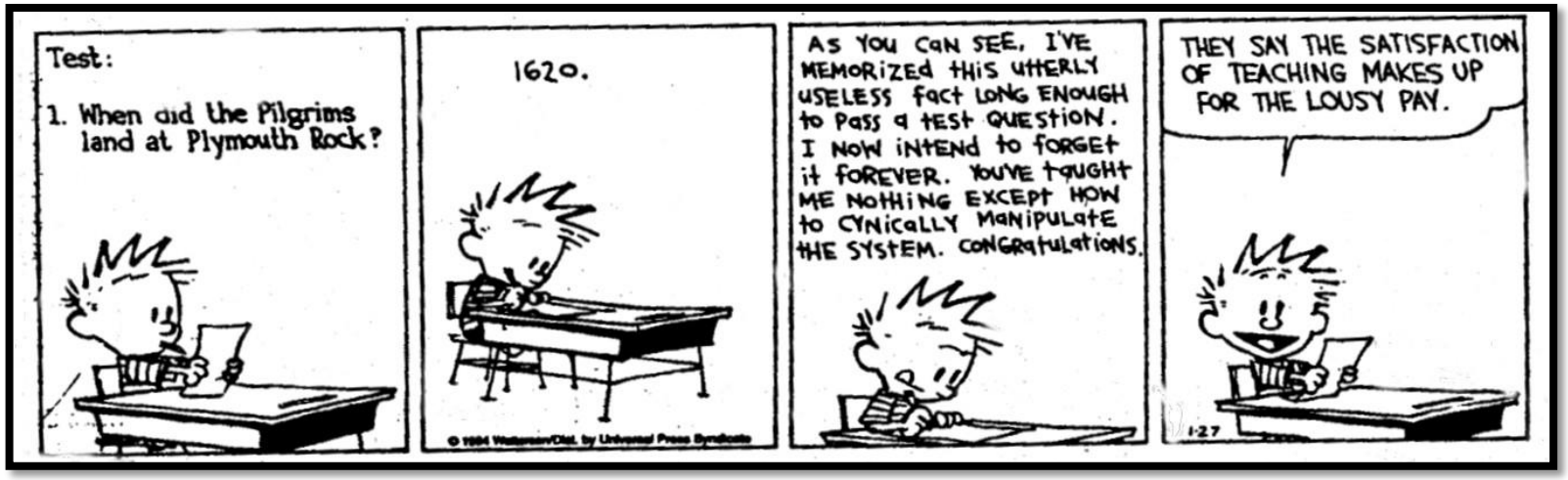
Fall 2015

Midterm review session



$\exists! x \; P(x)$

logic ⇒ quantifiers

The domain of discourse is the set of all people in Washington and the set of all paper-based objects.

object x takes object y

The predicates are **Student**(x), **Exam**(x), **Takes**(x, y) (meaning ~~that student x takes exam y~~), and **Equal**(x, y) (meaning that x and y are the same object).

"All exams are taken by at least one student."

$\cancel{\exists x \forall y (Exam(y) \wedge Student(x) \rightarrow Takes(x,y))}$

$$\forall x (Exam(x) \rightarrow \exists y \; Student(y) \wedge Takes(y,x))$$

"Every student takes exactly one exam."

$$\forall x \; (Student(x) \rightarrow (\forall y \forall z \; (Exam(y) \wedge Exam(z) \wedge Takes(x,y) \wedge Takes(x,z) \rightarrow Equal(y,z))))$$

$(\exists w \; Exam(w) \wedge Takes(x,w))$

logic ⇒ quantifiers

The domain of discourse is the set of all people in Washington and the set of all paper-based objects.

