Warm-Up

"Dr. Evil will attack you with laser sharks, unless you pay him one-million dollars."

How would you translate "unless" into logic?

Warm-Up – Solution

"Dr. Evil will attack you with laser sharks, unless you pay him one-million dollars."

If you pay Dr. Evil his one-million dollars, are you safe from the laser sharks?

This is Dr. Evil! He hasn't promised you that's his **full** list of demands.

If you do not pay Dr. Evil one-million dollars, then he will attack you with laser sharks.

Is the only promise you really have.

Warm-Up – Solution

"Dr. Evil will attack you with laser sharks, unless you pay him one-million dollars."

p: Dr. Evil will attack you with laser sharks

q: You pay him one-million dollars

The last slide would give us: $\neg q \rightarrow p$

If Dr. Evil doesn't attack you with laser sharks, you must have paid him his million dollars, right? $\neg p \rightarrow q$ Are those both good translations?

xkcd.com/1153

Our First Proof and Digital Logic

CSE 311 Fall 2020
Lecture 3

Today

10 minutes of syllabus

Our first proof!

Contrapositives and digital logic.

Announcements

Homework 1 Problem 6 clarified (download a new version of the pdf).

Office Hours start this week.

Order of Operations

Just like you were taught PEMDAS

e.g. $3 + 2 \cdot 4 = 11$ not 24.

Logic also has order of operations.

Parentheses

Negation

And

Or, exclusive or

Implication

Biconditional

For this course: each of these is it's own level!
e.g. "and"s have precedence over "or"s

Within a level, apply from left to right.

Other authors place And, Or at the same level – it's good practice to use parentheses even if not required.

Office Hours

A chance to talk to staff about the class.

Advice:
You don't have to have a question to come to office hours! (It can help, though)
Aim as early in the week as possible.
We won't answer every kind of question in office hours:

 We don't "pregrade" homework. We won't tell you whether something is right or wrong.

 We will help on homework, but not usually by "giving hints." We'll usually ask questions about what you've tried, ask questions to help you decide what to do next, or point you to good examples to look at.

You're allowed to talk to others at office hours, as long as you're still following the collaboration policy.

Homework Submissions

Make sure we can read what you submit.

We can't spend 5 minutes per submission deciding if that's a p or a q.

Typesetting guarantees we can read it.

Microsoft Word's equation editor is now halfway decent!

LaTeX is the industry standard for typesetting (if you go to CS grad school, you'll use it for all your papers). Overleaf is the easiest way to get started.

Need to know the code for a symbol? [Detexify]! Word uses LaTeX codes...mostly...
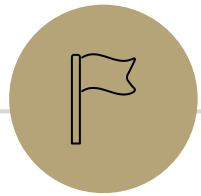
Our First Proof

Last Time

We showed

DeMorgan's Laws:

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

And the Law of Implication

$p \rightarrow q \equiv \neg p \lor q$

Properties of Logical Connectives

For every propositions p, q, r the following hold:

- **Identity**
  - $p \wedge \mathrm{T} \equiv p$
  - $p \vee \mathrm{F} \equiv p$
- **Domination**
  - $p \vee \mathrm{T} \equiv \mathrm{T}$
  - $p \wedge \mathrm{F} \equiv \mathrm{F}$
- **Idempotent**
  - $p \vee p \equiv p$
  - $p \wedge p \equiv p$
- **Commutative**
  - $p \vee q \equiv q \vee p$
  - $p \wedge q \equiv q \wedge p$

- **Associative**
  - $(p \vee q) \vee r \equiv p \vee (q \vee r)$
  - $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$
- **Distributive**
  - $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
  - $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
- **Absorption**
  - $p \vee (p \wedge q) \equiv p$
  - $p \wedge (p \vee q) \equiv p$
- **Negation**
  - $p \vee \neg p \equiv \mathrm{T}$
  - $p \wedge \neg p \equiv \mathrm{F}$

Using Our Rules

WOW that was a lot of rules.

Why do we need them? Simplification!

