Intro to Discrete Structures
Lecture 3

Pawel M. Wocjan

School of Electrical Engineering and Computer Science

University of Central Florida

`wocjan@eecs.ucf.edu`

Laws in Propositional Logic & Arithmetic

- Identity laws

$$p \wedge T \equiv p \qquad a \cdot 1 = a$$

$$p \vee F \equiv p \qquad a + 0 = a$$

- Commutative laws

$$p \wedge q \equiv q \wedge p \qquad a \cdot b = b \cdot a$$

$$p \vee q \equiv q \vee p \qquad a + b = b + a$$

Laws in Propositional Logic & Arithmetic

- Associative laws

$$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r) \qquad a \cdot (b \cdot c) = a \cdot (b \cdot c)$$

$$(p \vee q) \vee r \equiv p \vee (q \vee r) \qquad a + (b + c) = a + (b + c)$$

- Distributive laws

$$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r) \qquad a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$

$$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r) \qquad a + (b \cdot c)$$

Further Laws in Propositional Logic

- Domination laws

$$
\begin{aligned}
p \vee T &\equiv T \\
p \wedge F &\equiv F
\end{aligned}
$$

- Idempotent laws

$$
\begin{aligned}
p \vee p &\equiv p \\
p \wedge p &\equiv p
\end{aligned}
$$

- Double negation

$$\neg\neg p \equiv p$$

Further Laws in Propositional Logic

- De Morgan laws

$$\begin{aligned}\neg(p \wedge q) &\equiv \neg p \vee \neg q \\ \neg(p \vee q) &\equiv \neg p \wedge \neg q\end{aligned}$$

- Absorption laws

$$\begin{aligned}p \vee (p \wedge q) &\equiv p \\ p \wedge (p \vee q) &\equiv p\end{aligned}$$

- Negation laws

$$\begin{aligned}p \vee \neg p &\equiv T \\ p \wedge \neg p &\equiv F\end{aligned}$$

300

Which of the following two compound propositions

$$(G \to S) \vee (G \to J)$$

$$G \to (S \vee J)$$

is the correct translation of “Greeks carry Swords or Javelins”

$$E\lambda\lambda\eta\nu\epsilon s\ \kappa\rho\alpha\tau\alpha\nu\epsilon\ \sigma\pi\alpha\theta\iota\alpha\ \eta\ \alpha\kappa o\nu\tau\iota\alpha.$$

into propositional logic?

300

It turns out that both compound propositions are equivalent.

How do we show that? One approach is via building the truth table and comparing the corresponding columns.

Let's do something fancier.

First, convince yourself that the following laws are correct:

$p \to q$	$\equiv$	$\neg p \vee q$	implication in terms of or	(impl-or)
$p \vee q$	$\equiv$	$q \vee p$	commutative law	(comm)
$p \vee p$	$\equiv$	p	idempotent law	(idem)
$p \vee (q \vee r)$	$\equiv$	$(p \vee q) \vee r$	associative law	(ass)

300

Second, apply these laws in a 'smart' way:

$$(G \longrightarrow S) \vee (G \longrightarrow J)$$

apply the law

$$\begin{array}{rcl}
\text{impl-or} & \equiv & (\neg G \vee S) \vee (\neg G \vee J) \\
\text{ass} & \equiv & \neg G \vee S \vee \neg G \vee J \\
\text{comm} & \equiv & \neg G \vee \neg G \vee S \vee J \\
\text{idem} & \equiv & \neg G \vee S \vee J \\
\text{ass} & \equiv & \neg G \vee (S \vee J) \\
\text{impl-or} & \equiv & G \longrightarrow (S \vee J) \quad \Box
\end{array}$$

Contraposition

- The logical equivalence

$$p \rightarrow q \quad \equiv \quad \neg q \rightarrow \neg p$$

is called contraposition. It is at the heart of the proof technique “Proof by contradition” (more on proofs later).

