WEEK 2 EXERCISE

Last Modified: March 9, 2010

Due Date: 13-Mar

For a problem with a (∗), you may skip if you find difficulities.

1. First order logic

In the lecture, we assumed that P and Q can be interchanged when the propositions P and Q are logically equivalent.

In this exericse, we will verify this.

All the objects concerned in the first two sections are propositions.

We denote $P_1 \equiv P_2$ if P_1 and P_2 are logically equivalent , $\mathcal{T}$ to be a tautology and $\mathcal{F}$ to be a contradiction.

Problem 1.1 (∗). Let P_1, P_2 and Q be propositions and if $P_1 \equiv P_2$, prove the followings:

(1) $(\sim P_1) \equiv (\sim P_2)$.
(2) $(Q \text{ and } P_1) \equiv (Q \text{ and } P_2)$.
(3) $(Q \text{ or } P_1) \equiv (Q \text{ or } P_2)$.
(4) $(P_1 \implies Q) \equiv (P_2 \implies Q)$.
(5) $(Q \implies P_1) \equiv (Q \implies P_2)$.
(6) $(Q \iff P_1) \equiv (Q \iff P_2)$.

Remark. You have to use the truth table to verify.

If you use the theorem $P \iff Q \equiv (P \implies Q) \wedge (Q \implies P)$ and assume they can be interchanged,

you already assume the replacement can be used.

Problem 1.2. Complete the problems in lecture note 2, slide 19.

Problem 1.3. Prove the following

(1) $(P \text{ and } (P \implies Q))$ is logically equivalent to Q.
(2) $(\mathcal{T} \text{ and } P)$ is logically equivalent to P.
(3) $(\mathcal{F} \text{ or } P)$ is logically equivalent to P.
(4) $(\mathcal{T} \text{ or } P)$ is logically equivalent to $\mathcal{T}$.
(5) $(\mathcal{F} \text{ and } P)$ is logically equivalent to $\mathcal{F}$.
(6) $(P \text{ or } P)$ is logically equivalent to P.
(7) $(P \text{ and } P)$ is logically equivalent to P.

Remark. Are $(P \text{ or } P)$, $(P \text{ and } P)$ logically equivalent?

Problem 1.4. Show that the relation $\equiv$ (logically equivalent) satisfying the following:

Reflexive: For each proposition P, $P \equiv P$ is true.

Symmetric: For each propositions P_1 and P_2, if $P_1 \equiv P_2$ then $P_2 \equiv P_1$.

Transitive: For each propositions P_1, P_2 and P_3, if $(P_1 \equiv P_2)$ and $(P_2 \equiv P_3)$ then $P_1 \equiv P_3$

Proof. Use a truth table to demostrate. □

2. Second order logic

In the lecture, we mentioned that a variable can represent not only values, but also other objects like human.

The ***domain of discourse*** is the collection of all possible objects that a variable can represent.

As the truth value of a proposition with FOR-ALL or THERE-EXISTS depends on all the possible propositions,

we must specify the ***domain of discourse*** before using the universal quantifier or the existential quantifier.

Usually, we use the brackets notation to denote the possible objects inside the ***domain of discourse***.

For example, $\{1, 2, 3\}$ has three objects 1, 2 and 3.

Problem 2.1. Let the domain of discourse to be $\{2, 3, 5\}$.

Let $P_1(x) :=$ "x is an odd number.",

$P_2(x) :=$ "x is an even number.",

$P_3(x) :=$ "x is an prime number.",

What is the truth value of the following propositions? Explain.

(1) $\forall x, P_1(x)$
(2) $\exists x, P_1(x)$
(3) $\forall x, P_3(x)$
(4) $\forall x, P_2(x)$ and $P_3(x)$
(5) $\forall x, P_2(x) \implies P_3(x)$
(6) $\exists x, P_3(x)$ and $P_2(x)$
(7) $\exists x, P_3(x) \implies P_2(x)$

Proof. We should translate the above symbolic notation to english so as to understand the proposition.

The first statement is "Every object is an odd number", clearly this is false as 2 is a possible object.

Note that there are subtle difference between the last two pairs of propositions.

The forth statement is "For each object, it is a prime and even number", false since 3 is odd.

