Functions and cardinality (solutions)

21-127 sections A and F | TA: Clive Newstead | 6th May 2014

What follows is a somewhat hastily written collection of solutions for my review sheet. I have omitted some details but the ingredients for the solution should all be there.

---

1 Determine which of the following functions are injective and which are surjective:

(a) $f : \mathbb{Z} \to \mathbb{N}$, where $\forall n \in \mathbb{Z}.\ f(n) = |n| + 1$;

(b) $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, where $\forall (n, k) \in \mathbb{N} \times \mathbb{N}.\ g(n, k) = 2^n \cdot 3^k$;

(c) $h : \mathcal{P}(\mathbb{N}) \to \mathcal{P}(\mathbb{N})$, where $\forall A \in \mathcal{P}(\mathbb{N}).\ h(A) = \mathbb{N} \setminus A$;

(d) $k : \mathbb{Z} \to \mathcal{P}(\mathbb{Z})$, where $\forall n \in \mathbb{Z}.\ k(n) = \{n, 1, -1\}$.

Using the above functions, compute the following sets:

$$\mathrm{PreIm}_f(\mathbb{N}), \quad \mathrm{Im}_g(\mathbb{N} \times \{1\}), \quad \mathrm{PreIm}_h(\varnothing), \quad \mathrm{PreIm}_h(\{\varnothing\}), \quad \mathrm{Im}_k(\{-1, 0, 1\})$$

Solution:

(a) f is not injective: for example, $f(1) = |1| + 1 = |-1| + 1 = f(-1)$.
f is surjective: if $n \in \mathbb{N}$ is arbitrary then $n = |n - 1| + 1 = f(n - 1)$, and $n - 1 \in \mathbb{Z}$.

(b) g is injective: if $f(n, k) = f(m, \ell)$ then $2^n \cdot 3^k = 2^m \cdot 3^\ell$, so $(n, k) = (m, \ell)$ by the fundamental theorem of arithmetic.
g is not surjective: for example, $5 \neq 2^n \cdot 3^k$ for any $n, k \in \mathbb{N}$, since that would imply $2 \mid 5$.

(c) h is injective: let $A, B \in \mathcal{P}(\mathbb{N})$ be arbitrary and suppose $\mathbb{N} \setminus A = \mathbb{N} \setminus B$. Then

$$n \in A \quad \Leftrightarrow \quad \neg(n \in \mathbb{N} \setminus A) \quad \Leftrightarrow \quad \neg(n \in \mathbb{N} \setminus B) \quad \Leftrightarrow \quad n \in B$$

so $A = B$ by double-containment.
h is surjective: if $A \in \mathcal{P}(\mathbb{N})$ is arbitrary then

$$A = \mathbb{N} \setminus (\mathbb{N} \setminus A) = h(\mathbb{N} \setminus A)$$

and $\mathbb{N} \setminus A \in \mathcal{P}(\mathbb{N})$.

(d) k is not injective: for example, $k(1) = \{1, 1, -1\} = \{1, -1\} = \{-1, 1, -1\} = k(-1)$, since sets don't count duplicate elements.
k is not surjective: for example, $\mathbb{Z} \neq \{n, 1, -1\}$ for any $n \in \mathbb{Z}$ as $\mathbb{Z}$ is infinite but each $\{n, 1, -1\}$ is finite.

Now for the (pre)images:

– $\mathrm{PreIm}_f(\mathbb{N}) = \{n \in \mathbb{Z} : |n| + 1 \in \mathbb{N}\} = \mathbb{Z}$; in general, the preimage of the codomain of a function is the entire domain.

– $\mathrm{Im}_g(\mathbb{N} \times \{1\}) = \{x \in \mathbb{N} : x = 2^n \cdot 3^1 \text{ for some } n \in \mathbb{N}\} = \{2^n \cdot 3 : n \in \mathbb{N}$

– $\mathrm{PreIm}_h(\varnothing) = \{A \subseteq \mathbb{N} : N \setminus A \in \varnothing\} = \varnothing$, since $\varnothing$ contains no elements.