Logic and Bit Operations

- Decimal numbers

$$134 = 1 \cdot 10^2 + 3 \cdot 10^1 + 4 \cdot 10^0$$

$$\begin{aligned} d_{n-1} \ldots d_1 d_0 &= d_{n-1} \cdot 10^{n-1} + \ldots + d_1 \cdot 10^1 + d_0 \cdot 10^0 \\ &= \sum_{j=0}^{n-1} d_j \cdot 10^j \,, \quad d_j \in \{0, \ldots, 9\} \end{aligned}$$

Logic and Bit Operations

- Binary numbers

$$
\begin{aligned}
10000110 &= 1 \cdot 2^7 + 1 \cdot 2^2 + 1 \cdot 1 \cdot 2^1 \\
b_{m-1} \dots b_1 b_0 &= b_{n-1} \cdot 2^{m-1} + \dots + b_1 \cdot 2^1 + b_0 \cdot 2^0 \\
&= \sum_{k=0}^{m-1} b_k \cdot 2^k\,, \quad b_k \in \{0, 1\}
\end{aligned}
$$

Bit Operators OR, AND, and XOR

- Identify T with 1 and F with 0

x	y	$x \vee y$	$x \wedge y$	$x \oplus y$
0	0	0	0	0
0	1	1	0	1
1	0	1	0	1
1	1	1	1	0

Adding Binary Numbers

- How can we add two m-bit numbers $x = x_{m-1} \ldots x_1 x_0$ and $y = x_{m-1} \ldots x_1 x_0$?
- Express the sum $z = z_m z_{m-1} \ldots z_1 z_0$ in terms of the bits of x and y.

Half adder

- Let us start with the LSB (least significant bit):

x_0	0	0	1	1
y_0	0	1	0	1
c_0z_0	00	01	01	10

- Express the carry-bit c_0 and z_0 in terms of x_0 and y_0.

Half adder

- Let us start with the LSB (least significant bit):

x_0	0	0	1	1
y_0	0	1	0	1
$c_0 z_0$	00	01	01	10

- Express the carry-bit c_1 and z_0 in terms of x_0 and y_0:
  - $c_1 = x_0 \wedge y_0$
  - $z_0 = x_0 \oplus y_0$

Full adder

- Consider the kth bit where $k > 1$ (that is, not the LSB)

c_k	0	0	0	0	1	1	1	1
x_k	0	0	1	1	0	0	1	1
y_k	0	1	0	1	0	1	0	1
$c_{k+1}z_k$	00	01	01	10	01	10	10	11

- Express c_{k+1} and z_k in terms of c_k, x_k, and y_k:

Full adder

- Consider the kth bit where $k > 1$ (that is, not the LSB)

c_k	0	0	0	0	1	1	1	1
x_k	0	0	1	1	0	0	1	1
y_k	0	1	0	1	0	1	0	1
$c_{k+1}z_k$	00	01	01	10	01	10	10	11

- Express c_{k+1} and z_k in terms of c_k, x_k, and y_k:
  - $c_{k+1} = (c_k \wedge x_k) \vee (c_k \wedge y_k) \vee (x_k \wedge y_k)$
  - $z_k = c_k \oplus x_k \oplus y_k$

I. Indiana Jones / Indiana Janet

- On your quest for the Grail of Eternal Truth, you enter the Chamber of Propositional Logic in the Temple of Logic.
- There are three statues of the Egyptian deities Thoth (Baboon), Ra (Hawk), and Anubis (Jackal) on the altar in front of you.
- Based upon the inscriptions on the statues, you have to determine the statue under which the key to the Chamber of Predicate Logic is hidden.

II. Indiana Jones / Indiana Janet

- Having deciphered the hieroglyphs of the ancient (and very expensive) text “Intro to Discrete Mathematics” by the evil high priest Rosen, you know that none or just one of the inscriptions is true:
  - Thoth: The key is here.
  - Ra: The key is not here.
  - Anubis: The key is not under Thoth’s statue.
- If you do not pick up the correct statue within five minutes, the floor will crumble and you will fall into a pit with ferocious crocodiles. Hurry up, the water of the clepsydra is already dripping ...

III. Indiana Jones / Indiana Janet

- It turns out that the high priest is more evil that you anticipated. A new challenge awaits you in the chamber to which you just gained access. This time at least one of the inscriptions is true and at least one of them is false:
  - Thoth: The key is not under Ra's statue.
  - Ra: The key is not here.
  - Anubis: The key is not here.
- Solve this challenge whenever you want.

1.3. Predicates and Quantifiers

A declarative sentence is a **predicate** if

- it contains one or more variables, and
- it is not a proposition, but
- it becomes a proposition when the variables in it are replaced by certain by certain allowable choices.

