Programming + Microprocessors ≡ Superpower!

What are your super powerful programs/processors doing?
  Logic and Proofs!
  Induction ≡ Recursion.

What can computers do?
  Work with discrete objects.
  Discrete Math ⇒ immense application.

Computers learn and interact with the world?
  E.g. machine learning, data analysis, robotics, ...
  Probability!

See note 1, for more discussion.
Instructor: Sanjit Seshia.
Professor of EECS (office: 566 Cory)
Starting 12th year at Berkeley.
PhD: in Computer Science, from Carnegie Mellon University.
Research: Formal Methods (a.k.a. Computational Proof
Methods)
    applied to cyber-physical systems (e.g. “self-driving” cars),
    computer security, ...
Taught: 149, 172, 144/244, 219C, EECS149.1x on edX, ...
Instructors

Jean Walrand – Prof. of EECS – UCB
257 Cory Hall – walrand@berkeley.edu

I was born in Belgium and came to Berkeley for my PhD. I have been teaching at UCB since 1982.

My wife and I live in Berkeley. We have two daughters (UC alumni – Go Bears!). We like to ski and play tennis (both poorly). We enjoy classical music and jazz.

My research interests include stochastic systems, networks and game theory.

(1)
Course Webpage: http://www.eecs70.org/

Explains policies, has office hours, homework, midterm dates, etc.

Two midterms, final.
  midterm 1 before drop date.
  midterm 2 before grade option change.

Questions/Announcements ⇒ piazza: 
piazza.com/berkeley/fall2016/cs70
Today: Note 1. (Note 0 is background. Do read/skim it.)

The language of proofs!

1. Propositions.
2. Propositional Forms.
3. Implication.
4. Truth Tables
5. Quantifiers
6. More De Morgan’s Laws
Propositions: Statements that are true or false.

\[
\begin{array}{ll}
\sqrt{2} \text{ is irrational} & \text{Proposition} \quad \text{True} \\
2 + 2 = 4 & \text{Proposition} \quad \text{True} \\
2 + 2 = 3 & \text{Proposition} \quad \text{False} \\
826\text{th digit of pi is 4} & \text{Proposition} \quad \text{False} \\
\text{Jon Stewart is a good comedian} & \text{Not a Proposition} \\
\text{All evens} > 2 \text{ are unique sums of 2 primes} & \text{Proposition} \quad \text{False} \\
4 + 5 & \text{Not a Proposition.} \\
x + x & \text{Not a Proposition.}
\end{array}
\]

Again: “value” of a proposition is ... True or False
Propositional Forms.

Put propositions together to make another...

Conjunction (“and”): $P \land Q$

“$P \land Q$” is True when both $P$ and $Q$ are True. Else False.

Disjunction (“or”): $P \lor Q$

“$P \lor Q$” is True when at least one $P$ or $Q$ is True. Else False.

Negation (“not”): $\neg P$

“$\neg P$” is True when $P$ is False. Else False.

Examples:

$\neg \text{“(2 + 2 = 4)”}$ – a proposition that is ... False

“2 + 2 = 3” $\land$ “2 + 2 = 4” – a proposition that is ... False

“2 + 2 = 3” $\lor$ “2 + 2 = 4” – a proposition that is ... True
Propositional Forms: quick check!

\[ P = \text{"}\sqrt{2} \text{ is rational"} \]
\[ Q = \text{"826th digit of pi is 2"} \]

\[ P \] is ... False .
\[ Q \] is ... True .

\[ P \land Q \] ... False
\[ P \lor Q \] ... True
\[ \neg P \] ... True
Propositions:

$P_1$ - Person 1 rides the bus.
$P_2$ - Person 2 rides the bus.

Suppose we can’t have either of the following happen: That either person 1 or person 2 ride the bus and person 3 or 4 ride the bus. Or that person 2 or person 3 ride the bus and that either person 4 ride the bus or person 5 doesn’t.

