מתמטיקה בדידה

Discrete Math

Lecture 2

Last Week: Propositions

<u>Definition</u>: A proposition is a statement that is either TRUE or FALSE.

We can combine propositions using logical (Boolean) operators:

$\wedge$:= AND

$\vee$:= OR

$\neg$:= NOT

$\rightarrow$:= IMPLIES (if… then)

Last Week: Truth Tables

Indicate the true/false value of a proposition for each possible setting of its variables

Example:

P	Q	P implies Q
T	T	T
T	F	F
F	T	T
F	F	T

An implication is true exactly when:

1. the if-part is false or
2. the then-part is true

$\neg P \vee Q$

Last Week: Equivalence

$(P \rightarrow Q)$ and $(\neg P \vee Q)$ are <u>logically equivalent</u>.

$$(P \rightarrow Q) \equiv (\neg P \vee Q)$$

<u>Definition</u>: Two propositional formulas are <u>equivalent</u> if and only if they have the same truth value for all assignments of their variables

Assignment	הצבה
Equivalent	שקול

Example: Logical Distributive Law

Proposition: $P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$

(Just like $x(y+z) = xy + xz.$)

Distributive law חוק הפילוג

Proof: Logical Distributive Law

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

n

2^n

P	Q	R	Q ∨ R	P ∧ Q	P ∧ R	P ∧ (Q ∨ R)	(P ∧ Q) ∨ (P ∧ R)
T	T	T	T	T	T	T	T
T	T	F	T	T	F	T	T
T	F	T	T	F	T	T	T
T	F	F	T	F	F	F	F
F	T	T	T	F	F	F	F
F	T	F	T	F	F	F	F
F	F	T	T	F	F	F	F
F	F	F	F	F	F	F	F

Logical Deduction

Modus Ponens (sound):

$$\frac{(P \rightarrow Q),\ P}{Q}$$

P	Q	P implies Q
T	T	T
T	F	F
F	T	T
F	F	T

Contrapositive (sound):

$$\frac{(\neg Q \rightarrow \neg P)}{(P \rightarrow Q)}$$

Converse (not sound):

$$\frac{(P \rightarrow Q)}{(Q \rightarrow P)}$$

בחנו את עצמכם

Claim: Let $x \in \mathbb{Z}$, and suppose that x^2 is even (that is, $x^2=2y$ for some $y \in \mathbb{Z}$. Then x is even.

Hint: Assume that $x=2z+1$ for some $z \in \mathbb{Z}$.

Proof: On the board.

Another Sound Rule

$$(\neg P \rightarrow F) \equiv (T \rightarrow P)$$

$$\overline{}$$

$$P$$

Q	P	Q implies P
T	T	T
T	F	F
F	T	T
F	F	T

Proof by Contradiction

To prove proposition P:

1. Prove that “(not P) implies F.”
2. Write, “Assume not P.”
3. Show that F logically follows.

Contradiction	סתירה
Proof by contradiction	הוכחה בדרך השלילה

Example: Proof by Contradiction

<u>Theorem</u>: $\sqrt{2}$ is irrational

<u>Proof</u>: By contradiction. On the board.

Summary: Proof Methods

<u>Last week</u>

1. Proving implication
   a) Direct proof
   b) Contrapositive
2. If and only if
3. By comparing truth tables

<u>Today</u>

1. By contradiction

Predicate Logic

Predicates

Predicates are propositions with variables.

Examples:

$P(n) :=$ "n is a square"

$n = 4$: $P(4) = T$

$n = 5$: $P(5) = F$

$P(x,y) := [x+2 = y]$

$x=1$ and $y=3$: $P(1,3) = T$

$x=1$ and $y=4$: $P(1,4) = F$

$\neg P(1,4) = T$

$P(x,y) :=$ "x^y is rational"

$x=2/3$ and $y=2$: $P(2/3,2) = T$

$x=\sqrt{2}$ and $y=1$: $P(\sqrt{2},1) = F$

Predicates

Some predicates are sometimes true and some predicates are always true.

For example:

The predicate $P(x) := [x^2 \geq 0]$ is always true (when x is a real number).