The allowable choices constitute what is called the **universe** or the **domain** (or **universe of discourse** or **domain of discourse**) for the predicate.

Predicates

- When we examine the sentence "The number $x + 2$ is greater than 1" in light of this definition, we find that it is a predicate that contains the single variable x.
- The universe could be the natural numbers $\mathbb{N}$, the integers $\mathbb{Z}$, the rational numbers $\mathbb{Q}$, or the real numbers $\mathbb{R}$.
- We choose the universe to be $\mathbb{R}$.
- Let us use $P(x)$ as a short hand notation for "The number $x + 2$ is strictly greater than 1."
- Determine the truth values of $P(-\sqrt{2})$ and $P(-0.5)$.

Predicates

- Recall that $P(x)$ denotes the predicate “The number $x + 2$ is strictly greater than 1.”
- We have $-\sqrt{2} + 2 \leq 1$, so the truth value of $P(-\sqrt{2})$ is F.
- We have $-0.5 + 2 = 1.5 > 1$, so the truth value of $P(-0.5)$ is T.

Predicates

- Let $Q(x, y)$ denote the predicate "$x = y + 3$." Let the universe $\mathbb{N} \times \mathbb{N}$, that is, pairs of natural numbers.
- Determine the truth values of
  - $Q(1, 2)$
  - $Q(3, 0)$

Predicates

- Let $Q(x, y)$ denote the predicate "$x = y + 3$." Let the universe $\mathbb{N} \times \mathbb{N}$, that is, pairs of natural numbers.
- Determine the truth values of
  - $Q(1, 2)$
  - $Q(3, 0)$
- The truth value of
  - $Q(1, 2)$ is F since $1 \neq 2 + 3 = 5$
  - $Q(3, 0)$ is T since $3 = 0 + 3$.

n-ary Predicates

- In general, a predicate involving the n variables $x_1, x_2, \ldots, x_n$ can be denoted by

$$P(x_1, x_2, \ldots, x_n)$$

- P is called a n-**place predicate** or a n-**ary predicate**.
- P is also refered to as a **propositional function**.

Predicate Calculus

- When the variables in a predicate are assigned values, the resulting statement becomes a proposition with a certain truth value.
- **Quantification** is another important way to create a proposition from a predicate.
- Quantification expresses the extent to which a predicate is true over a range of elements. In English, the words *all*, *some*, *many*, *none*, and *few* are used in quantification.
- We focus on **universal** and **existential** quantification. The area of logic that deals with predicates and quantifiers is called **predicate calculus**.

Universal Quantification

Definition 1:

- The **universal quantification** of $P(x)$ is the statement

  "$P(x)$ for all the values of x in the domain."

- The notation $\forall x\, P(x)$ denotes the universal quantification of $P(x)$.
- Here $\forall$ is called the **universal quantifier**.
- We read $\forall x\, P(x)$ as "for all $xP(x)$" or "for every $xP(x)$.
- An element for which $P(x)$ is false is called a **counterexample** of $\forall x P(x)$.

Existential Quantification

Definition 2:

- The **existential quantification** of $P(x)$ is the statement

  "There exists an element x in the domain such that $P(x)$."

- The notation $\exists x\, P(x)$ denotes the existential quantification of $P(x)$.

- Here $\exists$ is called the **existential quantifier**.

Universal vs. Existential

	When true?	When false?
$\forall x P(x)$	$P(x)$ is true for every x.	There is an x for which $P(x)$ is false.
$\exists x P(x)$	There is an x for which $P(x)$ is true.	$P(x)$ is false for every x.

Universal vs. Existential

- Let $Q(x)\ :x < 0$.
- Assume that the domain of Q is the set of **integers** $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \ldots\}$.
- Determine the truth values of $\forall x\, Q(x)$ and $\exists x\, Q(x)$:

Universal vs. Existential

- Let $Q(x)\ : x < 0$.
- Assume that the domain of Q is the set of **integers** $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \ldots\}$.
- Determine the truth values of $\forall x\, Q(x)$ and $\exists x\, Q(x)$:
  - $\forall x\, Q(x)$ is F.

