas)**.** The following are the only legal formulas:

1. every variable $p, q, r, \ldots$ is a formula
2. $\top$ and $\bot$ are formulas, (TRUE and FALSE)
3. If ϕ and ψ are formulas, then $\phi \wedge \psi$ is a formula, (AND)
4. If If ϕ and ψ are formulas, then $\phi \vee \psi$ is a formula, (OR)
5. If ϕ and ψ are formulas, then $\phi \Rightarrow \psi$ is a formula, (IMPLIES)
6. If ϕ is a formula, then $\neg\phi$ is a formula. (NOT)

no truth table defined yet!

Definition (Propositional formulas)**.** The following are the only legal formulas:

1. every variable $p, q, r, \ldots$ is a formula
2. $\top$ and $\bot$ are formulas, (TRUE and FALSE)
3. If ϕ and ψ are formulas, then $\phi \wedge \psi$ is a formula, (AND)
4. If If ϕ and ψ are formulas, then $\phi \vee \psi$ is a formula, (OR)
5. If ϕ and ψ are formulas, then $\phi \Rightarrow \psi$ is a formula, (IMPLIES)
6. If ϕ is a formula, then $\neg\phi$ is a formula. (NOT)

no truth table defined yet!

p	q	$p \Rightarrow q$
0	0	1
0	1	1
1	0	0
1	1	1

Definition (Propositional formulas)**.** The following are the only legal formulas:

1. every variable $p, q, r, \ldots$ is a formula
2. $\top$ and $\bot$ are formulas, (TRUE and FALSE)
3. If ϕ and ψ are formulas, then $\phi \wedge \psi$ is a formula, (AND)
4. If If ϕ and ψ are formulas, then $\phi \vee \psi$ is a formula, (OR)
5. If ϕ and ψ are formulas, then $\phi \Rightarrow \psi$ is a formula, (IMPLIES)
6. If ϕ is a formula, then $\neg\phi$ is a formula. (NOT)

no truth table defined yet!

p	q	$p \Rightarrow q$
0	0	1
0	1	1
1	0	0
1	1	1

- "p implies q" means "whenever p is true, then q is true"

Definition (Propositional formulas)**.** The following are the only legal formulas:

1. every variable $p, q, r, \dots$ is a formula
2. $\top$ and $\bot$ are formulas, (TRUE and FALSE)
3. If ϕ and ψ are formulas, then $\phi \wedge \psi$ is a formula, (AND)
4. If If ϕ and ψ are formulas, then $\phi \vee \psi$ is a formula, (OR)
5. If ϕ and ψ are formulas, then $\phi \Rightarrow \psi$ is a formula, (IMPLIES)
6. If ϕ is a formula, then $\neg\phi$ is a formula. (NOT)

no truth table defined yet!

p	q	$p \Rightarrow q$
0	0	1
0	1	1
1	0	0
1	1	1

- "p implies q" means "whenever p is true, then q is true"
- We also say "If p then q".

Definition (Propositional formulas). The following are the only legal formulas:

1. every variable $p, q, r, \ldots$ is a formula
2. $\top$ and $\bot$ are formulas, (TRUE and FALSE)
3. If ϕ and ψ are formulas, then $\phi \land \psi$ is a formula, (AND)
4. If If ϕ and ψ are formulas, then $\phi \lor \psi$ is a formula, (OR)
5. If ϕ and ψ are formulas, then $\phi \Rightarrow \psi$ is a formula, (IMPLIES)
6. If ϕ is a formula, then $\neg\phi$ is a formula. (NOT)

no truth table defined yet!

p	q	$p \Rightarrow q$
0	0	1
0	1	1
1	0	0
1	1	1

- "p implies q" means "whenever p is true, then q is true"
- We also say "If p then q".
- This is wrong only when p is true and q is false

Definition (Propositional formulas)**.** The following are the only legal formulas:

1. every variable $p, q, r, \ldots$ is a formula
2. $\top$ and $\bot$ are formulas, (TRUE and FALSE)
3. If ϕ and ψ are formulas, then $\phi \wedge \psi$ is a formula, (AND)
4. If If ϕ and ψ are formulas, then $\phi \vee \psi$ is a formula, (OR)
5. If ϕ and ψ are formulas, then $\phi \Rightarrow \psi$ is a formula, (IMPLIES)
6. If ϕ is a formula, then $\neg\phi$ is a formula. (NOT)

no truth table defined yet!

p	q	$p \Rightarrow q$
0	0	1
0	1	1
1	0	0
1	1	1

- "p implies q" means "whenever p is true, then q is true"
- We also say "If p then q".
- This is wrong only when p is true and q is false

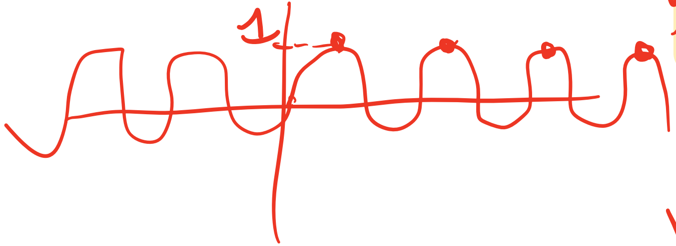
Which of these statements are true?

- ✓ If cats can fly, the Earth is flat.
- ✓ If $0 = 1$, then cos is injective.
- ✗ If $1 = 1$, then sin is injective.

p true

q ?

✓ If cats are mammals, then the sun looks yellow.



Definition. Let φ be a formula. A satisfying assigment for φ is a way to evaluate the variables/input so that φ becomes true.

Definition. Let φ be a formula. A satisfying assigment for φ is a way to evaluate the variables/input so that φ becomes true.

Satisfying assignment "=" row in truth table that finishes with 1

Definition. Let φ be a formula. A satisfying assigment for φ is a way to evaluate the variables/input so that φ becomes true.

Satisfying assignment "=" row in truth table that finishes with 1

satisfying assignments for $(p \vee q) \wedge (\neg p \vee \neg q)$

$\{(0,1),(1,0)\}$

p	q	$\neg p$	$\neg q$	$p \vee q$	$\neg p \vee \neg q$	$(p \vee q) \wedge (\neg p \vee \neg q)$
0	0	1	1	0	1	0
0	1	1	0	1	1	1
1	0	0	1	1	1	1
1	1	0	0	1	0	0

Definition. Let φ be a formula. A satisfying assigment for φ is a way to evaluate the variables/input so that φ becomes true.

Satisfying assignment "=" row in truth table that finishes with 1

satisfying assignments for $(p \vee q) \wedge (\neg p \vee \neg q)$

$\{(0,1),(1,0)\}$

p	q	$\neg p$	$\neg q$	$p \vee q$	$\neg p \vee \neg q$	$(p \vee q) \wedge (\neg p \vee \neg q)$
0	0	1	1	0	1	0
0	1	1	0	1	1	1
1	0	0	1	1	1	1
1	1	0	0	1	0	0

To find the satisfying assignments of a formula: no better way than building the truth table.

Definition. Let φ be a formula. A satisfying assigment for φ is a way to evaluate the variables/input so that φ becomes true.

Satisfying assignment "=" row in truth table that finishes with 1

satisfying assignments for $(p \vee q) \wedge (\neg p \vee \neg q)$

$\{(0,1),(1,0)\}$

p	q	$\neg p$	$\neg q$	$p \vee q$	$\neg p \vee \neg q$	$(p \vee q) \wedge (\neg p \vee \neg q)$
0	0	1	1	0	1	0
0	1	1	0	1	1	1
1	0	0	1	1	1	1
1	1	0	0	1	0	0

To find the satisfying assignments of a formula: no better way than building the truth table.
Problem with a $1'000'000 reward: find a faster method to even find one satisfying assignment.

Definition. Let φ be a formula. A satisfying assigment for φ is a way to evaluate the variables/input so that φ becomes true.

Satisfying assignment "=" row in truth table that finishes with 1

satisfying assignments for $(p \vee q) \wedge (\neg p \vee \neg q)$

$\{(0,1),(1,0)\}$

p	q	$\neg p$	$\neg q$	$p \vee q$	$\neg p \vee \neg q$	$(p \vee q) \wedge (\neg p \vee \neg q)$
0	0	1	1	0	1	0
0	1	1	0	1	1	1
1	0	0	1	1	1	1
1	1	0	0	1	0	0

To find the satisfying assignments of a formula: no better way than building the truth table.
Problem with a \$1'000'000 reward: find a faster method to even find one satisfying assignment.

Definition. Two formulas φ and ψ are logically equivalent if they have **exactly** the same satisfying assignments.

We write: $\varphi \equiv \psi$

p	p
0	0
1	1

p	$\neg p$	$\neg\neg p$
0	1	0
1	0	1

$p \equiv \neg\neg p$

Definition. Let φ be a formula. A satisfying assigment for φ is a way to evaluate the variables/input so that φ becomes true.