Propositional Form:

$$\neg(((P_1 \lor P_2) \land (P_3 \lor P_4)) \lor ((P_2 \lor P_3) \land (P_4 \lor \neg P_5)))$$

Who can ride the bus?
What combinations of people can ride the bus?

This seems ...complicated.

We need a way to keep track!
Truth Tables for Propositional Forms.

<table>
<thead>
<tr>
<th>$P$</th>
<th>$Q$</th>
<th>$P \land Q$</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$P$</th>
<th>$Q$</th>
<th>$P \lor Q$</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
</tbody>
</table>

One use for truth tables: Logical Equivalence of propositional forms!
Example: $\neg(P \land Q)$ logically equivalent to $\neg P \lor \neg Q$
...because the two propositional forms have the same...
....Truth Table!

<table>
<thead>
<tr>
<th>$P$</th>
<th>$Q$</th>
<th>$\neg(P \land Q)$</th>
<th>$\neg P \lor \neg Q$</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
</tbody>
</table>

DeMorgan’s Law’s for Negation: distribute and flip!

$\neg(P \land Q) \equiv \neg P \lor \neg Q$  
$\neg(P \lor Q) \equiv \neg P \land \neg Q$
Implication.

\[ P \implies Q \] interpreted as
If \( P \), then \( Q \).

True Statements: \( P, P \implies Q \).
Conclude: \( Q \) is true.

Example: Statement: If you stand in the rain, then you’ll get wet.

\[ P = \text{“you stand in the rain”} \]
\[ Q = \text{“you will get wet”} \]

Statement: “Stand in the rain”
Can conclude: “you’ll get wet.”
Non-Consequences/consequences of Implication

The statement “$P \implies Q$”

only is False if $P$ is True and $Q$ is False.

False implies nothing
$P$ False means $Q$ can be True or False
Anything implies true.
$P$ can be True or False when $Q$ is True

If chemical plant pollutes river, fish die.
If fish die, did chemical plant polluted river?

Not necessarily.

$P \implies Q$ and $Q$ are True does not mean $P$ is True

Instead we have:
$P \implies Q$ and $P$ are True does mean $Q$ is True.

Be careful out there!

Some Fun: use propositional formulas to describe implication?

$$((P \implies Q) \land P) \implies Q.$$
Implication and English.

\[ P \implies Q \]

- If \( P \), then \( Q \).
- \( Q \) if \( P \).
- \( P \) only if \( Q \).
- \( P \) is sufficient for \( Q \).
- \( Q \) is necessary for \( P \).
Truth Table: implication.

<table>
<thead>
<tr>
<th>$P$</th>
<th>$Q$</th>
<th>$P \implies Q$</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$P$</th>
<th>$Q$</th>
<th>$\neg P \lor Q$</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
</tbody>
</table>

$\neg P \lor Q \equiv P \implies Q$.

These two propositional forms are logically equivalent!
Contrapositive, Converse

- Contrapositive of $P \implies Q$ is $\neg Q \implies \neg P$.
  - If the plant pollutes, fish die.
  - If the fish don’t die, the plant does not pollute. (contrapositive)
  - If you stand in the rain, you get wet.
  - If you did not stand in the rain, you did not get wet. (not contrapositive!) converse!
  - If you did not get wet, you did not stand in the rain. (contrapositive.)

  Logically equivalent! Notation: $\equiv$.
  $$P \implies Q \equiv \neg P \lor Q \equiv \neg (\neg Q) \lor \neg P \equiv \neg Q \implies \neg P.$$ 

- Converse of $P \implies Q$ is $Q \implies P$.
  If fish die the plant pollutes.
  Not logically equivalent!

- Definition: If $P \implies Q$ and $Q \implies P$ is $P$ if and only if $Q$ or $P \iff Q$.
  (Logically Equivalent: $\iff$.)
Propositions?

- $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.
- $x > 2$
- $n$ is even and the sum of two primes

No. They have a free variable.

We call them predicates, e.g., $Q(x) = "x$ is even"

Same as boolean valued functions from 61A or 61AS!