The predicate $P(x) := [5x^2-7=0]$ is sometimes true (only when $x=\pm\sqrt{7/5}$)

Quantifiers in English

Always true

For all x, P(x) is true

P(x) is true for every x

For all x, $x^2 \geq 0$

$x^2 \geq 0$ for every x

Sometimes true

There exists an x s.t. P(x) is true

P(x) is true for some x

P(x) is true for at least one x

There exists an x s.t. $5x^2 - 7 = 0$

$5x^2 - 7 = 0$ for some x

$5x^2 - 7 = 0$ for at least one x

Quantifier כמת

Quantifiers

$\forall$**x for ALL x.**

A predicate P is true for all values x in some set D:

$$\forall x \in D, P(x)$$

$\exists$**y there EXISTS some y**

A predicate P is true for at least one value of y in D:

$$\exists y \in D, P(y)$$

For all	לכל
There exists	קיים
Domain	תחום

Mixing Quantifiers

Example:

Goldbach's conjecture: Every even integer greater than 2 is the sum of two primes.

For every integer n greater than 2, there exist primes p and q such that n=p+q.

`Evens` **– even numbers greater than 2.**

`Primes` **– Prime numbers.**

$$\forall n \in \texttt{Evens}\ \exists p,q \in \texttt{Primes},\ n=p+q.$$

Mixing Quantifiers

x,y range over *domain of discourse*

$\forall x\ \exists y,\ x < y$

Domain	Truth value
Integers $\mathbb{Z}$	True
Positive integers $\mathbb{Z}^+$	True
Negative integers $\mathbb{Z}^-$	False
Negative rationals $\mathbb{Q}^-$	True

Swapping Quantifiers

Swapping quantifier may totally change the meaning of a proposition:

$$\forall \mathbf{n} \in \mathrm{Evens}\ \ \exists \mathbf{p,q} \in \mathrm{Primes}, \mathbf{n=p+q}.$$

$$\exists \mathbf{p,q} \in \mathrm{Primes}\ \ \forall \mathbf{n} \in \mathrm{Evens}, \mathbf{n=p+q}.$$

The second proposition is clearly false!

Small Question

If we raise an irrational number to an irrational number can the result be irrational?

Write corresponding proposition in logic notation.

`Rationals` **– Rational numbers.**

`Irrationals` **– Irrational Numbers.**

<u>Proposition</u>:

$$\exists \mathbf{x},\mathbf{y} \in \texttt{Irrationals}, \mathbf{x}^{\mathbf{y}} \in \texttt{Rationals}$$

<u>True or False</u>?

$$\forall \mathbf{x} \in \texttt{Irrationals}\ \exists \mathbf{y} \in \texttt{Rationals}, \mathbf{x}^{\mathbf{y}} \in \texttt{Irrationals}$$

$\forall\exists$ versus $\exists\forall$

$\forall$ a $\in$ ATTACK $\exists$ d $\in$ DEFENSE

d protects against a

For every attack, I have a defense:

Against MYDOOM,	use Defender
Against ILOVEYOU,	use Norton
Against BABLAS,	use ZoneAlarm…

$\forall\exists$ is expensive!

$\exists\forall$

$\exists$**d** $\in$ **DEFENSE** $\forall$**a** $\in$ **ATTACK**

d protects against a

It's more efficient to have *one* defense that is good against *every* attack

Negating Quantifiers

"It is not the case that everyone likes to snowboard"

"There exists someone who does not like to snowboard"

$$\neg\forall x, P(x) \text{ is equivalent to } \exists x, \neg P(x)$$

"There does not exist anyone who likes skiing over magma"

"Everyone dislikes skiing over magma"

$$\neg\exists x, Q(x) \equiv \forall x, \neg Q(x)$$

Principle: moving a "not" across a quantifier changes the kind of quantifier.

Sets and Sequences

What is a Set?

Informally: A set is a collection of objects, which are called the elements of the set.

Elements can be anything:

1. numbers
2. names
3. other sets

Set	קבוצה
Element	אבר

Some Sets

Set	Symbol	Elements
Natural numbers	$\mathbb{N}$	{0,1,2,3,…}
Integers	$\mathbb{Z}$	{…,-3,-2,-1,0,1,2,3,…}
Rational numbers	$\mathbb{Q}$	1/2, -5/3, 16, etc.
Real numbers	$\mathbb{R}$	$\pi, e, -9, \sqrt{2}$ etc.
Complex numbers	$\mathbb{C}$	$i, \frac{19}{2}, \sqrt{2} - 2i$ etc.
Empty set	Φ	None

Empty set קבוצה ריקה

Some More Sets

A = {Alice, Charlie, Bob, Eve}	people
B = {red, blue, yellow}	colors
C = {{a,b},{a,c},{b,c}}	a set of sets
D = {1,2,4,8,16,…}	the powers of 2

E = {7, "Alon R.", $\pi/2$, T} a set with 4 elements: two numbers, a string, and a Boolean value.