The fifth statement is "For each object, if it is even then it is a prime", true as the only even number is a prime.

The others are left as exercise. □

Remark. If the domain of discourse has other positive even number like 4, then the fifth statement is false.

3. Translation

In the last exercise, we translated a proposition written in symbols to english. Now, we will do the reverse way.

Example 3.1. Let the domain of discourse be all the animals,

$E(x,y) :=$ "x eats y", $W(x) :=$ "x is white.", $R(x) :=$ "x is red." and $F(x) :=$ "x is a fish".

Let a be a speical white fish, the proposition "The speical white fish eats any fishes" is "$\forall x, F(y) \implies E(a,y)$".

Let b be a red fish which eats some fish (not necessary every).

The fish b can be described as "$F(b)$ and $R(b)$ and $(\exists x, F(x)$ and $E(b,x))$".

The proposition "There is animal which eats the red fish b" is "$\exists x, E(x,b)$".

The proposition "There is an animal which eats every red fish" is "$\exists x, \forall y, (F(y)$ and $R(y)) \implies E(x,y)$".

The proposition "The only animal that b eats is fish" is "$\forall x, E(b,x) \implies F(x)$".

The proposition "There is one and only one animal which eats every white animal" is

"$\exists y, (\forall t, W(t) \implies E(y,t))$ and $(\forall x,$ if $(\forall z, W(z) \implies E(x,z))$ then $x = y)$.

To explain in depth for the last one, logically "one and only one" means that there is at least one such object and whenever there are two objects satisfying the same properties then they are the same.

So, we first say that there is an animal which eats every white animal.

Secondly, whenever there is an animal which eats every white animal then they are the same.

Remark. "$\forall t, W(t)$ and $E(y,t)$" is the proposition "Every animal is white and eatten by y".

Problem 3.2. Accoring to the above example, write down the symbolic propositions of the followings:

(1) Every animal eat any fish.
(2) The only fish that b eats is the white fish a.
(3) There is a fish which every fish eat it.
(4) There is a red animal which eats all the white animal.
(5) Every white animal eats some red animal.
(6) There is an white animal which eats red fish.

Problem 3.3. Let the domain of discourse be all the real numbers,

$I(x) :=$ "x is an integer", $L(x,y) :=$ "x is less than y".

Write down the symbolic proposition for the following statements (any logically equivalent statement is acceptable):

(1) There is an integer less than 10.
(2) There is no the greatest integer.
(3) There is no greatest real number.
(4) $(*)$There is only one integer which is less than 2 and greater than 0.

4. Application in maths

In mathematics, we usually assume the domain of discourse to be all the real numbers.

Theorem 4.1 (Non-negative of square)**.** *$\forall x, x^2 \geq 0$ and equality holds if and only if $x = 0$*

i.e. Every square of a real number is non-negative and

the square of a number is zero if and only if the number itself is zero.

Here, we give a famous algebraic proof of the AGM-inequality, which we did geometrically in last exericse.

Example 4.2 (AGM-inequality)**.** Let x, y be real numbers, prove that

$$\frac{x+y}{2} \geq \sqrt{xy}$$

and equality holds iff $x = y$.

Proof. Let $a = \sqrt{x}$ and $b = \sqrt{y}$, by the non-negative of square, we have $(a-b)^2 \geq 0$.

i.e. $a^2 - 2ab + b^2 = x - 2\sqrt{xy} + y \geq 0 \iff x + y \geq 2\sqrt{xy} \iff \dfrac{x+y}{2} \geq \sqrt{xy}$.

Equality holds iff $a - b = 0$ i.e. $a = b \iff \sqrt{x} = \sqrt{y} \iff x = y$ □

Problem 4.3 (HM≤GM)**.** Let x, y be real numbers, prove that

$$\frac{2}{\frac{1}{a} + \frac{1}{b}} \leq \sqrt{ab}$$

and equality holds iff $x = y$.

Hints: Let $a = \frac{1}{x}$ and $b = \frac{1}{y}$ and use the AGM-inequality on a and b.

Theorem 4.4 (AM≤QM)**.** *Let x, y be real numbers, we always have*

$$\frac{x+y}{2} \leq \sqrt{\frac{x^2+y^2}{2}}$$

and equality holds iff $x = y$.

