DISCRETE MATH 37181 HOMEWORK SHEET 6

INSTRUCTIONS. Try these sometime after your tutorial and before the next lecture. Set aside some time each week to keep up with the homework. Partial solutions at the end of the PDF.

1. (a) Write down a precise definition for $f \in O(g)$ (g dominates f).

   (b) Write down a precise definition for a function $f : A \to B$ to be *one-to-one*.[1]

   (c) Write down a precise definition for a function $f : A \to B$ to be *onto*.[2]

   (d) Write down a precise statement of the *pigeonhole principle*.

   (e) Write down a precise statement of the *generalised pigeonhole principle*.

   (f) Write down a precise definition for an *equivalence relation* on a set A.

   (g) Write down a precise statement of a *partition* of a set A.

2. For each of the following functions, guess a Big-O form from one of those in Table 1 from the tutorial worksheet, then prove your guess.

   (a) $f(n) = 4n + 7$

   (b) $g(n) = 5n^2 + 3n \log_2 n$

   (c) $h(n) = 1 + 2 + \cdots + n$

3. Show that g dominates f in each of the following

   (a) $f(n) = 6n + 10, \quad g(n) = 0.05n^2$

   (b) $f(n) = 3n^2, \quad g(n) = 2^n + 2n$.

4. Prove that:

   If $S \subseteq \mathbb{N}_+$ and $|S| > 6$ then S contains three distinct elements x, y, z such that $x + y + z \equiv 0 \mod 3$.

5. Let A, B be finite sets and $f : A \to B$ a function. Prove that if f is one-to-one then $|A| \leqslant |B|$.

Date: Week 6.

[1] also called *injective*

[2] also called *surjective*

6. Let A, B, C be sets and $f : A \to B, g : B \to C$. Recall that $g \circ f : A \to C$ is the function defined as $g \circ f(a) = g(f(a))$ for all $a \in A$.

   Prove that:

   If $f : A \to B, g : B \to C$ are one-to-one then $g \circ f$ is one-to-one.

7. In computer science it is useful to *compress* strings. For example, in a text file we might want to replace all strings *the* by κ and *murray* by $\delta\#$. For this, we assume we have a fixed finite *alphabet* of symbols available, say $a, b, c, \ldots, z, A, B, C, \ldots, Z, 0, 1, 2, 3, \ldots, 9$, plus a *space* symbol plus some finite list of special symbols $\kappa, \delta, \#, \ldots$.

   A *universal lossless compression algorithm* is an algorithm that rewrites *every* string as something shorter. How good would that be?

   Show that such an algorithm cannot exist (use PHP).

Brief solutions:

1. (a) Let $f, g : \mathbb{N}_+ \to \mathbb{R}$. We say that g *dominates* f if there exist constants $m \in \mathbb{R}^+$ and $k \in \mathbb{Z}^+$ such that $|f(n)| \leqslant m|g(n)|$ for all $n \in \mathbb{N}, n \geqslant k$.

   (b) $\forall x, y \in A$ if $f(x) = f(y)$ then $x = y$.

   (c) $\forall y \in B\ \exists x \in A$ such that $f(x) = y$.

   (d) If m pigeons occupy n pigeonholes and $m > n$ then some pigeonhole has at least two pigeons in it.

   (e) If m pigeons occupy n pigeonholes and $m > kn$ then some pigeonhole has more than k pigeons in it.

   (f) A relation $\subseteq A \times A$ which is reflexive (includes (a, a) for every $a \in A$), symmetric (if $(a, b) \in \mathscr{R}$ then so is (b, a)) and transitive (if $(a, b), (b, c) \in \mathscr{R}$ then so is (a, c)).

   (g) See the worksheet from last week: a set of sets A_i so that A is the union of all the A_i and $A_i \cap A_j = \emptyset$ for all $i \neq j$. So (imprecisely) a partition is a way of dividing up the set into disjoint smaller sets which cover the whole set.

2. (a) Guess $O(n)$. There exists $m = 5, k = 7$ so that
$$f(n) = 4n + 7 \leqslant 4n + n \text{ (since } n \geqslant 7) \ = 5n$$
   for all $n \geqslant 7$.

   Guess $O(n^2)$ since the log is smaller than n. Proof: if $n \geqslant 1$ then $\log_2 n \leqslant n$ since $n \leqslant 2^n$ (prove this by induction to be very rigorous).
   Then
$$5n^2 + 3n \log_2 n \leqslant 5n^2 + 3n.n \text{ (since } n \geqslant \log_2 n) \ = 8n^2$$
   so $m = 8, k = 1$.