- $P(n) = "\sum_{i=1}^{n} i = \frac{n(n+1)}{2}"$
- $R(x) = "x > 2"
- $G(n) = "n$ is even and the sum of two primes"

Next: Statements about boolean valued functions!!
There exists quantifier:

$(\exists x \in S)(P(x))$ means "$P(x)$ is true for some $x$ in $S$"

Wait! What is $S$?

$S$ is the **universe**: “the type of $x$”.

Universe examples include..

- $N = \{0, 1, \ldots\}$ (natural numbers).
- $Z = \{\ldots, -1, 0, 1, \ldots\}$ (integers)
- $Z^+$ (positive integers)
- See note 0 for more!
Quantifiers..

There exists quantifier:
\((\exists x \in S)(P(x))\) means "\(P(x)\) is true for some \(x\) in \(S\)"
For example:
\((\exists x \in N)(x = x^2)\)
Equivalent to "\((0 = 0) \lor (1 = 1) \lor (2 = 4) \lor \ldots\)"
Much shorter to use a quantifier!

For all quantifier;
\((\forall x \in S)(P(x))\). means “For all \(x\) in \(S\) \(P(x)\) is True .”
Examples:
“Adding 1 makes a bigger number.”
\((\forall x \in N) (x + 1 > x)\)
"the square of a number is always non-negative"
\((\forall x \in N)(x^2 \geq 0)\)
Quantifiers are not commutative.

Consider this English statement: "there is a natural number that is the square of every natural number", i.e. the square of every natural number is the same number!

\[(\exists y \in \mathbb{N}) \ (\forall x \in \mathbb{N}) \ (y = x^2)\]  False

Consider this one: "the square of every natural number is a natural number"...

\[(\forall x \in \mathbb{N})(\exists y \in \mathbb{N}) \ (y = x^2)\]  True
Consider
\[ \neg (\forall x \in S)(P(x)), \]
By DeMorgan’s law,
\[ \neg (\forall x \in S)(P(x)) \iff \exists (x \in S)(\neg P(x)). \]
English: there is an \( x \) in \( S \) where \( P(x) \) does not hold.
What we do in this course! We consider claims.

Claim: \( (\forall x) P(x) \) "For all inputs \( x \) the program works."
For False, find \( x \), where \( \neg P(x) \).
Counterexample.
Bad input.
Case that illustrates bug.
For True: prove claim. Next lectures...
Negation of exists.

Consider

$$\neg(\exists x \in S)(P(x))$$

Equivalent to:

$$\neg(\exists x \in S)(P(x)) \iff \forall x \in S \neg P(x).$$

English: means that for all $x$ in $S$, $P(x)$ does not hold.
Theorem: $\forall n \in \mathbb{N} \ (n \geq 3 \implies \neg(\exists a, b, c \in \mathbb{N} \ a^n + b^n = c^n))$

Which Theorem?

Fermat's Last Theorem!

Remember Right-Angled Triangles: for $n = 2$, we have 3,4,5 and 5,7, 12 and ... (Pythagorean triples)

1637: Proof doesn’t fit in the margins.

1993: Wiles ...(based in part on Ribet’s Theorem)

DeMorgan Restatement:
Theorem: $\neg(\exists n \in \mathbb{N} \exists a, b, c \in \mathbb{N} \ (n \geq 3 \land a^n + b^n = c^n))$
Summary.

Propositions are statements that are true or false.
Propositional forms use \( \land, \lor, \neg \).
The meaning of a propositional form is given by its truth table.
Logical equivalence of forms means same truth tables.

Implication: \( P \implies Q \iff \neg P \lor Q \).
Contrapositive: \( \neg Q \implies \neg P \)
Converse: \( Q \implies P \)

Predicates: Statements with “free” variables.
Quantifiers: \( \forall x \ P(x), \exists y \ Q(y) \)

Now can state theorems! And disprove false ones!

DeMorgans Laws: “Flip and Distribute negation”
\[ \neg(P \lor Q) \iff (\neg P \land \neg Q) \]
\[ \neg \forall x \ P(x) \iff \exists x \ \neg P(x). \]

Next Time: proofs!