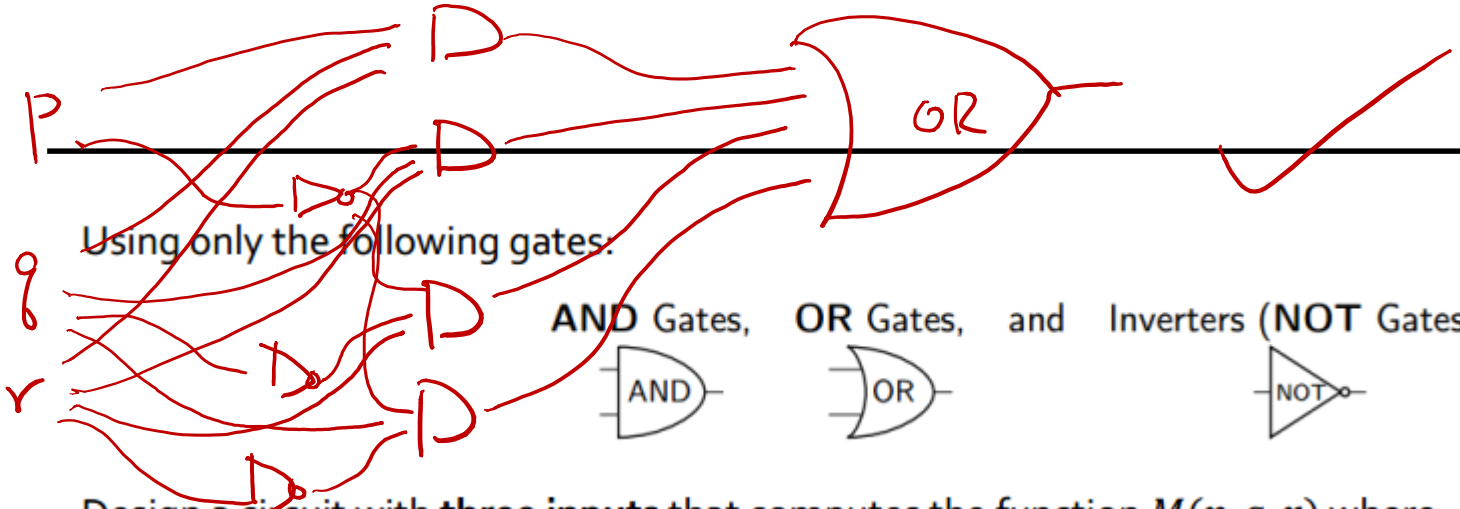
The predicates are **Student**(x), **Exam**(x), **Takes**(x, y) (meaning that student x takes exam y), and **Equal**(x, y) (meaning that x and y are the same object).

Translate the following statement into English
(try to make the translation as simple as possible):

$$\forall x \forall y\ ((\text{Student}(x) \land \text{Student}(y) \land \neg\text{Equal}(x, y)) \rightarrow (\exists z\ \text{Exam}(z) \land \text{Takes}(x, z) \land \neg\text{Takes}(y, z)))$$

For all pairs of distinct students, there is an exam that one student takes, but the other student doesn't.

circuits



Using only the following gates:

AND Gates, **OR** Gates, and Inverters (**NOT** Gates),

Design a circuit with **three inputs** that computes the function $M(p,q,r)$ where

$$M(T,q,r) = q \wedge r$$
$$M(F,q,r) = q \vee r$$

p	q	r	$q \wedge r$	$q \vee r$	M
T	T	T	T	T	T
T	F	T	F	T	F
T	T	F	F	T	F
T	F	F	F	F	F
F	T	T	T	T	T
F	F	T	F	T	T
F	T	F	F	T	T
F	F	F	F	F	F

$$M = pqr + p'qr + p'q'r + p'qr'$$

$$M = qr + p'(q'r + qr')$$

functions

Each of the following functions maps the non-negative integers $\mathbb{N}$ to the non-negative integers $\mathbb{N}$. For each one, indicate the following: (i) whether the function is one-to-one, (ii) whether the function is onto. Briefly justify your answers

(a) $f(n) = 3^n$ 1-1 but not onto

increasing

f(n) is never even

(b) $f(n) = n + 1$ if n is even and $f(n) = 3n+1$ if n is odd.

1-1 b/c both cases are increasing and 1st case outputs odd, 2nd outputs even

not onto never takes 0.

(c) $f(n) = n^2 - 2n + 1$

(d) $f(n)$ = the smallest integer k such that $3k \geq n + 1$.

(e) $f(n)$ = # of distinct prime factors dividing $n + 1$.

not 1-1

$f(2) = f(4) = 1$

onto b/c

$f(0) = 0$

and $f(p_1 \cdots p_n - 1) = n$

(tricky)

sets

Prove that $A = B$ if and only if $\mathcal{P}(\mathcal{P}(A)) = \mathcal{P}(\mathcal{P}(B))$.

