CSC165 fall 2017

Mathematical expression: predicate logic

Danny Heap
csc16517f@cs.toronto.edu
BA4270 (behind elevators)
Web page:
http://www.teach.cs.toronto.edu/~heap/165/F17/
416-978-5899

Using Course notes: Mathematical Expression: predicate logic

Outline

compare and contrast...

"If it rains, then I will wear sneakers."

"If and only if it rains, then I will wear sneakers."

what's a predicate?

$n > 7.2$

x is tall

predicate definitions

quantifiers $\forall$ and $\exists$

$n > 7.2$

translate quantified predicates

quantified binary predicates

$x + y = 17$

multiple quantifier examples

order matters!

$x + y = 17$

$\exists$: examples

$\forall$: lack of counterexamples

negate quantified predicates

① $\forall x \in \mathbb{Z}, \exists y \in \mathbb{Z}, x+y=17$

② $\exists y \in \mathbb{Z}, \forall x \in \mathbb{Z}, x+y=17$

$\neg(\exists y \in \mathbb{Z}, \forall x \in \mathbb{Z}, x+y=17)$

$\forall y \in \mathbb{Z}, \neg(\forall x \in \mathbb{Z}, x+y=17)$

$\forall y \in \mathbb{Z}, \exists x \in \mathbb{Z}, \neg(x+y=17)$

$\forall y \in \mathbb{Z}, \exists x \in \mathbb{Z}, x+y \neq 17$

Suppose we have predicates $P(x)$, $Q(x)$

$\neg(\neg P(x)) \longrightarrow P(x)$

$\neg(P(x) \wedge Q(x)) \equiv \neg P(x) \vee \neg Q(x)$ } DMZ

$\neg(P(x) \vee Q(x)) \equiv \neg P(x) \wedge \neg Q(x)$

$\neg(P(x) \Rightarrow Q(x)) \equiv P(x) \wedge \neg Q(x)$

$|||$

$\neg(\neg P(x) \vee Q(x)) \equiv P(x) \wedge \neg Q(x)$

$P \Leftrightarrow Q \equiv P \Rightarrow Q \wedge Q \Rightarrow P$

Computer Science
UNIVERSITY OF TORONTO

manipulate negation

$\neg(\forall x \in \mathbb{N}, \exists y \in \mathbb{N}, x \geq 5 \vee x^2 - y \geq 30)$

$\exists x \in \mathbb{N}, \forall y \in \mathbb{N}, x < 5 \wedge x^2 - y < 30$

properties of integers, mostly $\mathbb{N}$ – Number Theory

– encryption

RSA

d divides n : "$\exists k \in \mathbb{Z}, n = kd$. We write $d \mid n$", for $d, n \in \mathbb{Z}$

$3 \mid 15 \rightarrow T$, since $15 = 5 \cdot 3$

$4 \mid 15 \rightarrow F$,

QR Theorem $\forall n \in \mathbb{N}^+, \forall k \in \mathbb{Z}$

$\exists q, r \in \mathbb{Z}$

$k = q \cdot n + r$

$\wedge \; n > r \geq 0$

divisibility

primes

$p \in \mathbb{N}$ prime

Notes

annotated week 1