# PMT Additional Exercises (Week 5)

Nicholas Sim

November 2nd, 2017

## 1 Discrete Structures: Functions

We have seen in the lectures that if $R$ is an equivalence relation on a set $A$, it will partition $A$ into its quotient set $A/R$. Prop. 2.17 shows that $A/R = \{[a] : a \in A\}$.

Suppose that every equivalence class $[a]$ has a (unique, distinguished) representative $\bar{a}$.

1. Let $A, B$ be finite sets, and define $f : A \to B$ to be surjective.[1] Show that there is an equivalence relation $R$ on $A$, where $(a_1, a_2) \in R$ if and only if $f(a_1) = f(a_2)$.
2. Let $g : B \to A$ be a function where $g(b) = \bar{a}$, the unique representative of $[a]$ where $f(a) = b$. Show that $g$ is injective.[2]
3. Define $g' : B \to A/R$ similarly to $g$, except mapping to the equivalence class $[a]$ instead of $\bar{a}$. Show that $g'$ is a bijection.

   The following questions test your understanding of the definitions.

4. (*) Suppose $A \neq \varnothing$, and $f : A \to B$. Show that there is a function $g : B \to A$ such that $(g \circ f)(a) = a$ for any $a \in A$. *[thanks to A. Corti]*
5. Let $A, B$ be finite sets of $m, n$ elements respectively.
   (a) (*) How many injections $A \to B$ are there?
   (b) Let $n = 2$ How many surjections?
   (c) (**) Now $n > 2$. How many surjections?
   (d) How many bijections?

   *[Hint: consider cases $m$ larger than $n$, etc.]*

## 2 Logic: Natural Deduction

Prove the following using Natural Deduction:

1. $A \to B, A \to \neg B \vdash \neg A$
2. $\neg B \to \neg A \vdash A \to B$ (the contrapositive)
3. $\vdash A \to A$
4. $\vdash A \vee \neg A$ (obviously, you're not allowed to use EM for this one)
5. $(A \to (B \to C)) \vdash ((A \to B) \to (A \to C))$
6. *[Q1a of the 2015 exam]* $B, \neg C \to \neg A \vee \neg B \vdash A \to C$
7. $A \to (B \to C) \vdash B \to (A \to C)$

[1] *surjective* here means every element in $B$ is mapped by at least 1 element in $A$.

[2] *injective* maps preserve distinctness: if $g(b_1) = g(b_2)$, then we can conclude $b_1 = b_2$. Say: "No two $b$s map to the same $a$."

## 3 Solutions to Functions

1. This is a routine verification of R, S, T, which I will omit.

2. Since $f$ is surjective, $g$ is injective.
(another proof) We defined $R$ such that $f(a_1) = f(a_2) = b$ if and only if $a_1, a_2$ belong to the same equivalence class. So $f$ maps all the members of $[a]$ to the same value of $b$. Now suppose $g(b_1) = g(b_2) = \bar{a} \in A$. Then $b_1 = f(\bar{a}) = b_2$.

3. It suffices to show that $g'$ is surjective (argue injective via surjectivity of $f$, alternatively, proof similar to injectivity of $g$). Suppose for a contradiction that $g'$ is not surjective. Then $\exists a \in A$ such that $f(a) \notin B$. But $f$ is a function (hence maps all the elements in its domain).

4. We need $A \neq \varnothing$, because to be a function, $g$ must map any value in $B$ to some value. Define $g$ as follows. Fix $b \in B$. If $b \notin \text{image}(f)$, then let $g(b) = a_0$ (choose any $a_0 \in A$). If $b$ is in the image of $f$, then $\exists a_b \in A$ s.t. $f(a_b) = b$. Let $g(b) = a_b$.

   (proof) Pick $a \in A$ arbitrarily and verify $(g \circ f)(a) = a$. Let $f(a) = b$ and clearly $a = a_b$ by construction. Then $g(f(a_b)) = g(b) = a_b = a$ as required.

5. $|A| = m, |B| = n$.

   (a) Suppose $m > n$. There can be no injections. For $m \leq n$, we need to choose $m$ distinct elements to map to, from $n$ possible values, where order (permutation) matters. So $\frac{n!}{(m-n)!}$.

   (b) Try inclusion-exclusion. There are $n^m$ possible functions $A \to B$ ($n$ choices for $m$ inputs). But $n = 2$, so just $2^m$. There are only two possible non-surjective functions (send all elements in $A$ to the first value, or the second value). So $2^m - 2$.

   (c) (Why can't we just count? Think about this)
   Consider $n = 3$. Write $1, 2, 3$ for the elements of $B$. We need to subtract the non-surjective functions from $3^m$. There are $2^m$ functions each including only (1, 2), (1, 3), or (2, 3). But the Principle of Inclusion-Exclusion tells us that we have subtracted 3 functions twice. So $3^m - 3(2^m) + 3$.
   Construction: we want $n^m - (n)(n-1)^m + \binom{n}{2}(n-2)^m - \dots$
   Claim: This formula works

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)^m$$

   Satisfy yourself that this is correct.

   (d) This is just the number of injections when $m = n$, i.e. $m!$.

## 4 Solutions to Natural Deduction

Full proofs are not included, but you can ask me for clarifications.

1. Suppose $A$. Then from the givens, we can use $\to E$ to get both $B, \neg B$. Contradiction. So we get $\neg A$ by $\neg I$.

2. Suppose $A$. We want to get $B$, so suppose $\neg B$. Get $\neg A$ by $\to E$, then $B$ by $PC$. Conclude $A \to B$ using $\to I$.

3. This one can't be that hard! Do it yourself.

4. Note: if we could use equivalences, this is exactly the same as the last. This appears in the notes, and the overall form is a proof by contradiction.

5. This is slightly messy, but we'll just try:
Suppose $A \to B$. We want to get $A \to C$. So suppose $A$. $B$ follows using $\to E$. $B \to C$ from using $\to E$ on the given. Then we get $C$, thus $A \to C$. Finally we have $((A \to B) \to (A \to C))$.

6. Suppose $A$. We want to get $C$. Suppose $\neg C$. Then we get $\neg A \vee \neg B$. Perform $\vee E$ to get $\neg B$: but this contradicts the given $B$. So after some $\perp I$, we get $C$ via $PC$. And that's all we need to conclude $A \to C$.

7. Suppose $B$. We will show $A \to C$. Suppose $A$. Then we have $B \to C$, but we have $B$, so we have $C$.