Just prove $\boxed{A = B \iff P(A) = P(B)}$

$(\iff P(P(A)) = P(P(B)))$

$$\boxed{A = B \equiv \forall x\,(x \in A \longleftrightarrow x \in B)}$$

Suppose $A = B$. Then $\forall x$

$$x \in P(A) \overset{\text{def}}{\longleftrightarrow} x \subseteq A \overset{A=B}{\longleftrightarrow} x \subseteq B \overset{\text{def}}{\longleftrightarrow} x \in P(B)$$

Hence $P(A) = P(B)$.

Suppose $P(A) = P(B)$. Then $\forall x$

$$x \in A \longleftrightarrow \{x\} \subseteq A \longleftrightarrow \{x\} \in P(A)$$

$$\{x\} \in P(B) \longleftrightarrow \{x\} \subseteq B \longleftrightarrow x \in B.$$

$\Rightarrow A = B.$

$\rightarrow = 2^{j+1}(j-1+j+1)+2 = 2^{j+1}\cdot(2j)+2 = j\cdot 2^{j+2}+2$

induction

Prove that for every positive integer n, it holds that

$$P(n) = \text{“}\sum_{k=1}^{n} k\,2^k = (n-1)2^{n+1}+2\text{”}$$

We will prove $P(n)$ for all pos int. n by

<u>Base case:</u> $P(1) =$ “$1\cdot 2^1 = (1-1)2^{1+1}+2$” true

$2 = 2$

$\Rightarrow P(j+1)$

<u>IH:</u> Assume $P(j)$ for some $j \geq 1$

<u>IS:</u> By the IH $\sum_{k=1}^{j} k\,2^k = (j-1)2^{j+1}+2$

Add $(j+1)2^{(j+1)}$ to both sides: $\boxed{\sum_{k=1}^{j+1} k\,2^k} = (j-1)2^{j+1}+2+(j+1)2^{j+1}$

Therefore by induction, $P(n)$ $\forall n \geq 1$.

induction (inequality)

Prove that if $n > 6$ is an integer then $3^n < n!$

p prime and $p \mid ab$ then $p \mid a$ or $p \mid b$.

modular congruences

Prove that if p is a prime number and $ab \equiv ac \pmod{p}$ then either

$$a \equiv 0 \pmod{p} \quad \text{or} \quad b \equiv c \pmod{p}$$

(1) $ab \equiv ac \pmod{p} \Rightarrow a(b-c) \equiv 0 \pmod{p}$

$\Rightarrow p \mid a(b-c)$

$\Rightarrow p \mid a$ or $p \mid b-c$ by unique factorization

$\Rightarrow a \equiv 0 \pmod{p}$ or $b \equiv c \pmod{p}$

If $a \equiv 0 \pmod{p}$ then ☺

(2) If $a \not\equiv 0 \pmod{p}$ then $\gcd(a, p) = 1$

b/c p is prime $\Rightarrow \exists$ mult. inverse a^{-1} modulo p

So $a^{-1}(ab) \equiv a^{-1}(ac) \pmod{p}$

$\Rightarrow b \equiv c \pmod{p}$.

formal proof

Give a formal proof that: $\forall x\, Q(x) \to \forall x\, (P(x) \to Q(x))$

$$\left(\forall x\, P(x) \wedge \forall x\, Q(x)\right) \to \forall x\, \left(P(x) \to Q(x)\right)$$

By direct proof:

1) $\forall x\, P(x) \wedge \forall x\, Q(x)$ — Assumption
2) $\forall x\, P(x)$ — Elim-$\wedge$, (1)
3) $\forall x\, Q(x)$ — Elim-$\wedge$, (1)
4) $P(c)$ for some arb. c — Inst-$\forall$, (2)
5) $Q(c)$ — Inst-$\forall$, (3)
6) $Q(c) \vee \neg P(c)$ — Intro-$\vee$, (5)
7) $P(c) \to Q(c)$ — Law of Impl, (6)
8) $\forall x\, (P(x) \to Q(x))$ — Intro-$\forall$, (7) b/c c arbitrary $\square$

tofu catr

Some red cats don't like tofu.

$\exists x\ (Red(x) \wedge Cat(x) \wedge \neg LikesTofu(x))$

Incorrect:

$\exists x\ (Red(x) \wedge Cat(x) \rightarrow \neg LikesTof$