Let's go back to the "law of implication" example.

p	q	$p \to q$
T	T	T
T	F	F
F	T	T
F	F	T

When is the implication true? Just "or" each of the three "true" lines!

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

Also seems pretty reasonable

So is $(p \wedge q) \vee (\neg p \wedge q) \vee (\neg p \wedge \neg q) \equiv (\neg p \vee q)$

i.e. are these both alternative representations of $p \to q$?

Our First Proof

We could make another truth table (you should! It's a good exercise)

But we have another technique that is nicer.

Let's try that one

Then talk about why it's another good option.

We're going to give an iron-clad guarantee that:

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

i.e. that this is another valid "law of implication"

Our First Proof

How do we write a proof?

It's not always plug-and-chug...we'll be highlighting strategies throughout the quarter.

To start with:

Make sure we know what we want to show...

Our First Proof

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

None of the rules look like this

Practice of Proof-Writing:
Big Picture…WHY do we think this might be true?

The last two "pieces" came from the vacuous proof lines…maybe the "$\neg p$" came from there? Maybe that **simplifies** down to $\neg p$

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

Let's apply a rule

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

The law says:

$p \land (q \lor r) \equiv (p \land q) \lor (p \land r)$

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

Our First Proof

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

None of the rules look like this

Practice of Proof-Writing:
Big Picture...WHY do we think this
might be true?

The last two "pieces" came from the $\equiv (\neg p \vee q)$
vacuous proof lines...maybe the "$\neg p$"
came from there? Maybe that
simplifies down to $\neg p$

Our First Proof

$$(p \wedge q) \vee (\neg p \wedge q) \vee (\neg p \wedge \neg q) \equiv (p \wedge q) \vee [(\neg p \wedge q) \vee (\neg p \wedge \neg q)]$$

Set ourselves an intermediate goal.
Let's try to simplify those last two pieces

Associative law
Connect up the things we're working on.

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

Our First Proof

$$(p \wedge q) \vee (\neg p \wedge q) \vee (\neg p \wedge \neg q) \equiv (p \wedge q) \vee [(\neg p \wedge q) \vee (\neg p \wedge \neg q)]$$
$$\equiv (p \wedge q) \vee [\neg p \wedge (q \vee \neg q)]$$

Set ourselves an intermediate goal.
Let's try to simplify those last two pieces

Distributive law
We think $\neg p$ is important, let's isolate it.

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

Our First Proof

$(p \wedge q) \vee (\neg p \wedge q) \vee (\neg p \wedge \neg q) \equiv (p \wedge q) \vee [(\neg p \wedge q) \vee (\neg p \wedge \neg q)]$
$\equiv (p \wedge q) \vee [\neg p \wedge (q \vee \neg q)]$
$\equiv (p \wedge q) \vee [\neg p \wedge \text{T}]$

Set ourselves an intermediate goal. Let's try to simplify those last two pieces

Negation
Should make things simpler.

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

Our First Proof

$(p \land q) \lor (\neg p \land q) \lor (\neg p \land \neg q) \equiv (p \land q) \lor [(\neg p \land q) \lor (\neg p \land \neg q)]$
$\equiv (p \land q) \lor [\neg p \land (q \lor \neg q)]$
$\equiv (p \land q) \lor [\neg p \land T]$
$\equiv (p \land q) \lor [\neg p]$

Set ourselves an intermediate goal. Let's try to simplify those last two pieces

Identity
Should make things simpler.

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

Our First Proof

$(p \land q) \lor (\neg p \land q) \lor (\neg p \land \neg q) \equiv (p \land q) \lor [(\neg p \land q) \lor (\neg p \land \neg q)]$
$$\equiv (p \land q) \lor [\neg p \land (q \lor \neg q)]$$
$$\equiv (p \land q) \lor [\neg p \land \text{T}]$$
$$\equiv (p \land q) \lor [\neg p]$$
$$\equiv [\neg p] \lor (p \land q)$$

Stay on target:
We met our intermediate goal.
Don't forget the final goal!
We want to end up at $(\neg p \lor q)$