Satisfying assignment "=" row in truth table that finishes with 1

satisfying assignments for $(p \vee q) \wedge (\neg p \vee \neg q)$

$\{(0,1),(1,0)\}$

p	q	$\neg p$	$\neg q$	$p \vee q$	$\neg p \vee \neg q$	$(p \vee q) \wedge (\neg p \vee \neg q)$
0	0	1	1	0	1	0
0	1	1	0	1	1	1
1	0	0	1	1	1	1
1	1	0	0	1	0	0

To find the satisfying assignments of a formula: no better way than building the truth table.
Problem with a \$1'000'000 reward: find a faster method to even find one satisfying assignment.

Definition. Two formulas φ and ψ are logically equivalent if they have **exactly** the same satisfying assignments.

We write: $\varphi \equiv \psi$

$5 \times (3+2) = 5 \times 3 + 5 \times 2$

$(5+3)+2$

Standard equivalences to know (some proofs in HÜ):

$\varphi \wedge (\psi \vee \theta) \equiv (\varphi \wedge \psi) \vee (\varphi \wedge \theta)$ $\varphi \wedge (\psi \wedge \theta) \equiv (\varphi \wedge \psi) \wedge \theta$ $\varphi \wedge \top \equiv \varphi$

$(\varphi \vee (\psi \wedge \theta) \equiv (\varphi \vee \psi) \wedge (\varphi \vee \theta))$ $\varphi \vee (\psi \vee \theta) \equiv (\varphi \vee \psi) \vee \theta$ $\varphi \vee \bot \equiv \varphi$

Distributivity laws   Associativity laws   Identity laws

Theorem. The following formulas are logically equivalent:

$$\left.\begin{aligned} \neg\neg\varphi &\equiv \varphi \\ \neg(\varphi \wedge \psi) &\equiv \neg\varphi \vee \neg\psi \\ \neg(\varphi \vee \psi) &\equiv \neg\varphi \wedge \neg\psi \end{aligned}\right\}\text{De Morgan's rules}$$

Theorem. The following formulas are logically equivalent:

$$\left.\begin{aligned} \neg\neg\varphi &\equiv \varphi \\ \neg(\varphi \wedge \psi) &\equiv \neg\varphi \vee \neg\psi \\ \neg(\varphi \vee \psi) &\equiv \neg\varphi \wedge \neg\psi \end{aligned}\right\}\text{De Morgan's rules}$$

φ	$\neg\varphi$	$\neg\neg\varphi$
0	1	0
1	0	1

Theorem. The following formulas are logically equivalent:

$$\left.\begin{aligned}\neg\neg\varphi &\equiv \varphi\\ \neg(\varphi\land\psi) &\equiv \neg\varphi\lor\neg\psi\\ \neg(\varphi\lor\psi) &\equiv \neg\varphi\land\neg\psi\end{aligned}\right\}\text{De Morgan's rules}$$

φ	$\neg\varphi$	$\neg\neg\varphi$
0	1	0
1	0	1

φ	ψ	$\neg\varphi$	$\neg\psi$	$\neg\varphi\lor\neg\psi$ $\equiv$	$\neg(\varphi\land\psi)$	$\varphi\land\psi$
0	0	1	1	1	1	0
0	1	1	0	1	1	0
1	0	0	1	1	1	0
1	1	0	0	0	0	1

Theorem. The following formulas are logically equivalent:

$$\left.\begin{array}{r}\neg\neg\varphi \equiv \varphi \\ \neg(\varphi \wedge \psi) \equiv \neg\varphi \vee \neg\psi \\ \neg(\varphi \vee \psi) \equiv \neg\varphi \wedge \neg\psi\end{array}\right\}\text{De Morgan's rules}$$

φ	$\neg\varphi$	$\neg\neg\varphi$
0	1	0
1	0	1

φ	ψ	$\neg\varphi$	$\neg\psi$	$\neg\varphi \vee \neg\psi$	$\neg(\varphi \wedge \psi)$
0	0	1	1	1	1
0	1	1	0	1	1
1	0	0	1	1	1
1	1	0	0	0	0

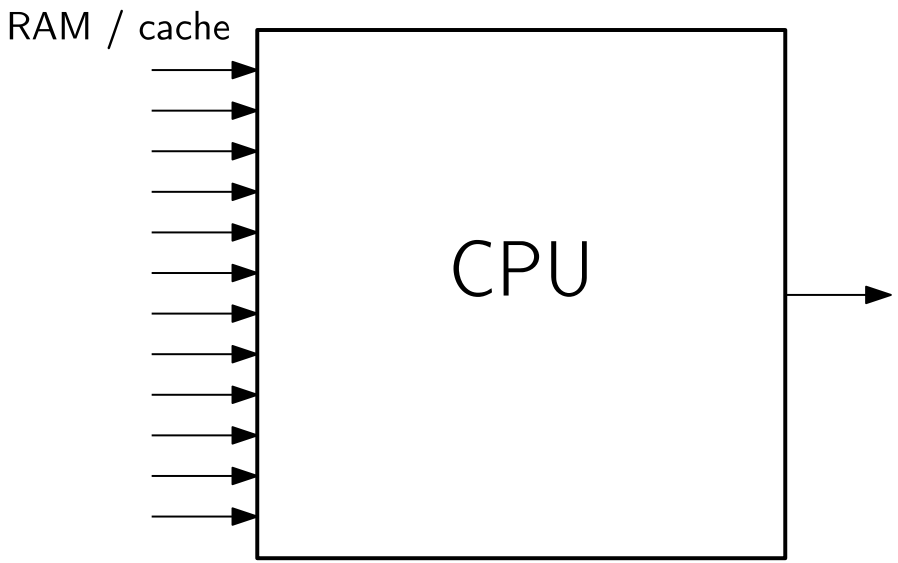
φ	ψ	$\neg\varphi$	$\neg\psi$	$\neg\varphi \wedge \neg\psi$	$\neg(\varphi \vee \psi)$
0	0	1	1	1	1
0	1	1	0	0	0
1	0	0	1	0	0
1	1	0	0	0	0

- We have seen how to compute a truth table, given any formula

- We have seen how to compute a truth table, given any formula
- Can one do the reverse? “Given a truth table, compute a formula”

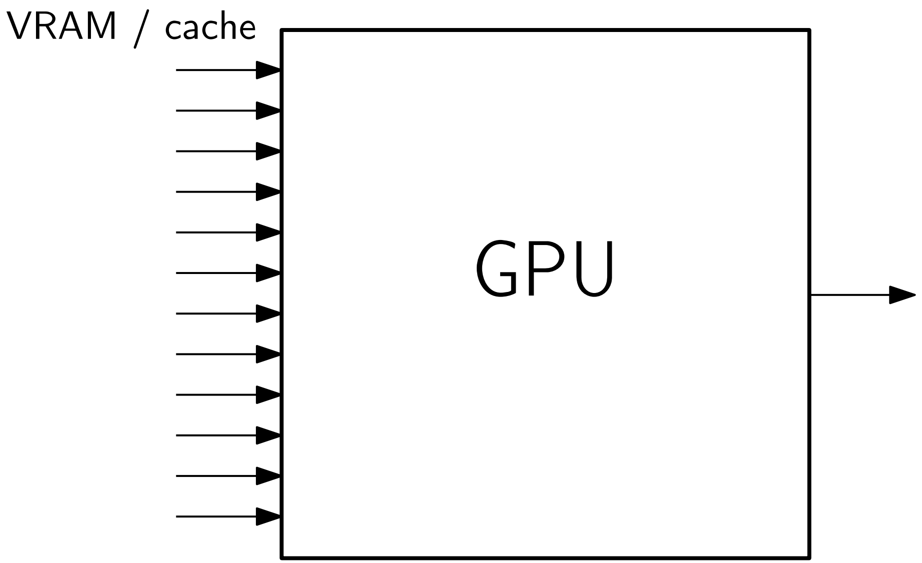
- We have seen how to compute a truth table, given any formula
- Can one do the reverse? "Given a truth table, compute a formula"

Concrete application: modelize the behavior of any digital system using logic/electronic circuits