Proof. Compare $\left(\frac{x+y}{2}\right)^2$ with $\frac{x^2+y^2}{2}$, we have $\frac{x^2+y^2}{2} - \left(\frac{x+y}{2}\right)^2 = \frac{2(x^2+y^2)-(x^2+y^2+2xy)}{4} = \frac{x^2+y^2-2xy}{2} = \frac{(x-y)^2}{2}$.

Their difference is a square of $(x - y)$ divided by 2, which is always non-negative.

It is zero if and only if $x = y$ □

Theorem 4.5 (AGM-inequality)**.** *Let $x_1, x_2, \ldots, x_n$ be real numbers, we always have*

$$\frac{x_1 + x_2 + \cdots + x_n}{n} \geq \sqrt[n]{x_1 x_2 \cdots x_n}$$

and equality holds iff $x_1 = x_2 = x_3 = \cdots = x_n$.

Proof. We will prove this later. □

5. Euclidean algorithm for finding greatest common divisor

Usually, we use the term "greatest common divisor" instead of "highest common factor".

Theorem 5.1. *Let m, n be two positive integers and $\gcd(m, n)$ be their **greatest common divisor.***

There are some integers x_0 and y_0 such that $mx_0 + ny_0 = \gcd(m, n)$

i.e. You can find some multiple of m and n such that the sum is exactly the highest common factor.

Example 5.2. As an example, let $m = 15$ and $n = 80$, we know that $\gcd(m, n) = 5$.

In fact, $80 \times (1) + 15 \times (-5) = 5$.

There are infinitely many pairs, whcih can be found as follows:

$5 = n \cdot (1) + m \cdot (-5) = n \cdot (1 + m - m) + m \cdot (-5 + n - n)$

$\therefore 5 = n \cdot (1 + m) - mn + m \cdot (-5 - n) + mn = n \cdot (1 + m) + m \cdot (-5 - n)$

Therefore, putting back m and n, we have $5 = 80 \times (1 + 15) + 15 \times (-5 - 80) = 80 \times (16) + 15 \times (-85)$.

Theorem 5.3. *Let m, n be integers and $d = \gcd(m, n)$ and if x_0, y_0 are integers such that $mx_0 + ny_0 = d$ then*

$$m(x_0 + kn) + n(y_0 - km) = d$$

i.e. The pairs can be described as $(x_0 + kn, y_0 - km)$ for all integers k.

If we want to find every such pair, the problem is reduced to finding a particular pair of multiple.

To find a particular one, we use the following method.

Theorem 5.4 (Extended Euclidean algorithm)**.** *Assume $m > n$, define the numbers r_k, q_k, x_k, y_k as follows:*

$$\begin{aligned}
&r_0 = m \\
&r_1 = n \\
&r_k = r_{k-2} \bmod r_{k-1}\ \text{, for } k > 1 \\
&q_k = \frac{r_{k-2} - r_k}{r_{k-1}},\ \text{for } k > 1 \\
&x_0 = 1 \\
&y_0 = 0 \\
&x_1 = 0 \\
&y_1 = 1 \\
&x_k = x_{k-2} - q_k x_{k-1},\ \text{for } k > 1 \\
&y_k = y_{k-2} - q_k y_{k-1},\ \text{for } k > 1
\end{aligned}$$

Compute the numbers starting from $k = 2, 3, \ldots$ until $r_k = 0$.

Then $r_{k-1} = \gcd(m, n)$ and $mx_{k-1} + ny_{k-1} = r_{k-1} = \gcd(m, n)$.

For each k, we have $mx_k + ny_k = r_k$.

Remark. The q_k's are the quotient, so we can find the q_k and r_k by doing a simple division on r_{k-2} and r_{k-1}.

You can quickly find $\gcd(m, n)$ by computing r_k only.

Example 5.5. We find the pair for $m = 130$ and $n = 15$, knowing $\gcd(130, 15) = 5$, as follow:

k	r_k	q_k	x_k	y_k	Formulae
0	130		1	0	
1	15		0	1	
2	10	8	1	-8	$130 = 15 \cdot 8 + 10$
3	5	1	-1	9	$15 = 10 \cdot 1 + 5$
4	0	2	3	-26	$10 = 5 \cdot 2 + 0$

First, we write down the row for $k = 0$ and $k = 1$.