If we apply the distribution rule,
We'd get a $(\neg p \lor q)$

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

Our First Proof

$$(p \land q) \lor (\neg p \land q) \lor (\neg p \land \neg q) \equiv (p \land q) \lor [(\neg p \land q) \lor (\neg p \land \neg q)]$$
$$\equiv (p \land q) \lor [\neg p \land (q \lor \neg q)]$$
$$\equiv (p \land q) \lor [\neg p \land \text{T}]$$
$$\equiv (p \land q) \lor [\neg p]$$
$$\equiv [\neg p] \lor (p \land q)$$

Stay on target:
We met our intermediate goal.
Don't forget the final goal!
We want to end up at $(\neg p \lor q)$

If we apply the distribution rule,
We'd get a $(\neg p \lor q)$

Commutative
$$\equiv (\neg p \lor q)$$
Make the expression look exactly like the law (more on this later)

Our First Proof

$(p \land q) \lor (\neg p \land q) \lor (\neg p \land \neg q) \equiv (p \land q) \lor [(\neg p \land q) \lor (\neg p \land \neg q)]$
$\equiv (p \land q) \lor [\neg p \land (q \lor \neg q)]$
$\equiv (p \land q) \lor [\neg p \land \mathrm{T}]$
$\equiv (p \land q) \lor [\neg p]$
$\equiv [\neg p] \lor (p \land q)$
$\equiv (\neg p \lor p) \land (\neg p \lor q)$

Stay on target:
We met our intermediate goal.
Don't forget the final goal!
We want to end up at $(\neg p \lor q)$

If we apply the distribution rule,
We'd get a $(\neg p \lor q)$

Distributive $\equiv (\neg p \lor q)$
Creates the $(\neg p \lor q)$ we were hoping for.

Our First Proof

$(p \land q) \lor (\neg p \land q) \lor (\neg p \land \neg q) \equiv (p \land q) \lor [(\neg p \land q) \lor (\neg p \land \neg q)]$
$\equiv (p \land q) \lor [\neg p \land (q \lor \neg q)]$
$\equiv (p \land q) \lor [\neg p \land \text{T}]$
$\equiv (p \land q) \lor [\neg p]$
$\equiv [\neg p] \lor (p \land q)$
$\equiv (\neg p \lor p) \land (\neg p \lor q)$
$\equiv (p \lor \neg p) \land (\neg p \lor q)$
$\equiv \text{T} \land (\neg p \lor q)$

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

Stay on target:
We met our intermediate goal.
Don't forget the final goal!
We want to end up at $(\neg p \lor q)$

If we apply the distribution rule,
We'd get a $(\neg p \lor q)$

Commutative
Make the expression look exactly like the law (more on this later)
Identity
Simplifies the part we want to disappear.

Simplify $\mathbb{T} \wedge (\neg p \vee q)$ to $(\neg p \vee q)$

For every propositions p, q, r the following hold:

- **Identity**
  - $p \wedge \mathrm{T} \equiv p$
  - $p \vee \mathrm{F} \equiv p$
- **Domination**
  - $p \vee \mathrm{T} \equiv \mathrm{T}$
  - $p \wedge \mathrm{F} \equiv \mathrm{F}$
- **Idempotent**
  - $p \vee p \equiv p$
  - $p \wedge p \equiv p$
- **Commutative**
  - $p \vee q \equiv q \vee p$
  - $p \wedge q \equiv q \wedge p$

- **Associative**
  - $(p \vee q) \vee r \equiv p \vee (q \vee r)$
  - $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$
- **Distributive**
  - $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
  - $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
- **Absorption**
  - $p \vee (p \wedge q) \equiv p$
  - $p \wedge (p \vee q) \equiv p$
- **Negation**
  - $p \vee \neg p \equiv \mathrm{T}$
  - $p \wedge \neg p \equiv \mathrm{F}$

Our First Proof

$(p \land q) \lor (\neg p \land q) \lor (\neg p \land \neg q) \equiv (p \land q) \lor [(\neg p \land q) \lor (\neg p \land \neg q)]$

$\equiv (p \land q) \lor [\neg p \land (q \lor \neg q)]$

Stay on target:
We met our intermediate goal.
Don't forget the final goal!
We want to end up at $(\neg p \lor q)$

$\equiv (p \land q) \lor [\neg p \land \text{T}]$

$\equiv (p \land q) \lor [\neg p]$

$\equiv [\neg p] \lor (p \land q)$

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

If we apply the distribution rule,
We'd get a $(\neg p \lor q)$

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

$\equiv \text{T} \land (\neg p \lor q)$

$\equiv (\neg p \lor q) \land \text{T}$

Commutative followed by **Identity**
Look exactly like the law, then apply it.