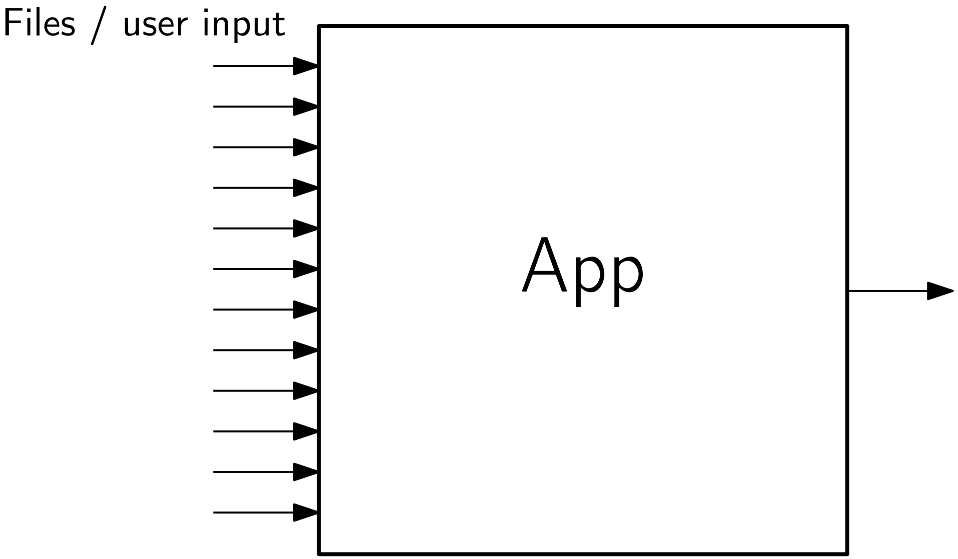
- We have seen how to compute a truth table, given any formula
- Can one do the reverse? "Given a truth table, compute a formula"

Concrete application: modelize the behavior of any digital system using logic/electronic circuits



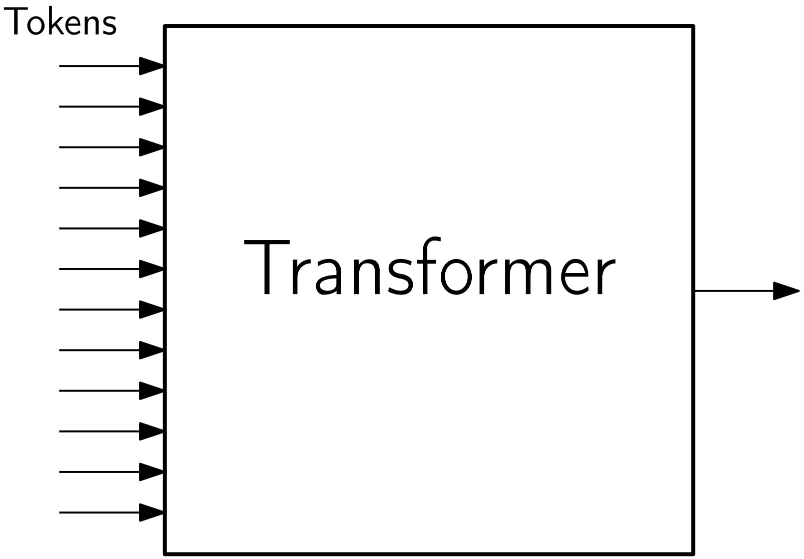
- We have seen how to compute a truth table, given any formula
- Can one do the reverse? "Given a truth table, compute a formula"

Concrete application: modelize the behavior of any digital system using logic/electronic circuits



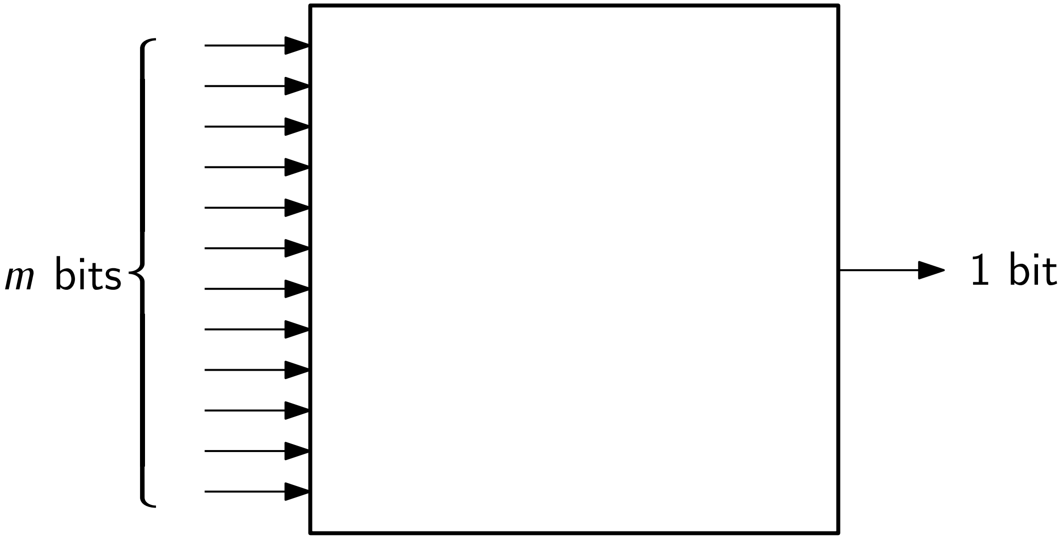
- We have seen how to compute a truth table, given any formula
- Can one do the reverse? "Given a truth table, compute a formula"

Concrete application: modelize the behavior of any digital system using logic/electronic circuits



- We have seen how to compute a truth table, given any formula
- Can one do the reverse? "Given a truth table, compute a formula"

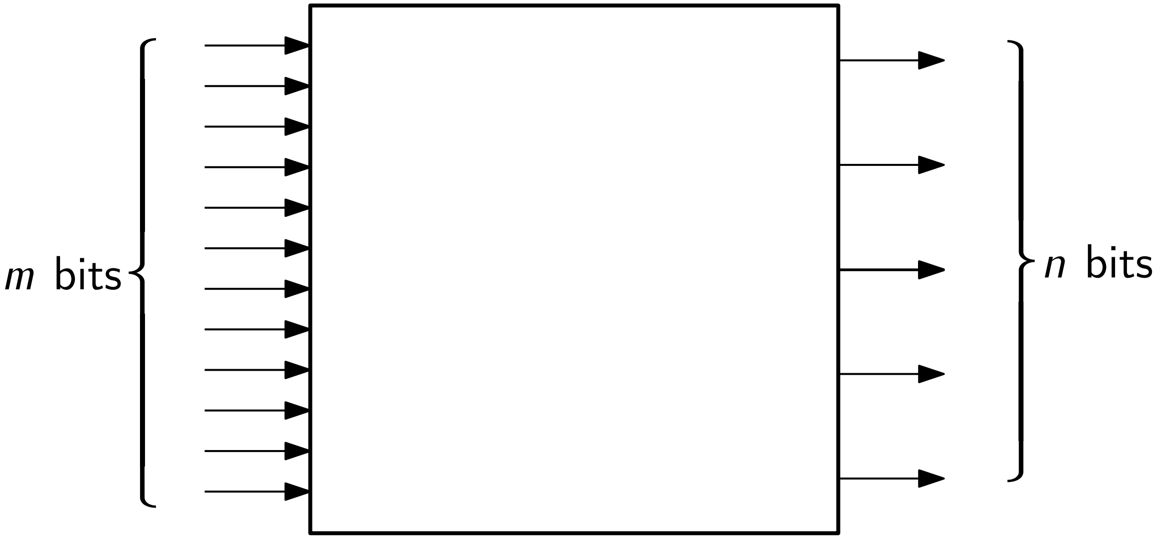
Concrete application: modelize the behavior of any digital system using logic/electronic circuits



Function $\{0,1\}^m \to \{0,1\}$

- We have seen how to compute a truth table, given any formula
- Can one do the reverse? "Given a truth table, compute a formula"

Concrete application: modelize the behavior of any digital system using logic/electronic circuits



Function $\{0,1\}^m \to \{0,1\}^n$

- We have seen how to compute a truth table, given any formula
- Can one do the reverse? "Given a truth table, compute a formula"

Concrete application: modelize the behavior of any digital system using logic/electronic circuits

p_1	p_2	p_3	p_4	p_5	p_6	?
0	0	0	0	0	0	$out_{(0,0,0,0,0,0)}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
b_1	b_2	b_3	b_4	b_5	b_6	$out_{(b_1,b_2,b_3,b_4,b_5,b_6)}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
1	1	1	1	1	1	$out_{(1,1,1,1,1,1)}$

- We have seen how to compute a truth table, given any formula
- Can one do the reverse? "Given a truth table, compute a formula"

Concrete application: modelize the behavior of any digital system using logic/electronic circuits

p_1	p_2	p_3	p_4	p_5	p_6	?
0	0	0	0	0	0	$out_{(0,0,0,0,0,0)}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
b_1	b_2	b_3	b_4	b_5	b_6	$out_{(b_1,b_2,b_3,b_4,b_5,b_6)}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
1	1	1	1	1	1	$out_{(1,1,1,1,1,1)}$

Procedure:

- Make a list L of all satisfying assignments $(b_1, \ldots, b_n)$

- We have seen how to compute a truth table, given any formula
- Can one do the reverse? "Given a truth table, compute a formula"