    A counterexample for $\forall x\, Q(x)$ is 1 since $Q(1)$ is F ($1 \not< 0$).
  - $\exists x\, Q(x)$ is T.

    For example, $Q(x)$ is T for $x = -2$ ($-2 < 0$).

Universal vs. Existential

- Let $Q(x) \, : x < 0$.
- Assume that the domain of Q is the set of **natural numbers** $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$.
- Determine the truth values of $\forall x \, Q(x)$ and $\exists x \, Q(x)$:

Universal vs. Existential

- Let $Q(x)\ : x < 0$.
- Assume that the domain of Q is the set of **natural number** $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$.
- Determine the truth values of $\forall x\, Q(x)$ and $\exists x\, Q(x)$:
  - $\forall x\, Q(x)$ is still F.

    A counterexample for $\forall x\, Q(x)$ is 1 since $Q(1)$ is F ($1 \not< 0$).
  - But $\exists x\, Q(x)$ becomes F when we change the domain from $\mathbb{Z}$ to $\mathbb{N}$!

    There does not exist an element $x \in \mathbb{N}$ such that $x < 0$ (since 0 is the smallest number in $\mathbb{N}$).

Empty Domains

- Generally, an implicit assumption is made that the domains of discourse for quantifiers are nonempty.
- If the domain is empty, then
  - $\forall x\, Q(x)$ is T for any predicate Q since there are no elements x in the domain for which $P(x)$ is F.
  - $\exists x\, Q(x)$ is F for any predicate Q because when the domain is empty, there can be no element in the domain for which $P(x)$ is T.

Finite Domains

- Assume the domain of the predicate $P(x)$ is **finite** – say, its elements are $v_1, \ldots, v_m$.
  - $\forall x\, P(x)$ is the same as the conjuction

    $$P(v_1) \wedge P(v_2) \wedge \cdots \wedge P(v_m)$$

    because this conjuction is true if and only if $P(v_1)$, $P(v_2)$, . . . , $P(v_m)$ are all true.
  - What compound proposition does $\exists x\, P(x)$ correspond to?

Finite Domains

- Assume the domain of the predicate $P(x)$ is **finite** – say, its elements are $v_1, \ldots, v_m$.
  - $\forall x\, P(x)$ is the same as the conjuction

    $$P(v_1) \wedge P(v_2) \wedge \cdots \wedge P(v_m)$$

    because this conjuction is true if and only if $P(v_1)$, $P(v_2)$, . . . , $P(v_m)$ are all true.
  - $\exists x\, P(x)$ is the same as the disjuction

    $$P(v_1) \vee P(v_2) \vee \cdots \vee P(v_m)$$

  because this disjuction is true if and only if at least one of $P(v_1)$, $P(v_2)$, . . . , $P(v_m)$ is true.

Precedence of Quantifiers

- The quantifiers $\forall$ and $\exists$ have a higher precedence then all logical operators from propositional calculus.
- For example,
$$\forall x\, P(x) \vee Q(x)$$
means
$$\big(\forall x\, P(x)\big) \vee Q(x)$$
rather than
$$\forall x\, \big(P(x) \vee Q(x)\big)\,.$$

Binding Variables

- When a quantifier is used on the variable x, we say that this occurence of the variable is **bound**.
- An occurence of a variable that is not bound by a quantifier or set equal to a particular value is said to be **free**.
- All variables that occur in a predicate must be bound or set equal to a particular value to turn it into a proposition.

  This can be done by a combination of $\forall$, $\exists$, and value assignments.
- The part of a logical expression to which a quantifier is applied is called the **scope** of this quantifier.

Binding Variables – Examples

- $$\exists x(x + y = 1)$$

  - The variable x is bound by the existential quantifier.
  - The variable y is free because it is not bound by a quantifier and no value is assigned to this variable.

Binding Variables – Examples

- $$\exists x \big(P(x) \wedge Q(x) \big) \vee \forall x R(x)$$

  - All variables are bound.
  - The scope of the first quantifier, $\exists x$, is the expression $P(x) \wedge Q(x)$.
  - The scope of the second quantifier, $\forall x$, is the expression $R(x)$.

    We could have written the above expression using two different variables x and y as

    $$\exists x \big(P(x) \wedge Q(x) \big) \vee \forall y R(y)$$

    because the scopes do not overlap.