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

We're done!!!

Commutativity

We had the expression $(p \wedge q) \vee [\neg p]$

But before we applied the distributive law, we switched the order...why?

The law says $p \vee (q \wedge r) \equiv (\text{p} \vee q) \wedge (p \vee r)$

not $(q \wedge r) \vee p \equiv (q \vee p) \wedge (r \vee p)$

So **technically** we needed to commute first.

Eventually (in about 2 weeks) we'll skip this step. For now, we're doing two separate steps.

Remember this is the "training wheel" stage. The point is to be careful.

More on Our First Proof

We now have an ironclad guarantee that

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

Hooray! But we could have just made a truth-table. Why a proof?

Here's one reason.

Proofs don't *just* give us an ironclad guarantee. They're also an explanation of *why* the claim is true.

The key insight to our simplification was "the last two pieces were the vacuous truth parts – the parts where p was false"

That's in there, *in the proof.*

Our First Proof

$(p \wedge q) \vee (\neg p \wedge q) \vee (\neg p \wedge \neg q) \equiv (p \wedge q) \vee [(\neg p \wedge q) \vee (\neg p \wedge \neg q)]$ Associative

The last two terms are "vacuous truth" – they simplify to $\neg p$

$\equiv (p \wedge q) \vee [\neg p \wedge (q \vee \neg q)]$ Distributive

$\equiv (p \wedge q) \vee [\neg p \wedge \text{T}]$ Negation

$\equiv (p \wedge q) \vee [\neg p]$ Identity

$\equiv [\neg p] \vee (p \wedge q)$ Commutative

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

p no longer matters in $p \wedge q$ if $\neg p$ automatically makes the expression true.

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

$\equiv \text{T} \wedge (\neg p \vee q)$ Negation

$\equiv (\neg p \vee q) \wedge \text{T}$ Commutative

$\equiv (\neg p \vee q)$ Identity

More on Our First Proof

With practice (and quite a bit of squinting) you can see not just the ironclad guarantee, but also the reason why something is true.

That's not easy with a truth table.

Proofs can also communicate intuition about why a statement is true.
We'll practice extracting intuition from proofs more this quarter.

Converse, Contrapositive

Implication:

If it's raining, then I have my umbrella.

$$p \rightarrow q$$

Contrapositive:

$$\neg q \rightarrow \neg p$$ If I don't have my umbrella, then it is not raining.

Converse:

If I have my umbrella, then it is raining.

$$q \rightarrow p$$

Inverse:

$$\neg p \rightarrow \neg q$$ If it is not raining, then I don't have my umbrella.

How do these relate to each other?

p	q	$p \rightarrow q$	$q \rightarrow p$	$\neg p$	$\neg q$	$\neg p \rightarrow \neg q$	$\neg q \rightarrow \neg p$
T	T						
T	F						
F	T						
F	F						

Converse, Contrapositive

Implication:

$$p \rightarrow q$$

Contrapositive:

$$\neg q \rightarrow \neg p$$

Converse:

$$q \rightarrow p$$

Inverse:

$$\neg p \rightarrow \neg q$$

An **implication** and its **contrapositive** have the same truth value!

p	q	$p \rightarrow q$	$q \rightarrow p$	$\neg p$	$\neg q$	$\neg p \rightarrow \neg q$	$\neg q \rightarrow \neg p$
T	T	T	T	F	F	T	T
T	F	F	T	F	T	T	F
F	T	T	F	T	F	F	T
F	F	T	T	T	T	T	T

Contrapositive

We showed $p \rightarrow q \equiv \neg q \rightarrow \neg p$ with a truth table. Let's do a proof.