Concrete application: modelize the behavior of any digital system using logic/electronic circuits

p_1	p_2	p_3	p_4	p_5	p_6	?
0	0	0	0	0	0	$out_{(0,0,0,0,0,0)}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
b_1	b_2	b_3	b_4	b_5	b_6	$out_{(b_1,b_2,b_3,b_4,b_5,b_6)}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
1	1	1	1	1	1	$out_{(1,1,1,1,1,1)}$

Procedure:

- Make a list L of all satisfying assignments $(b_1, \ldots, b_n)$
- $L \subseteq \{0,1\}^n$

- We have seen how to compute a truth table, given any formula
- Can one do the reverse? "Given a truth table, compute a formula"

Concrete application: modelize the behavior of any digital system using logic/electronic circuits

p_1	p_2	p_3	p_4	p_5	p_6	?
0	0	0	0	0	0	$out_{(0,0,0,0,0,0)}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
b_1	b_2	b_3	b_4	b_5	b_6	$out_{(b_1,b_2,b_3,b_4,b_5,b_6)}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
1	1	1	1	1	1	$out_{(1,1,1,1,1,1)}$

Procedure:

- Make a list L of all satisfying assignments $(b_1, \ldots, b_n)$
- $L \subseteq \{0,1\}^n$
- For each $(b_1, \ldots, b_n) \in L$, define $\psi_{(b_1,\ldots,b_n)}$ by

$$\bigwedge_{i \in \{1,\ldots,n\}: b_i = 1} p_i \wedge \bigwedge_{i \in \{1,\ldots,n\}: b_i = 0} \neg p_i$$

- We have seen how to compute a truth table, given any formula
- Can one do the reverse? "Given a truth table, compute a formula"

Concrete application: modelize the behavior of any digital system using logic/electronic circuits

p_1	p_2	p_3	p_4	p_5	p_6	?
0	0	0	0	0	0	$out_{(0,0,0,0,0,0)}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
b_1	b_2	b_3	b_4	b_5	b_6	$out_{(b_1,b_2,b_3,b_4,b_5,b_6)}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
1	1	1	1	1	1	$out_{(1,1,1,1,1,1)}$

Procedure:

- Make a list L of all satisfying assignments $(b_1, \ldots, b_n)$
- $L \subseteq \{0,1\}^n$
- For each $(b_1, \ldots, b_n) \in L$, define $\psi_{(b_1,\ldots,b_n)}$ by

$$\bigwedge_{i \in \{1,\ldots,n\} : b_i = 1} p_i \wedge \bigwedge_{i \in \{1,\ldots,n\} : b_i = 0} \neg p_i$$

- φ is the formula

$$\bigvee_{(b_1,\ldots,b_n) \in L} \psi_{(b_1,\ldots,b_n)}$$

- We have seen how to compute a truth table, given any formula
- Can one do the reverse? "Given a truth table, compute a formula"

Concrete application: modelize the behavior of any digital system using logic/electronic circuits

p_1	p_2	p_3	?
0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	1

Procedure:

- Make a list L of all satisfying assignments $(b_1, \ldots, b_n)$
- $L \subseteq \{0, 1\}^n$
- For each $(b_1, \ldots, b_n) \in L$, define $\psi_{(b_1,\ldots,b_n)}$ by

$$\bigwedge_{i \in \{1,\ldots,n\}: b_i = 1} p_i \wedge \bigwedge_{i \in \{1,\ldots,n\}: b_i = 0} \neg p_i$$

- φ is the formula

$$\bigvee_{(b_1,\ldots,b_n) \in L} \psi_{(b_1,\ldots,b_n)}$$

- We have seen how to compute a truth table, given any formula
- Can one do the reverse? "Given a truth table, compute a formula"

Concrete application: modelize the behavior of any digital system using logic/electronic circuits

p_1	p_2	p_3	?
0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	1

Procedure:

- Make a list L of all satisfying assignments $(b_1, \ldots, b_n)$
- $L \subseteq \{0, 1\}^n$
- For each $(b_1, \ldots, b_n) \in L$, define $\psi_{(b_1,\ldots,b_n)}$ by

$$\bigwedge_{i \in \{1,\ldots,n\} : b_i = 1} p_i \wedge \bigwedge_{i \in \{1,\ldots,n\} : b_i = 0} \neg p_i$$

- φ is the formula

$$\bigvee_{(b_1,\ldots,b_n) \in L} \psi_{(b_1,\ldots,b_n)}$$

- We have seen how to compute a truth table, given any formula
- Can one do the reverse? "Given a truth table, compute a formula"

Concrete application: modelize the behavior of any digital system using logic/electronic circuits

p_1	p_2	p_3	?
0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	1

$(\neg p_1 \wedge \neg p_2 \wedge p_3)$

Procedure:

- Make a list L of all satisfying assignments $(b_1, \ldots, b_n)$
- $L \subseteq \{0,1\}^n$
- For each $(b_1, \ldots, b_n) \in L$, define $\psi_{(b_1,\ldots,b_n)}$ by

$$\bigwedge_{i \in \{1,\ldots,n\} : b_i = 1} p_i \wedge \bigwedge_{i \in \{1,\ldots,n\} : b_i = 0} \neg p_i$$

- φ is the formula

$$\bigvee_{(b_1,\ldots,b_n) \in L} \psi_{(b_1,\ldots,b_n)}$$

- We have seen how to compute a truth table, given any formula
- Can one do the reverse? "Given a truth table, compute a formula"

Concrete application: modelize the behavior of any digital system using logic/electronic circuits

p_1	p_2	p_3	?
0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	1

$(\neg p_1 \wedge \neg p_2 \wedge p_3)$

$(\neg p_1 \wedge p_2 \wedge \neg p_3)$

$(p_1 \wedge \neg p_2 \wedge \neg p_3)$

Procedure:

- Make a list L of all satisfying assignments $(b_1, \ldots, b_n)$
- $L \subseteq \{0,1\}^n$
- For each $(b_1, \ldots, b_n) \in L$, define $\psi_{(b_1,\ldots,b_n)}$ by

$$\bigwedge_{i \in \{1,\ldots,n\} : b_i = 1} p_i \wedge \bigwedge_{i \in \{1,\ldots,n\} : b_i = 0} \neg p_i$$

- φ is the formula

$$\bigvee_{(b_1,\ldots,b_n) \in L} \psi_{(b_1,\ldots,b_n)}$$

Computing a formula from its satisfying assignments

- We have seen how to compute a truth table, given any formula
- Can one do the reverse? "Given a truth table, compute a formula"

Concrete application: modelize the behavior of any digital system using logic/electronic circuits

p_1	p_2	p_3	?	
0	0	0	0	
0	0	1	1	$(\neg p_1 \land \neg p_2 \land p_3)$
0	1	0	1	$(\neg p_1 \land p_2 \land \neg p_3)$
0	1	1	0	
1	0	0	1	$(p_1 \land \neg p_2 \land \neg p_3)$
1	0	1	0	
1	1	0	0	
1	1	1	1	$(p_1 \land \cancel{\neg} p_2 \land \cancel{\neg} p_3)$

Procedure:

- Make a list L of all satisfying assignments $(b_1, \ldots, b_n)$
- $L \subseteq \{0,1\}^n$
- For each $(b_1, \ldots, b_n) \in L$, define $\psi_{(b_1,\ldots,b_n)}$ by

$$\bigwedge_{i\in\{1,\ldots,n\}:b_i=1} p_i \land \bigwedge_{i\in\{1,\ldots,n\}:b_i=0} \neg p_i$$

- φ is the formula

$$\bigvee_{(b_1,\ldots,b_n)\in L} \psi_{(b_1,\ldots,b_n)}$$

- We have seen how to compute a truth table, given any formula
- Can one do the reverse? "Given a truth table, compute a formula"

Concrete application: modelize the behavior of any digital system using logic/electronic circuits

p_1	p_2	p_3	φ
0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	1

Procedure:

- Make a list L of all satisfying assignments $(b_1, \dots, b_n)$
- $L \subseteq \{0,1\}^n$
- For each $(b_1, \dots, b_n) \in L$, define $\psi_{(b_1,\dots,b_n)}$ by

