37181 DISCRETE MATHEMATICS

Lecture 2: more on logic

PLAN

- quantified statements
- negation of quantified statements
- SAT and P=?NP

Statements can contain *variables*.

Eg:

- $P(x)$: "the number x is greater than or equal to 3"
- $Q(x)$: "x lives in Queensland"

"$x \geqslant 3$"

VARIABLES

Statements can contain *variables*.

$\mathbb{N}$ natural numbers 0, 1, 2, 3

Eg:

- $P(x)$: "the number x is greater than or equal to 3"
- $Q(x)$: "x lives in Queensland"

The *universe of discourse* is the set of objects over which the statement could be defined.

real numbers

- for $P(x)$ the universe of discourse could be $\mathbb{R}$ or $\mathbb{Z}$ or $\mathbb{N}$ (we would need to be told)

integers −1, 0, 1, 2

- for $Q(x)$ the universe might be all people, or all students at QUT.

there is

We have the symbols $\forall$ ="for all" and $\exists$ ="there exists".

Eg: Let the universe of discourse be $\mathbb{Z}$.

strictly

- $\forall x, x^2 > x$ reads as "for all integers x, x^2 is greater than x"

quantifier

Is this true? NO : because

$x = 0$ $\quad 0^2 \not> 0$

$x = 1$ $\quad 1^2 = 1 \not> 1$

only need to give one example.

We have the symbols $\forall$ = "for all" and $\exists$ = "there exists".

Eg: Let the universe of discourse be $\mathbb{Z}$.

- $\forall x, x^2 > x$ reads as "for all integers x, x^2 is greater than x"

  Is this true?

- $\exists x, x^2 \leqslant x$ reads as "there exists (there is) some integer x whose square is smaller than or equal to itself"

  Is this true?

Yes $x = 0$

(or $x = 1$)

Rather than say " Let the universe of discourse be" we often hide this (make it *implicit*), or write

- $\forall x \in \mathbb{Z}, x^2 > x$

in

set of integers

PRACTICE

Let $B(x)$ be the statement "x lives in Bondi".

Let $C(x)$ be the statement "x lives in Cabramatta".

PRACTICE

Let $B(x)$ be the statement "x lives in Bondi".

Let $C(x)$ be the statement "x lives in Cabramatta".

Write these in symbols:

Let the universe of discourse be all UTS students.

- "All UTS students live in Bondi"

$$\boxed{\forall x,\ B(x).}$$

- "All UTS students either live in Cabramatta or do not live in Bondi"

$$\forall x \left(C(x) \vee \neg B(x) \right)$$

Can you work out, *intuitively* what the meaning of

- $\neg(\forall x, B(x))$

is?

Its not the case that all UTS students live in Bondi.

Equivalent to saying:

$$\exists x \ \neg B(x).$$

Formally, to negate a quantified statement you switch ∀ and ∃ at the front, then negate the proposition.

$$\neg(\forall x P(x)) = \exists x \neg P(x)$$

$$\neg(\exists x P(x)) = \forall x \neg P(x)$$

$\forall x \left(B(x) \wedge \neg C(x) \wedge \ldots \right)$

PRACTICE

Check the course notes, and Week 1 homework sheet, to practice turning English sentences into symbolic statements, and backwards, and negating them.

SAT = satisfiability

3-SAT is the following problem: on input an expression of the form

$$(x_1 \vee y_1 \vee z_1) \wedge (x_2 \vee y_2 \vee z_2) \wedge \ldots \wedge (x_n \vee y_n \vee z_n)$$

where x_i, y_i, z_i are propositions p or $\neg p$, answer yes or no: there is some assignment of truth values to the variables which makes the whole statement true.

~~$x_1 \to 0$ $x_2 \to$~~

For example

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

$p = 1$
$q = 1$
$r = 0$

yes, this input is satisfiable.

SAT

3-SAT is the following problem: on input an expression of the form

$$(x_1 \vee y_1 \vee z_1) \wedge (x_2 \vee y_2 \vee z_2) \wedge \ldots (x_n \vee y_n \vee z_n)$$

where x_i, y_i, z_i are propositions p or $\neg p$, answer yes or no: there is some assignment of truth values to the variables which makes the whole statement true.

For example

1 1 0 → 0

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

If I tell you a particular truth assignment, like $p = 0, q = 1, r = 0$ etc, you can easily compute (in a number of steps polynomial in n) the truth value of the statement.

eg $p = 0$, $q = 1$, $r = 0$.

If an instance of a solution can be *verified* in polynomial time (number of steps), we say a problem is in NP.

"EASY"

If a solution can be found in polynomial time (number of steps), we say the problem is in *P*.

"NOT SO EASY"

p	q	r
1	1	1
1	1	0
1	0	1
1	0	0
...		

— 3 variable

2^3 — exponential.

SAT

If an instance of a solution can be *verified* in polynomial time (number of steps), we say a problem is in NP.

If a solution can be found in polynomial time (number of steps), we say the problem is in *P*.

No-one knows if you can always find a truth assignment, or show there is none, making a general 3-SAT expression true, in polynomially many steps. If you can, you will get $1M

3-SAT is an important problem, even though it may seem abstract and useless, because Cook and Levin showed that every other candidate to solve the P=NP problem is related to this one. (Keyword: NP-complete)

?

COMING UP

In your tutorial class Wednesday/Thursday/Friday, lots of practice to fully understand the content presented in lectures 1-2.

After the workshop, do the homework sheet to consolidate your learning, and be ready for the uncoming quizzes.

Next lecture:

- proof methods: direct, contrapositive, contradiction