Try this one on your own. Remember

1. Know what you're trying to show.

2. Stay on target – take steps to get closer to your goal.

Hint: think about your tools.

There are lots of rules with AND/OR/NOT,

but very few with implications...

Fill out the poll everywhere for Activity Credit!

Go to pollev.com/cse311 and login with your UW identity
Or text cse311 to 22333

Contrapositive

$$p \rightarrow q \equiv \neg p \lor q \qquad \text{Law of Implication}$$
$$\equiv q \lor \neg p \qquad \text{Commutativity}$$
$$\equiv \neg\neg q \lor \neg p \qquad \text{Double Negation}$$
$$\equiv \neg q \rightarrow \neg p \qquad \text{Law of Implication}$$

All of our rules deal with ORs and ANDs, let's switch the implication to just use AND/NOT/OR.
And do the same with our target
    It's ok to work from both ends. In fact it's a very common strategy!
Now how do we get the top to look like the bottom?
    Just a few more rules and we're done!
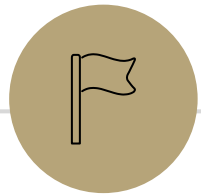
Digital Logic

Digital Circuits

Computing With Logic

T corresponds to 1 or "high" voltage

F corresponds to 0 or "low" voltage

Gates

Take inputs and produce outputs (functions)

Several kinds of gates

Correspond to propositional connectives (most of them)

And Gate

AND Connective   vs.   **AND Gate**

$p \wedge q$

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F
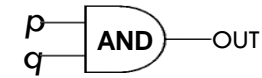
p	q	OUT
1	1	1
1	0	0
0	1	0
0	0	0
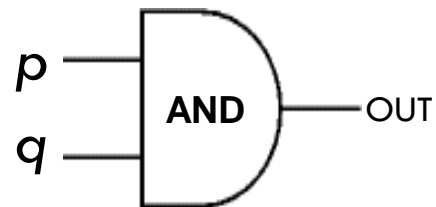
"block looks like D of AND"

Or Gate

OR Connective   vs.   OR Gate

$p \vee q$

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F
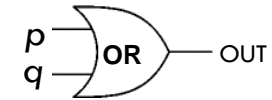
p	q	OUT
1	1	1
1	0	1
0	1	1
0	0	0

p —— OR —— OUT
q
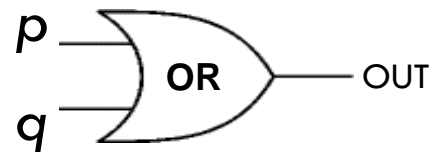
"arrowhead block looks like V"