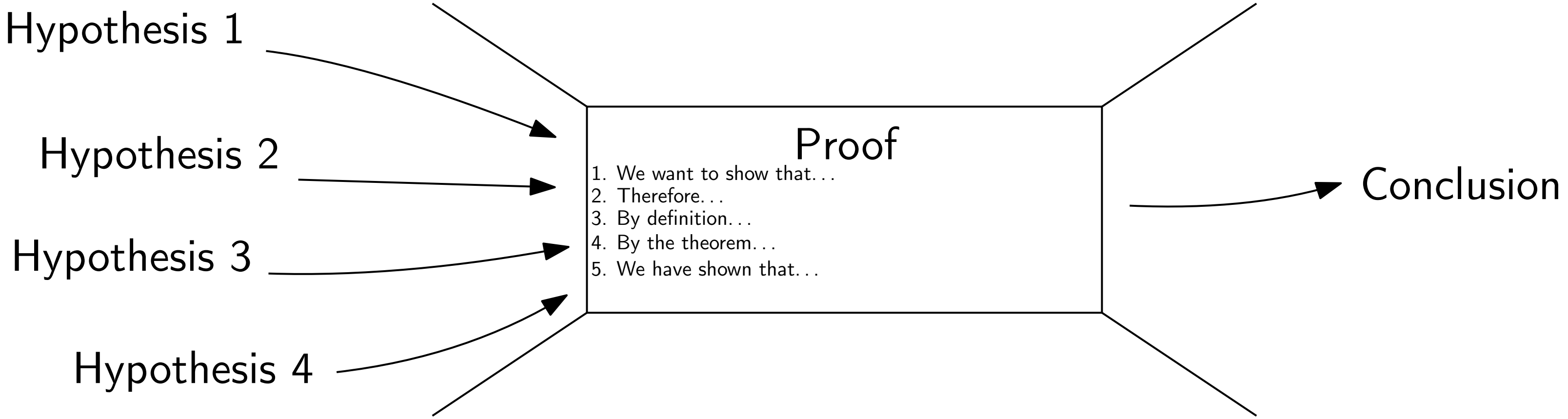
$$\bigwedge_{i \in \{1,\dots,n\} : b_i = 1} p_i \wedge \bigwedge_{i \in \{1,\dots,n\} : b_i = 0} \neg p_i$$

- φ is the formula

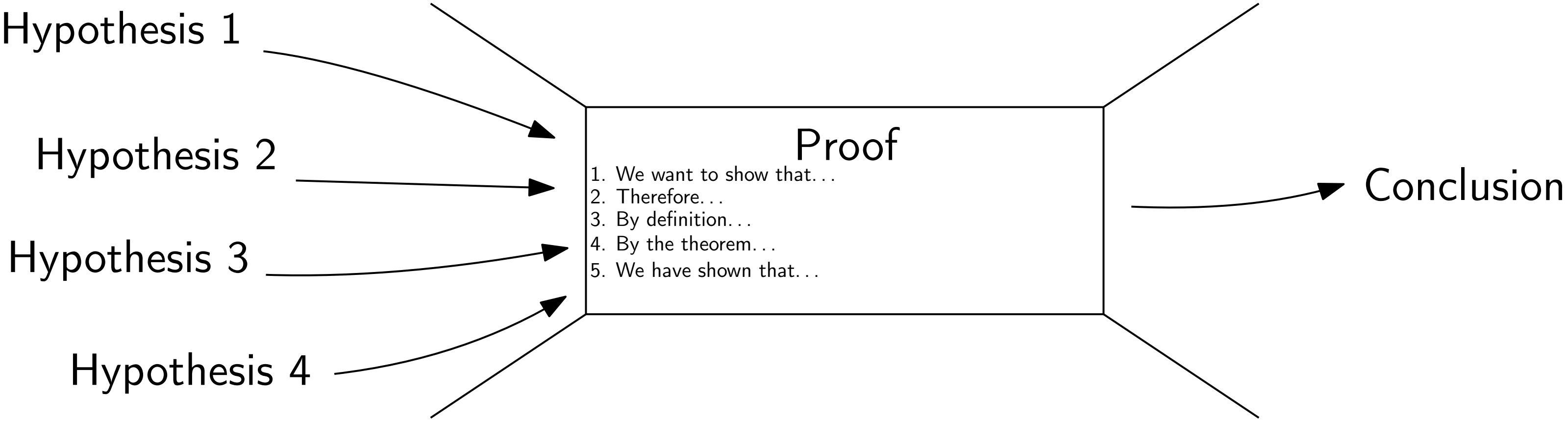
$$\bigvee_{(b_1,\dots,b_n) \in L} \psi_{(b_1,\dots,b_n)}$$

$\varphi : (\neg p_1 \wedge \neg p_2 \wedge p_3) \vee (\neg p_1 \wedge p_2 \wedge \neg p_3) \vee (p_1 \wedge \neg p_2 \wedge \neg p_3) \vee (p_1 \wedge \cancel{\neg} p_2 \wedge \cancel{\neg} p_3)$

Proof methods

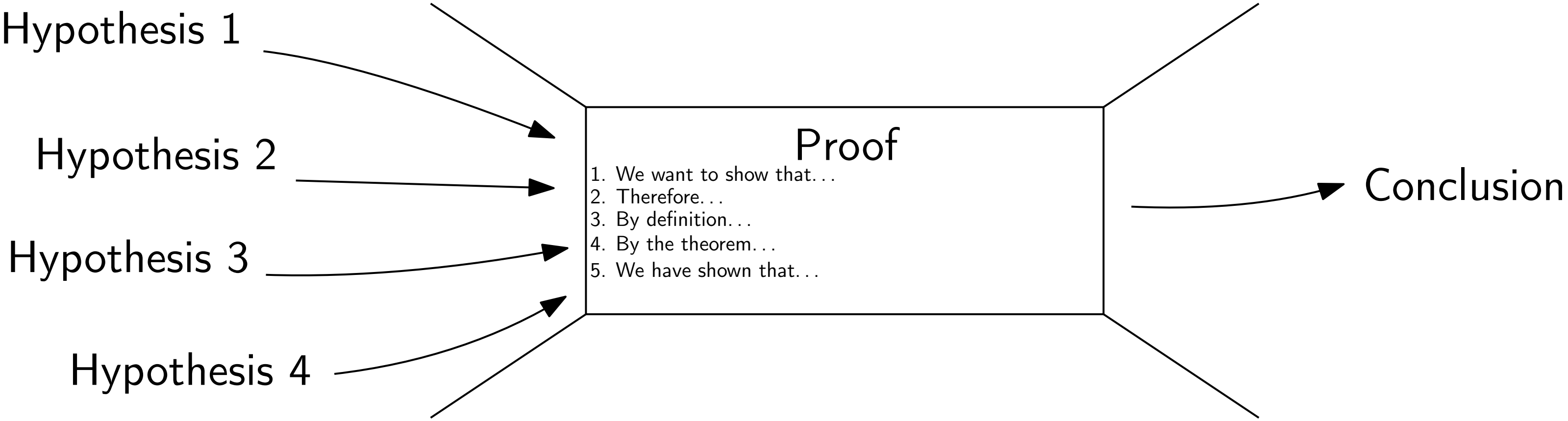


- A proof is a sequence of steps, like a cooking recipe. At each step:
  - Apply a definition
  - Apply a hypothesis
  - Apply a logical rule



- A proof is a sequence of steps, like a cooking recipe. At each step:
  - Apply a definition
  - Apply a hypothesis
  - Apply a logical rule

How to prove that $\varphi \Rightarrow \psi$ is true?

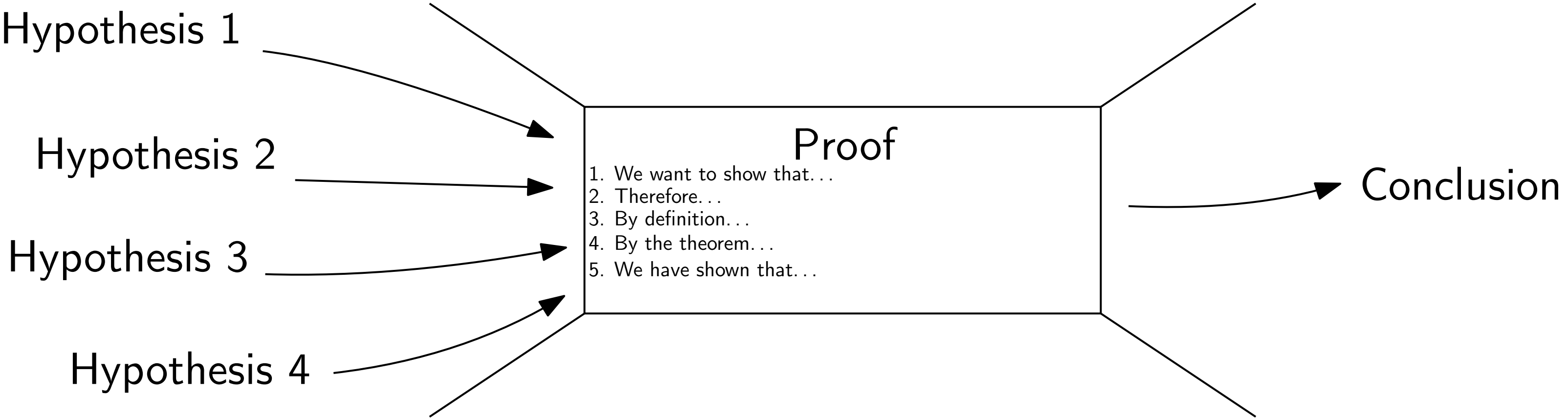


- A proof is a sequence of steps, like a cooking recipe. At each step:
  - Apply a definition
  - Apply a hypothesis
  - Apply a logical rule

How to prove that $\varphi \Rightarrow \psi$ is true?