   (c) Induction we know this equals $\frac{n(n+1)}{2} = \frac{1}{2}n^2 + \frac{1}{2}n$ so $O(n^2)$, quadratic:
$$\frac{1}{2}n^2 + \frac{1}{2}n \leqslant \frac{1}{2}n^2 + \frac{1}{2}n^2 = n^2$$
   for any $n \geqslant 1$ so $k = m = 1$.

3. (a) $f(n) = 6n + 10 \leqslant 6n + n$ (assuming $n \geqslant 10$)
$$= 7n = \frac{7}{0.05}(0.05n) = 140(0.05n) \leqslant 140(0.05n^2)$$
   if $n \geqslant 1$, so with $k = 10$ and $m = 140$ we have $f \in O(g)$.

   Note there are many different ways to show this.

(b) I will show $3n^2 - 2n \leqslant 2^n$ for all $n \geqslant ?$ by induction. So I will have $m = 1$ and $k = ?$. The statement $P(n) : 3n^2 - 2n \leqslant 2^n$ is true for $n = 1$, so we have $P(1)$. Assume $P(s)$. Then to show $P(s+1)$ we have:

$$3(s+1)^2 - 2(s+1) = 3(s^2 + 2s + 1) - 2s - 2 = 3s^2 + 6s + 3 - 2s - 2$$
$$= 3s^2 - 2s + 6s + 1 \leqslant 2^s + 6s + 1$$

by inductive assumption. To finish I need to show $6s + 1 \leqslant 2^s$, which I will prove separately below. However, this is only true for $s \geqslant ?$ so I will have to change the value of $k = ?$ to $k = 6$ and start over.

Lemma 1. *For all $n \geqslant 6$, $6n + 1 \leqslant 2^n$*

Proof. Induction: true for $n = 6$ since $37 < 2^6 = 64$. (also true for smaller, but 6 is fine for Big O proofs.)
Assume true for $t \geqslant 6$, then

$$6(t+1) + 1 = 6t + 1 + 6 < 6t + 1 + 6t + 1$$

(since $6 < 6t + 1$)

$$\leqslant 2^t + 2^t = 2^{t+1}.$$

Then by PMI $P(n)$ is true for all $n \geqslant 6$. □

Now I start again, using the lemma. Let $P(n)$ be the statement: $3n^2 - 2n \leqslant 2^n$
$P(6)$ since $LHS = 3.36 - 12 = 96$ and $RHS = 2^6 = 64$ Not true.
So I change my value of $k = ?$ again.

FINAL PROOF:
Let $P(n)$ be the statement: $3n^2 - 2n \leqslant 2^n$. $P(10)$ is true since $LHS = 3.100 - 20 = 280$ and $RHS = 2^{10} = 1024$. Assume $P(s)$. $P(s+1)$:

$$LHS = 3(s+1)^2 - 2(s+1) = 3(s^2 + 2s + 1) - 2s - 2 = 3s^2 + 6s + 3 - 2s - 2$$
$$= 3s^2 - 2s + 6s + 1 \leqslant 2^s + 6s + 1$$

by inductive assumption.

$$\leqslant 2^s + 2^s$$

by Lemma 1

$$= 2.2^s = 2^{s+1}$$

so by PMI $P(n)$ is true for all $n \geqslant 10$.

4. Pigeons are the elements in S, and pigeonholes are the remainders of each number mod 3, so a box labeled $0, 1$ and 2.

   Since we have at least 7 pigeons going into 3 boxes, at least one box has 3 elements, call these x, y, z. If the three elements have the same remainder mod 3, then $x + y + z \equiv 0 \mod 3$ (more detail: $x = 3p + i, y = 3q + i, z = 3r + i$ each with the same remainder i, then $x + y + z = 3(p + q + r + i)$.)

5. Suppose $|A| > |B|$. Let A be pigeons, B pigeonholes, and place each $a \in A$ into hole $f(a)$. Then since $|A| > |B|$ by PHP some hole has two elements of A in it, say $x, y \in A$, and $f(x) = f(y)$ since they are placed in the same hole. This shows f is not one-to-one. The result is the contrapositive.

6. Suppose $g \circ f(x) = g \circ f(y)$ for some $x, y \in A$. Then $g(f(x)) = g(f(y))$ and since g is one-to-one, this means $f(x) = f(y)$. But now since f is one-to-one this means $x = y$. This $g \circ f$ is one-to-one.