Not Gates

NOT Connective   vs.   **NOT Gate**

$\neg p$

p	$\neg p$
T	F
F	T

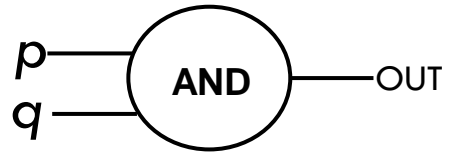| p	OUT
1	0
0	1

p ——NOT◯—— OUT
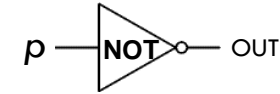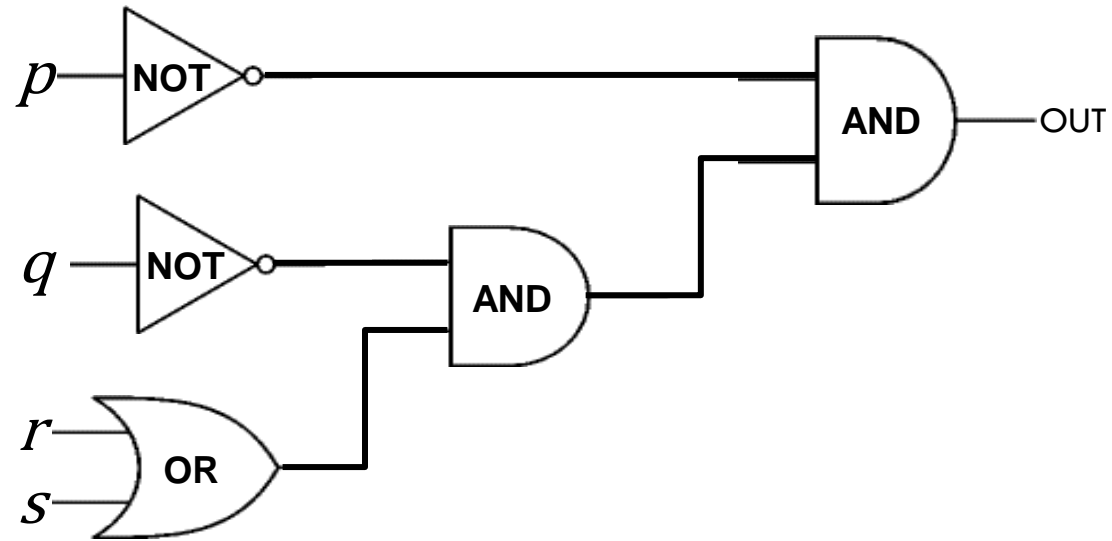
Also called *inverter*

p ——NOT◯—— OUT
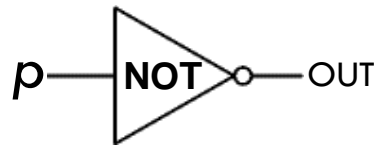
Blobs are Okay!

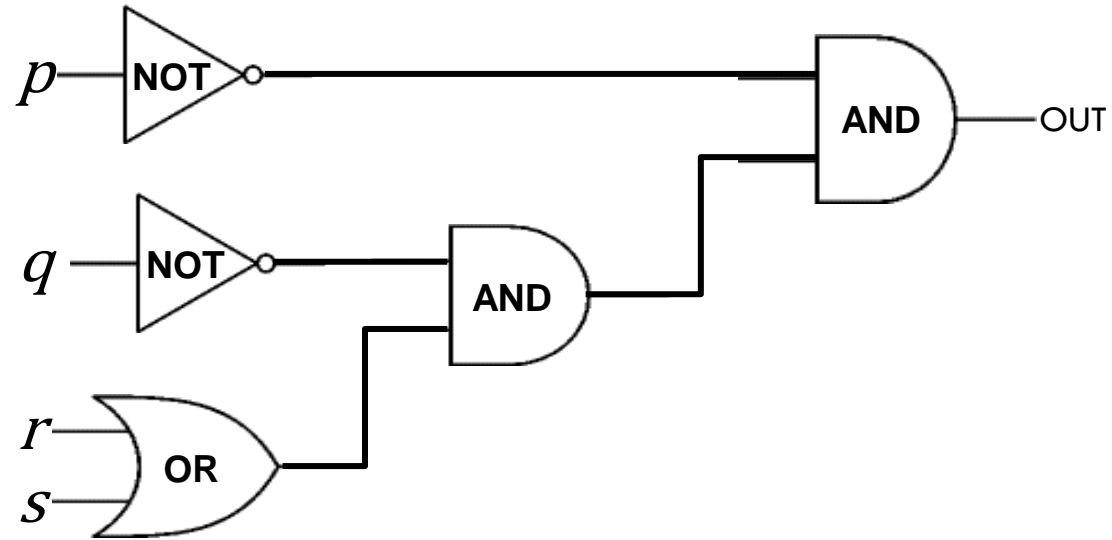**You may write gates using blobs instead of shapes!**
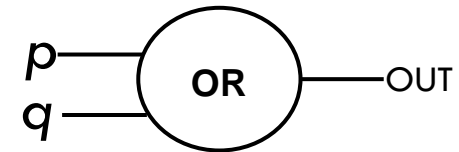
Combinational Logic Circuits