Direct proof

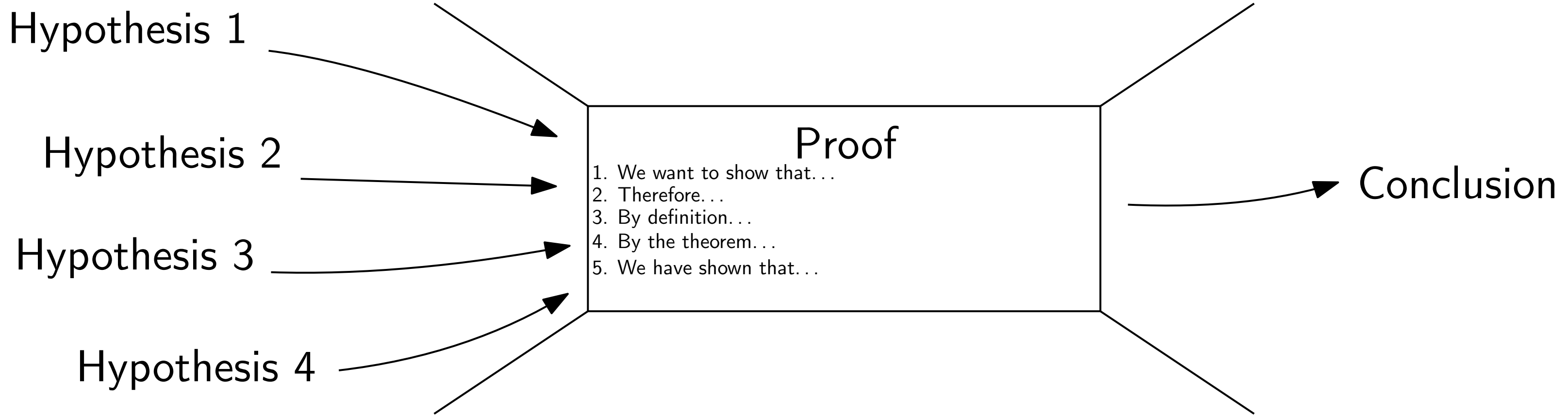
1. Assume that φ is true.
2. <insert rest of the proof>
3. We obtain that ψ is true.



- A proof is a sequence of steps, like a cooking recipe. At each step:
  - Apply a definition
  - Apply a hypothesis
  - Apply a logical rule

How to prove that $\varphi \Rightarrow \psi$ is true?

Direct proof	Proof by contraposition	Proof by contradiction
1. Assume that φ is true. 2. <insert rest of the proof> 3. We obtain that ψ is true.		



- A proof is a sequence of steps, like a cooking recipe. At each step:
  - Apply a definition
  - Apply a hypothesis
  - Apply a logical rule

How to prove that $\varphi \Rightarrow \psi$ is true?

Direct proof
1. Assume that φ is true.
2. <insert rest of the proof>
3. We obtain that ψ is true.

Proof by contraposition
1. Assume that ψ is false.
2. <insert rest of the proof>
3. We obtain that φ is false.

$(\neg \psi) \Rightarrow (\neg \varphi)$

Proof by contradiction

How to prove that $\varphi \Rightarrow \psi$ is true?

Proof by contraposition

1. Assume that ψ is false.
2. <insert rest of the proof>
3. We obtain that φ is false.

How to prove that $\varphi \Rightarrow \psi$ is true?

Proof by contraposition
1. Assume that ψ is false.
2. <insert rest of the proof>
3. We obtain that φ is false.

p	q	$p \Rightarrow q$
0	0	1
0	1	1
1	0	0
1	1	1

How to prove that $\varphi \Rightarrow \psi$ is true?

Proof by contraposition

1. Assume that ψ is false.
2. <insert rest of the proof>
3. We obtain that φ is false.

p	q	$p \Rightarrow q$
0	0	1
0	1	1
1	0	0
1	1	1

p	q	$\neg q$	$\neg p$	$(\neg q) \Rightarrow (\neg p)$
0	0	1	1	1
0	1	0	1	1
1	0	1	0	0
1	1	0	0	1

How to prove that $\varphi \Rightarrow \psi$ is true?

Proof by contraposition
1. Assume that ψ is false.
2. <insert rest of the proof>
3. We obtain that φ is false.

p	q	$p \Rightarrow q$
0	0	1
0	1	1
1	0	0
1	1	1

p	q	$\neg q$	$\neg p$	$(\neg q) \Rightarrow (\neg p)$
0	0	1	1	1
0	1	0	1	1
1	0	1	0	0
1	1	0	0	1

$$(p \Rightarrow q) \equiv ((\neg q) \Rightarrow (\neg p))$$

How to prove that $\varphi \Rightarrow \psi$ is true?

$(\varphi \Rightarrow \psi) \not\equiv (\neg\varphi \Rightarrow \neg\psi)$

Proof by contraposition

1. Assume that ψ is false.
2. <insert rest of the proof>
3. We obtain that φ is false.

p	q	$p \Rightarrow q$
0	0	1
0	1	1
1	0	0
1	1	1

p	q	$\neg q$	$\neg p$	$(\neg q) \Rightarrow (\neg p)$
0	0	1	1	1
0	1	0	1	1
1	0	1	0	0
1	1	0	0	1

$$(p \Rightarrow q) \equiv ((\neg q) \Rightarrow (\neg p))$$

$$(\varphi \Rightarrow \psi) \equiv ((\neg \psi) \Rightarrow (\neg \varphi))$$

How to prove that $\varphi \Rightarrow \psi$ is true?

Proof by contradiction

1. Assume that φ is true and that ψ is false.
2. <insert rest of the proof>
3. We obtain something we know is false.

like $0 = 1$

How to prove that $\varphi \Rightarrow \psi$ is true?

Proof by contradiction

1. Assume that φ is true and that ψ is false.
2. <insert rest of the proof>
3. We obtain something we know is false.

p	q	$p \Rightarrow q$
0	0	1
0	1	1
1	0	0
1	1	1

p	q	$\neg q$	$p \wedge \neg q$	$\perp$	$(p \wedge \neg q) \Rightarrow \perp$
0	0	1	0	0	1
0	1	0	0	0	1
1	0	1	1	0	0
1	1	0	0	0	1

How to prove that $\varphi \Rightarrow \psi$ is true?

Proof by contradiction

1. Assume that ϕ is true and that ψ is false.
2. <insert rest of the proof>
3. We obtain something we know is false.

p	q	$p \Rightarrow q$
0	0	1
0	1	1
1	0	0
1	1	1

p	q	$\neg q$	$p \wedge \neg q$	$\perp$	$(p \wedge \neg q) \Rightarrow \perp$
0	0	1	0	0	1
0	1	0	0	0	1
1	0	1	1	0	0
1	1	0	0	0	1

$$(p \Rightarrow q) \equiv ((p \wedge \neg q) \Rightarrow \perp)$$

How to prove that $\varphi \Rightarrow \psi$ is true?

Proof by contradiction

1. Assume that ϕ is true and that ψ is false.
2. <insert rest of the proof>
3. We obtain something we know is false.

p	q	$p \Rightarrow q$
0	0	1
0	1	1
1	0	0
1	1	1

p	q	$\neg q$	$p \wedge \neg q$	$\perp$	$(p \wedge \neg q) \Rightarrow \perp$
0	0	1	0	0	1
0	1	0	0	0	1
1	0	1	1	0	0
1	1	0	0	0	1

$$(p \Rightarrow q) \equiv ((p \wedge \neg q) \Rightarrow \perp)$$

$$(\varphi \Rightarrow \psi) \equiv ((\varphi \wedge \neg \psi) \Rightarrow \perp)$$

How to prove that $\varphi \Rightarrow \psi$ is true?

Proof by contradiction

1. Assume that ϕ is true and that ψ is false.
2. <insert rest of the proof>
3. We obtain something we know is false.

p	q	$p \Rightarrow q$
0	0	1
0	1	1
1	0	0
1	1	1

p	q	$\neg q$	$p \wedge \neg q$	$\perp$	$(p \wedge \neg q) \Rightarrow \perp$
0	0	1	0	0	1
0	1	0	0	0	1
1	0	1	1	0	0
1	1	0	0	0	1

$$(p \Rightarrow q) \equiv ((p \wedge \neg q) \Rightarrow \perp)$$

$$(\varphi \Rightarrow \psi) \equiv ((\varphi \wedge \neg \psi) \Rightarrow \perp)$$

$0 = 1$

"Best" proof method: maximizes the number of hypotheses!