Clearly, q_0 and q_1 are undefined, so we left it blank.

We can do a division on $130 \div 15$ to get $q_2 = 8$ and $r_2 = 10$.

x_2 and y_2 are obtained by subtracting q_2 times the number at $k = 1$ from the number at $k = 0$.

In general, after finding the quotient,

the number x_k, y_k are found by multipling the previous row's x and y by the quotient,

then subtract it from the previous two row's x and y.

Therefore, we get $130 \times (-1) + 15 \times (9) = 5$.

The other solutions are $130 \times (-1 + 15k) + 15 \times (9 - 130k)$ for any integer k.

Problem 5.6. Let $m = 2036$ and $n = 128$.

(1) Find $\gcd(m, n)$ by using the Euclidean algorithm.

(2) Hence find a pair of integers (x_0, y_0) such that $mx_0 + ny_0 = \gcd(m, n)$

(3) Find all such integer pairs.

Problem 5.7. Let $m = 144$ and $n = 89$.

(1) Find $\gcd(m, n)$ by using the Euclidean algorithm.

(2) Find a pair of integers (x_0, y_0) such that $mx_0 + ny_0 = \gcd(m, n)$

(3) Find all such integer pairs.

Remark. If m and n are Fibonacci numbers, it takes the longest steps to compute.

6. Synthetic substitution

Problem 6.1. Let $f(x) = 4x^5 - 3x^4 - 7x^3 - 10x + 1$ be a polynomial.

Using the synthetic substitution, find $f(3)$ and find the quotient when $f(x)$ is divided by $(x - 3)$.

7. Regular Expression

In the lecture, we discussed some of the regular expressions.

For detail, please check wikipedia.

.	matches any character including newline.
a{3,5}	matches any string of at least 3 'a' and at most 5 'a', i.e. "aaa" , "aaaa" and "aaaaa".
(ab){1,2}	matches "ab" , "abab".
ab{1,2}	matches "ab" , "abb"
+	means one or more
?	means zero or one
*	means zero or more
|	means alternative choice
{m,n}	means at least m times and at most n times
gr(a|e)y	matches "gray" or "grey"

Problem 7.1. Write down a regular expression (if exists) which matches

(1) Any even computer-integer

(2) Any odd computer-integer

(3) Any non-negative computer-integer

(4) Any string that starts with

(5) Any negative computer-integer

(6) Any negative odd copmuter-integer

(7) "apple" and "pipeapple"

(8) (*) Any string that has the same number of '0' and '1'

Remark. Actually, the last kind of string cannot be represented using regular expression.

The impossibility is guaranteed by the *pumping lemma for regular languages.*[1]

Problem 7.2. Describe what the following regular expression matches:

(1) [1-9][0-9]

(2) [1-9][0-9]{0,2}

(3) [\+\-]?[02468]

(4) [a-z]+

(5) [A-Z][a-z]*

(6) a((a|b)\{2,2})*b

(7) (aa|bb)+

(8) (aa)+|(bb)+

[1]We will discuss this once we finished the first seven chapters of Discrete Mathematics

8. Evaluation of arithmetic expression in C

The operator precedence is as usual, i.e. 1+2*3 are evaluated as 1 + (2*3).

The order for quotient and modulus are the same as multiplication and real division.

The operations are performed from left to right if they have the same precedence.

However, please note that -1 * 2 is interpreted as "the product of negative one and 2".

Therefore, in this sense, the unary operator - (negative) and + (positive) is the fastest.

Note that, the exponent "e" , "E" is NOT an operator.

The computer interpret "1E+2" directly as the real number 1×10^2.

The computer cannot understand "1E(3+4)".

It is not a computer real number, because it does not match the regular expression for a real number.

Problem 8.1. Evaluate the following expression as if in a computer:

(1) 1+2*3/2

(2) 1+3/2*2

(3) 1+42364117%11

(4) 71123/10

(5) 71123%10

(6) (((1+2)*3)4)*5

(7) 11+23.0/8

(8) 12.5/5+1e5

(9) 3e2/2+9%7

(10) 71123%100/10

(11) -1*-3+5