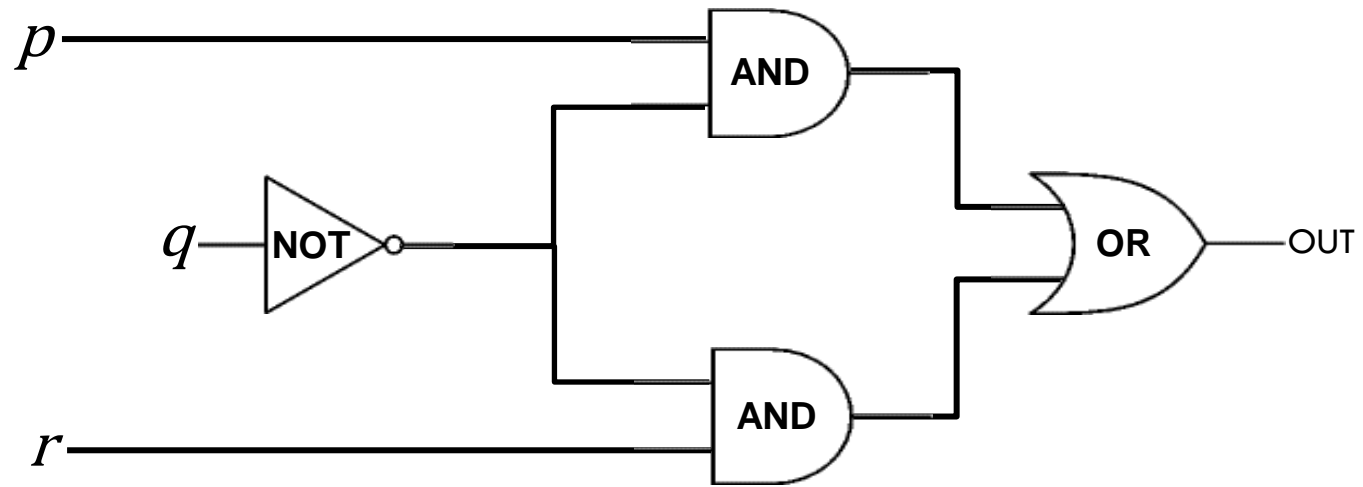**Values get sent along wires connecting gates**

Combinational Logic Circuits

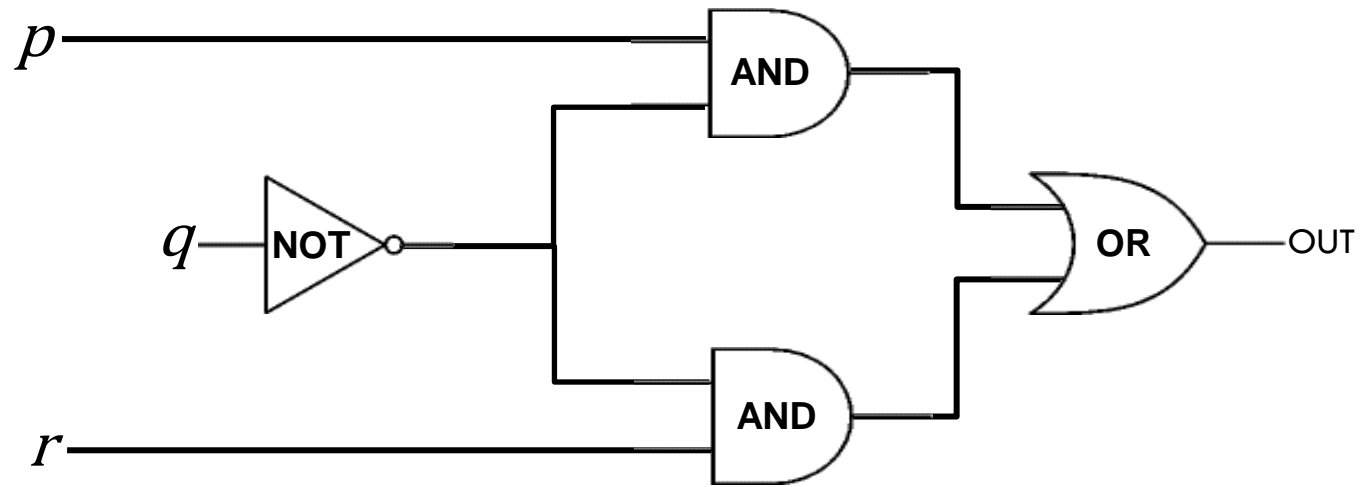**Values get sent along wires connecting gates**

$$\neg p \wedge (\neg q \wedge (r \vee s))$$
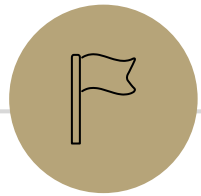
Combinational Logic Circuits