Predicate Logic

- Want: a logic in which we can express statements like

Some animal flies *Every mammal does not fly* *For every* x, *if* $x > 10$ *then* $2x > 20$

- Want: a logic in which we can express statements like

Some animal flies *Every mammal does not fly* *For every* x*, if* $x > 10$ *then* $2x > 20$

quantifiers

- Want: a logic in which we can express statements like

Some animal flies

it flies

Every mammal does not fly

For every x, *if* $x > 10$ *then* $2x > 20$

quantifiers

predicates

- Want: a logic in which we can express statements like

Some animal flies *Every mammal does not fly* *For every* x, *if* $x > 10$ *then* $2x > 20$

quantifiers predicates

Definition. The formulas of predicate logic are built as follows:

Predicate logic

- Want: a logic in which we can express statements like

Some animal flies   *Every mammal does not fly*   *For every* x, *if* $x > 10$ *then* $2x > 20$

quantifiers   predicates

Definition. The formulas of predicate logic are built as follows:

- Every predicate with variables $x, y, z, \dots$ is a formula

"x is a mammal", "$x > y$", "$x \in A$"

- Want: a logic in which we can express statements like

Some animal flies *Every mammal does not fly* *For every* x, *if* $x > 10$ *then* $2x > 20$

quantifiers predicates

Definition. The formulas of predicate logic are built as follows:

- Every predicate with variables $x, y, z, \ldots$ is a formula
- If φ and ψ are predicate formulas, then $\varphi \wedge \psi, \varphi \vee \psi, \varphi \Rightarrow \psi, \neg\varphi$ are also formulas

"x is a mammal", "$x > y$", "$x \in A$"

x is a mammal $\Rightarrow \neg(x$ flies)

$x > 10 \Rightarrow 2x > 20$

- Want: a logic in which we can express statements like

Some animal flies *Every mammal does not fly* *For every* x*, if* $x > 10$ *then* $2x > 20$

quantifiers predicates

Definition. The formulas of predicate logic are built as follows:

- Every predicate with variables $x, y, z, \ldots$ is a formula
- If φ and ψ are predicate formulas, then $\varphi \wedge \psi, \varphi \vee \psi, \varphi \Rightarrow \psi, \neg\varphi$ are also formulas
- If φ is a formula, then $\forall x \varphi$ is a formula

"x is a mammal", "$x > y$", "$x \in A$"

x is a mammal $\Rightarrow \neg$(x flies)

$x > 10 \Rightarrow 2x > 20$

$\forall x$(x is a mammal $\Rightarrow \neg x$ flies)

- Want: a logic in which we can express statements like

Some animal flies *Every mammal does not fly* *For every x, if $x > 10$ then $2x > 20$*

quantifiers predicates

Definition. The formulas of predicate logic are built as follows:

- Every predicate with variables $x, y, z, \ldots$ is a formula
- If φ and ψ are predicate formulas, then $\varphi \land \psi, \varphi \lor \psi, \varphi \Rightarrow \psi, \neg\varphi$ are also formulas
- If φ is a formula, then $\forall x \varphi$ is a formula
- If φ is a formula, then $\exists x \varphi$ is a formula

"x is a mammal", "$x > y$", "$x \in A$"

x is a mammal $\Rightarrow \neg$(x flies)

$x > 10 \Rightarrow 2x > 20$

$\forall x$(x is a mammal $\Rightarrow \neg x$ flies)

$\exists x$(x is an animal $\land$ x flies)

- Want: a logic in which we can express statements like

Some animal flies *Every mammal does not fly* *For every* x, *if* $x > 10$ *then* $2x > 20$

quantifiers predicates

Definition. The formulas of predicate logic are built as follows:

- Every predicate with variables $x, y, z, \ldots$ is a formula
- If φ and ψ are predicate formulas, then $\varphi \wedge \psi, \varphi \vee \psi, \varphi \Rightarrow \psi, \neg\varphi$ are also formulas
- If φ is a formula, then $\forall x \varphi$ is a formula
- If φ is a formula, then $\exists x \varphi$ is a formula

"x is a mammal", "$x > y$", "$x \in A$"

x is a mammal $\Rightarrow \neg$(x flies)

$x > 10 \Rightarrow 2x > 20$

$\forall x$(x is a mammal $\Rightarrow \neg x$ flies)

$\exists x$(x is an animal $\wedge$ x flies)

$\forall x$: For all possible values of x, ...

$\exists x$: There exists a possible value of x such that...

- Want: a logic in which we can express statements like

Some animal flies *Every mammal does not fly* *For every x, if $x > 10$ then $2x > 20$*

quantifiers predicates

Definition. The formulas of predicate logic are built as follows:

- Every predicate with variables $x, y, z, \ldots$ is a formula
- If φ and ψ are predicate formulas, then $\varphi \wedge \psi, \varphi \vee \psi, \varphi \Rightarrow \psi, \neg\varphi$ are also formulas
- If φ is a formula, then $\forall x \varphi$ is a formula
- If φ is a formula, then $\exists x \varphi$ is a formula

"x is a mammal", "$x > y$", "$x \in A$"

x is a mammal $\Rightarrow \neg(x$ flies$)$

$x > 10 \Rightarrow 2x > 20$

$\forall x(x$ is a mammal $\Rightarrow \neg x$ flies$)$

$\exists x(x$ is an animal $\wedge\, x$ flies$)$

$\forall x$: For all possible values of x, ...

$\exists x$: There exists a possible value of x such that...

$\forall x \in S$: for all x in the set S, ...

$\exists x \in S$: there exists some x in the set S such that...

$\varphi \Rightarrow \psi \rightsquigarrow \neg\psi \Rightarrow \neg\varphi$

Definition. The formulas of predicate logic are built as follows:

- Every predicate with variables $x, y, z, \ldots$ is a formula
- If φ and ψ are predicate formulas, then $\varphi \wedge \psi, \varphi \vee \psi, \varphi \Rightarrow \psi, \neg\varphi$ are also formulas
- If φ is a formula, then $\forall x \varphi$ is a formula
- If φ is a formula, then $\exists x \varphi$ is a formula

"x is a mammal", "$x > y$", "$x \in A$"

x is a mammal $\Rightarrow \neg(x$ flies)

$x > 10 \Rightarrow 2x > 20$

$\forall x(x$ is a mammal $\Rightarrow \neg x$ flies)

$\exists x(x$ is an animal $\wedge\, x$ flies)

- Because of proofs by contradiction/contraposition, one often has to compute $\neg\varphi$ for a formula φ

Definition. The formulas of predicate logic are built as follows:

- Every predicate with variables $x, y, z, \ldots$ is a formula
- If φ and ψ are predicate formulas, then $\varphi \wedge \psi, \varphi \vee \psi, \varphi \Rightarrow \psi, \neg\varphi$ are also formulas
- If φ is a formula, then $\forall x \varphi$ is a formula
- If φ is a formula, then $\exists x \varphi$ is a formula

"x is a mammal", "$x > y$", "$x \in A$"

x is a mammal $\Rightarrow \neg(x$ flies$)$

$x > 10 \Rightarrow 2x > 20$

$\forall x(x$ is a mammal $\Rightarrow \neg x$ flies$)$

$\exists x(x$ is an animal $\wedge\, x$ flies$)$

- Because of proofs by contradiction/contraposition, one often has to compute $\neg\varphi$ for a formula φ
- Here are some good shortcuts to remember for negation:

If φ is...	Then $\neg\varphi$ is equivalent to...
$\psi \wedge \theta$	$\neg\psi \vee \neg\theta$
$\psi \vee \theta$	$\neg\psi \wedge \neg\theta$
$\neg\psi$	ψ

De Morgan's rules

Definition. The formulas of predicate logic are built as follows:

- Every predicate with variables $x, y, z, \dots$ is a formula
- If φ and ψ are predicate formulas, then $\varphi \wedge \psi, \varphi \vee \psi, \varphi \Rightarrow \psi, \neg\varphi$ are also formulas
- If φ is a formula, then $\forall x \varphi$ is a formula
- If φ is a formula, then $\exists x \varphi$ is a formula

"x is a mammal", "$x > y$", "$x \in A$"

x is a mammal $\Rightarrow \neg(x$ flies$)$

$x > 10 \Rightarrow 2x > 20$

$\forall x(x$ is a mammal $\Rightarrow \neg x$ flies$)$

$\exists x(x$ is an animal $\wedge\, x$ flies$)$

- Because of proofs by contradiction/contraposition, one often has to compute $\neg\varphi$ for a formula φ
- Here are some good shortcuts to remember for negation:

If φ is...	Then $\neg\varphi$ is equivalent to...
$\psi \wedge \theta$	$\neg\psi \vee \neg\theta$
$\psi \vee \theta$	$\neg\psi \wedge \neg\theta$
$\neg\psi$	ψ
$\psi \Rightarrow \theta$	$\psi \wedge \neg\theta$