Order doesn't matter: A = {Alice, Charlie, Bob, Eve} is the same as A = {Eve, Alice, Bob, Charlie}.

Membership

<u>Notation</u>: x $\in$ A

<u>Terminology</u>: x is an element of A

x belongs to A

x is in A

<u>Examples</u>:

$\pi/2 \in$ {7, "Alon R.", $\pi/2$, T}

$\pi/3 \notin$ {7, "Alon R.", $\pi/2$, T}

14/2 $\in$ {7, "Alon R.", $\pi/2$, T}

"14/2" $\notin$ {"7", "Alon R.", $\pi/2$, T}

2/3 $\notin \mathbb{Z}$

Membership שייכות

In or not In?

An element is in or not in a set:

$\{7, \pi/2, 7\}$ is the same as $\{7, \pi/2\}$.

A set must be well defined. It should be totally clear what is an element in the set and what is not an element in the set.

Well defined מוגדר היטב

Quick Question

Does the following make sense?

$$\forall \mathbf{x} \in \neg\mathbb{Q}$$

NO! $\mathbb{Q}$ is a set!

Should write:

$$\forall \mathbf{x} \notin \mathbb{Q}$$

Containment (הכלה)

<u>Definition 1</u>: A is <u>contained</u> in B if and only if every element of A is also an element of B.

That is, $\forall x,\ \ x \in A \rightarrow x \in B$

Containment II

Notation: A $\subseteq$ B

Terminology: A is a **subset** of B

A is **contained** in B

Examples:

{{a,b},{a,c}} $\subseteq$ {{a,b},{a,c},{b,c}}

$\mathbb{R} \not\subseteq \mathbb{Q}$ A $\subseteq$ A $\mathbb{Z} \subseteq \mathbb{R}$

$\mathbb{R} \subseteq \mathbb{C}$ $\mathbb{C} \not\subseteq \mathbb{Z}$ {3} $\subseteq$ {5,7,3}

$\Phi \subseteq$ every set

subset תת-קבוצה

Strict Containment (הכלה ממש)

Definition 2: A is strictly contained in B iff:

1. every element of A is also an element of B,
2. there exists an element of B that is not an element of A.

That is:

1. $\forall x,\ \ x \in A \rightarrow x \in B$
2. $\exists x \in B, x \notin A$

Strict Containment II

Notation: $A \subset B$, $A \subsetneq B$

Terminology: A is a **strict subset** of B

A is **strictly contained** in B

Examples: $\{1,2\} \subset \{1,2,3\}$ $\mathbb{Q} \subset \mathbb{R}$ $\Phi \subset \{1\}$

Containment vs. Membership

Be careful not to confuse containment ($A \subseteq B$) with membership ($a \in A$).

<u>Examples</u>:

`Evens` **is a subset of** $\mathbb{N}$.

`Evens` **is not a member of** $\mathbb{N}$ **!**

`Jews` $\subseteq$ `Humans` "היהודים הם בני אדם"

`Jews` $\in$ `People` "היהודים הם עם ככל העמים"

Equality (שוויון)

<u>Definition</u>: Set A is <u>equal</u> to set B if and only if they have the same elements.

That is, $(A \subseteq B)\ AND\ (B \subseteq A)$

<u>Notation</u>: A=B

Complement of a Set

Definition 3: The complement of A is the set of all elements not in A.

Assumption: $A \subseteq \mathcal{U}$, where $\mathcal{U}$ is some universal set.

Notation: $\overline{A}$, A^c

Example: $\overline{\mathbb{R}^+} = \mathbb{R}^- \cup \{0\}$

complement	משלים
universal set	קבוצה אוניברסלית/היקום לצורך הדיון

The Empty Set

Definition 4: A set that does not have any elements is called empty.

There is a unique empty set, which we denote by Φ.

(Uniqueness of Φ follows from the fact that A=B if and only if A and B have the same elements.)

Empty set קבוצה ריקה

Power Set

<u>Definition 5</u>: The <u>power set</u> of a set A is the collection of all the subsets $S \subseteq A$.

<u>Notation</u>: P(A)

If A has n elements then P(A) has 2^n elements.

Power set קבוצת חזקה

Power Set: examples

- The elements of P({1,2}) are Φ,{1},{2}. And {1,2}
- P({a,b}) = {{a,b}, {a}, {b}, Φ}.

<u>Question</u>: What is P(Φ)?

<u>Answer</u>: {Φ}

<u>Question</u>: What is P(P(Φ))?

<u>Answer</u>: {{Φ}, Φ}