Wires can send one value to multiple gates!

Combinational Logic Circuits

Wires can send one value to multiple gates!

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

More Vocabulary

Vocabulary!

> ## A proposition is a....
> *Tautology* if it is always true.
> *Contradiction* if it is always false.
> *Contingency* if it can be both true and false.

$p \lor \neg p$

Tautology

If p is true, $p \lor \neg p$ is true; if p is false, $p \lor \neg p$ is true.

$p \oplus p$

Contradiction

If p is true, $p \oplus p$ is false; if p is false, $p \oplus p$ is false.

$(p \rightarrow q) \land p$

Contingency If p is true and q is true, $(p \rightarrow q) \land p$ is true;
If p is true and q is false, $(p \rightarrow q) \land p$ is false.

Another Proof

Let's prove that $(p \land q) \rightarrow (q \lor p)$ is a tautology.

Alright, what are we trying to show?

Another Proof

$(p \wedge q) \rightarrow (q \vee p)$ $\equiv \neg(p \wedge q) \vee (q \vee p)$
$\equiv (\neg p \vee \neg q) \vee (q \vee p)$
$\equiv \neg p \vee (\neg q \vee (q \vee p))$
$\equiv \neg p \vee ((\neg q \vee q) \vee p)$
$\equiv \neg p \vee ((q \vee \neg q) \vee p)$
$\equiv \neg p \vee (T \vee p)$
$\equiv \neg p \vee (p \vee T)$
$\equiv \neg p \vee p$
$\equiv p \vee \neg p$
$\equiv T$

Proof-writing tip:
Take a step back.
Pause and carefully look at what you have. You might see where to go next…

Law of Implication
DeMorgan's Law
It's easier if everything is AND/OR/NOT
Associative (twice)
Gets rid of some parentheses/just a gut feeling
Commutative, Negation
Put $q, \neg q$ next to each other.
Commutative, Domination
Simplify out the $q, \neg q$.
Commutative, Negation
Simplify out the T.
Simplify out the $p, \neg p$.

We're done!

Another Proof

$$(p \wedge q) \rightarrow (q \vee p) \equiv \neg(p \wedge q) \vee (q \vee p) \quad \text{Law of implication}$$
$$\equiv (\neg p \vee \neg q) \vee (q \vee p) \quad \text{DeMorgan's Law}$$
$$\equiv \neg p \vee (\neg q \vee (q \vee p)) \quad \text{Associative}$$
$$\equiv \neg p \vee ((\neg q \vee q) \vee p) \quad \text{Associative}$$
$$\equiv \neg p \vee ((q \vee \neg q) \vee p) \quad \text{Commutative}$$
$$\equiv \neg p \vee (\text{T} \vee p) \quad \text{Negation}$$
$$\equiv \neg p \vee (p \vee \text{T}) \quad \text{Commutative}$$
$$\equiv \neg p \vee p \quad \text{Domination}$$
$$\equiv p \vee \neg p \quad \text{Commutative}$$
$$\equiv \text{T} \quad \text{Negation}$$

Computing Equivalence

Given two propositions, can we write an algorithm to determine if they are equivalent?

What is the runtime of our algorithm?

Computing Equivalence

Given two propositions, can we write an algorithm to determine if they are equivalent?

Yes! Generate the truth tables for both propositions and check if they are the same for every entry.

What is the runtime of our algorithm?

Every atomic proposition has two possibilities (T, F). If there are n atomic propositions, there are 2^n rows in the truth table.