ψ	θ	$\psi \Rightarrow \theta$	$\neg(\psi \Rightarrow \theta)$
0	0	1	0
0	1	1	0
1	0	0	1
1	1	1	0

Definition. The formulas of predicate logic are built as follows:

- Every predicate with variables $x, y, z, \ldots$ is a formula
- If φ and ψ are predicate formulas, then $\varphi \wedge \psi, \varphi \vee \psi, \varphi \Rightarrow \psi, \neg\varphi$ are also formulas
- If φ is a formula, then $\forall x \varphi$ is a formula
- If φ is a formula, then $\exists x \varphi$ is a formula

"x is a mammal", "$x > y$", "$x \in A$"

x is a mammal $\Rightarrow \neg(x$ flies$)$

$x > 10 \Rightarrow 2x > 20$

$\forall x(x$ is a mammal $\Rightarrow \neg x$ flies$)$

$\exists x(x$ is an animal $\wedge\ x$ flies$)$

- Because of proofs by contradiction/contraposition, one often has to compute $\neg\varphi$ for a formula φ
- Here are some good shortcuts to remember for negation:

If φ is...	Then $\neg\varphi$ is equivalent to...
$\psi \wedge \theta$	$\neg\psi \vee \neg\theta$
$\psi \vee \theta$	$\neg\psi \wedge \neg\theta$
$\neg\psi$	ψ
$\psi \Rightarrow \theta$	$\psi \wedge \neg\theta$
$\forall x\, \psi$	$\exists x\, \neg\psi$
$\exists x\, \psi$	$\forall x\, \neg\psi$

Definition. The formulas of predicate logic are built as follows:

- Every predicate with variables $x, y, z, \ldots$ is a formula
- If φ and ψ are predicate formulas, then $\varphi \wedge \psi, \varphi \vee \psi, \varphi \Rightarrow \psi, \neg\varphi$ are also formulas
- If φ is a formula, then $\forall x \varphi$ is a formula
- If φ is a formula, then $\exists x \varphi$ is a formula

"x is a mammal", "$x > y$", "$x \in A$"

x is a mammal $\Rightarrow \neg(x$ flies)

$x > 10 \Rightarrow 2x > 20$

$\forall x(x$ is a mammal $\Rightarrow \neg x$ flies)

$\exists x(x$ is an animal $\wedge\, x$ flies)

- Because of proofs by contradiction/contraposition, one often has to compute $\neg\varphi$ for a formula φ
- Here are some good shortcuts to remember for negation:

If φ is...	Then $\neg\varphi$ is equivalent to...
$\psi \wedge \theta$	$\neg\psi \vee \neg\theta$
$\psi \vee \theta$	$\neg\psi \wedge \neg\theta$
$\neg\psi$	ψ
$\psi \Rightarrow \theta$	$\psi \wedge \neg\theta$
$\forall x \in S\, \psi$	$\exists x \in S\, \neg\psi$
$\exists x \in S\, \psi$	$\forall x \in S\, \neg\psi$

Theorem. Let $a \in \mathbb{R}$. If $a^2 = 0$, then $a = 0$.

Assume $a^2 = 0$.

????

Theorem. Let $a \in \mathbb{R}$. If $a^2 = 0$, then $a = 0$.

$$\forall \; a \in \mathbb{R} \quad (a^2 = 0 \implies a = 0)$$

Theorem. Let $a \in \mathbb{R}$. If $a^2 = 0$, then $a = 0$.

$$\forall \; a \in \mathbb{R} \quad (a^2 = 0 \implies a = 0)$$

$\varphi \Rightarrow \psi \rightsquigarrow (\varphi \wedge \neg \psi) \Rightarrow \bot$

Proof.

1. By contradiction, suppose that $a^2 = 0$ and $a \neq 0$.

Theorem. Let $a \in \mathbb{R}$. If $a^2 = 0$, then $a = 0$.

$$\forall \; a \in \mathbb{R} \quad (a^2 = 0 \implies a = 0)$$

Proof.

1. By contradiction, suppose that $a^2 = 0$ and $a \neq 0$.
2. Since $a \neq 0$, $\frac{1}{a}$ exists.

Theorem. Let $a \in \mathbb{R}$. If $a^2 = 0$, then $a = 0$.

$$\forall \ a \in \mathbb{R} \quad (a^2 = 0 \implies a = 0)$$

Proof.

1. By contradiction, suppose that $a^2 = 0$ and $a \neq 0$.
2. Since $a \neq 0$, $\frac{1}{a}$ exists.
3. Then $a^2 \times \frac{1}{a} = 0 \times \frac{1}{a}$.

Theorem. Let $a \in \mathbb{R}$. If $a^2 = 0$, then $a = 0$.

$$\forall \; a \in \mathbb{R} \quad (a^2 = 0 \implies a = 0)$$

Proof.

1. By contradiction, suppose that $a^2 = 0$ and $a \neq 0$.
2. Since $a \neq 0$, $\frac{1}{a}$ exists.
3. Then $a^2 \times \frac{1}{a} = 0 \times \frac{1}{a}$.
4. So $a = 0$.

Theorem. Let $a \in \mathbb{R}$. If $a^2 = 0$, then $a = 0$.

$$\forall \; a \in \mathbb{R} \quad (a^2 = 0 \implies a = 0)$$

Proof.

1. By contradiction, suppose that $a^2 = 0$ and $a \neq 0$.
2. Since $a \neq 0$, $\frac{1}{a}$ exists.
3. Then $a^2 \times \frac{1}{a} = 0 \times \frac{1}{a}$.
4. So $a = 0$.
5. Contradiction! $\square$

Theorem. Let $a, b \in \mathbb{N}$. If $a \times b$ is not divisible by 5, then a is not divisible by 5.

Theorem. Let $a, b \in \mathbb{N}$. If $a \times b$ is not divisible by 5, then a is not divisible by 5.

$$\forall a \in \mathbb{N} \forall b \in \mathbb{N} \qquad (\neg(a \times b \text{ divisible by } 5) \implies \neg(a \text{ is divisible by } 5))$$

Theorem. Let $a, b \in \mathbb{N}$. If $a \times b$ is not divisible by 5, then a is not divisible by 5.

$$\forall a \in \mathbb{N} \forall b \in \mathbb{N} \qquad (\neg(a \times b \text{ divisible by } 5) \implies \neg(a \text{ is divisible by } 5))$$

Contraposition of the implication:

$$\forall a \in \mathbb{N} \forall b \in \mathbb{N} \qquad (a \text{ is divisible by } 5 \implies a \times b \text{ divisible by } 5)$$

Theorem. Let $a, b \in \mathbb{N}$. If $a \times b$ is not divisible by 5, then a is not divisible by 5.

$$\forall a \in \mathbb{N} \forall b \in \mathbb{N} \qquad (\neg(a \times b \text{ divisible by } 5) \quad \implies \quad \neg(a \text{ is divisible by } 5))$$

Contraposition of the implication:

$$\forall a \in \mathbb{N} \forall b \in \mathbb{N} \qquad (a \text{ is divisible by } 5 \qquad \implies \quad a \times b \text{ divisible by } 5)$$

Proof.

1. By definition of being divisible by 5, we can write $a = 5 \times a'$ for some $a' \in \mathbb{N}$.

Theorem. Let $a, b \in \mathbb{N}$. If $a \times b$ is not divisible by 5, then a is not divisible by 5.

$$\forall a \in \mathbb{N} \forall b \in \mathbb{N} \qquad (\neg(a \times b \text{ divisible by } 5) \implies \neg(a \text{ is divisible by } 5))$$

Contraposition of the implication:

$$\forall a \in \mathbb{N} \forall b \in \mathbb{N} \qquad (a \text{ is divisible by } 5 \implies a \times b \text{ divisible by } 5)$$

Proof.

1. By definition of being divisible by 5, we can write $a = 5 \times a'$ for some $a' \in \mathbb{N}$.
2. Then $a \times b = 5 \times (a' \times b)$.

Theorem. Let $a, b \in \mathbb{N}$. If $a \times b$ is not divisible by 5, then a is not divisible by 5.

$$\forall a \in \mathbb{N} \forall b \in \mathbb{N} \qquad (\neg(a \times b \text{ divisible by } 5) \implies \neg(a \text{ is divisible by } 5))$$

Contraposition of the implication:

$$\forall a \in \mathbb{N} \forall b \in \mathbb{N} \qquad (a \text{ is divisible by } 5 \qquad \implies \quad a \times b \text{ divisible by } 5)$$

Proof.

1. By definition of being divisible by 5, we can write $a = 5 \times a'$ for some $a' \in \mathbb{N}$.
2. Then $a \times b = 5 \times a' \times b$.
3. So $a \times b$ is divisible by 5. $\square$

Proof by contradiction?

$(\ldots) \Rightarrow \perp$

1. a×b is not divisible by 5
2. a divisible by 5