– $\mathrm{PreIm}_h(\{\varnothing\}) = \{A \subseteq \mathbb{N} : N \setminus A \in \{\varnothing\}\} = \{A \subseteq \mathbb{N} : N \setminus A = \varnothing\} = \{\mathbb{N}\}$; note the difference between $\varnothing$ and $\{\varnothing\}$ in the previous part.

– $\mathrm{Im}_k(\{-1, 0, 1\}) = \{\{-1, 1, -1\}, \{0, 1, -1\}, \{1, 1, -1\}\} = \{\{1, -1\}, \{0, 1, -1\}\}$, again because sets don't count duplicate elements.

---

2 The following functions are bijective; find their inverses:

(a) $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$, where $\forall (x, y) \in \mathbb{Z} \times \mathbb{Z}.\ f(x, y) = (4x - y, y - 3x)$;

(b) $g : [8] \to \mathbb{Z}_8$, where $\forall n \in [8].\ g(n) = [\![3n + 5]\!]$;

Solution:

(a) For a function $F : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ to be an inverse, it would need in particular to satisfy

$$\forall (x, y), (a, b) \in \mathbb{Z} \times \mathbb{Z}.\ f(x, y) = (a, b) \Rightarrow (x, y) = F(a, b)$$

so *if it exists* we can find what it does to an arbitrary pair (a, b) by solving the equation $f(x, y) = (a, b)$ for (x, y). So let $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ be arbitrary and suppose

$$(4x - y, y - 3x) = (a, b), \quad \text{i.e.} \quad \begin{cases} 4x - y = a & (1) \\ -3x + y = b & (2) \end{cases}$$

Adding (2) to (1) gives $x = a + b$. Substituting this into (1) gives $4(a + b) - y = a$ and hence $y = 3a + 4b$.

Claim. The function $F : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ defined by $F(a, b) = (a + b, 3a + 4b)$ is an inverse for f. (*Proof.* Check both composites: tedious algebra.)

(b) For a function $G : \mathbb{Z}_8 \to [8]$ to be an inverse, it would need in particular to satisfy

$$\forall n \in [8].\forall [\![a]\!] \in \mathbb{Z}_8.\ g(n) = [\![a]\!] \Leftrightarrow n = G([\![a]\!])$$

so *if it exists* we can find out what it does to an arbitrary $[\![a]\!] \in \mathbb{Z}_8$ by solving the equation $g(n) = [\![a]\!]$. So let $[\![a]\!] \in \mathbb{Z}_8$ be arbitrary and suppose $[\![3n + 5]\!] = [\![a]\!]$. Then

$$3n + 5 \equiv a \bmod 8 \Rightarrow 3n \equiv a - 5 \bmod 8 \Rightarrow n \equiv 3a - 15 \bmod 8 \Rightarrow n \equiv 3a + 1 \bmod 8$$

The second implication holds because $3 \cdot 3 \equiv 1 \bmod 8$, and the third holds because $-15 \equiv 1 \bmod 8$.

But every congruence class $[\![n]\!]$ modulo 8 has a unique representative $n \in [8]$, so we can define $G([\![a]\!])$ to be the unique $n \in [8]$ such that $n \equiv 3a + 1 \bmod 8$. Explicitly,

$$G([\![0]\!]) = 1,\ G([\![1]\!]) = 4,\ G([\![2]\!]) = 7,\ G([\![3]\!]) = 2$$

$$G([\![4]\!]) = 5,\ G([\![5]\!]) = 8,\ G([\![6]\!]) = 3,\ G([\![7]\!]) = 6$$

Note that this is well-defined by Theorem 20 of your number theory notes.

Claim. $G = g^{-1}$. (*Proof.* Again, tedious algebra, just check the composites.)

---

3 Define a function $f : \mathbb{Z} \to \mathbb{Z}$ such that, for each $n \in \mathbb{Z}$, $|\text{PreIm}_f(\{n\})| = 2$. Does your function have an inverse? If so, find it; if not, explain why.

Solution: The function defined by $\forall x \in \mathbb{Z}.\ f(x) = \lfloor \frac{x}{2} \rfloor$ works, since given $y \in \mathbb{Z}$ we have $\text{PreIm}_f(y) = \{2y, 2y+1\}$. No such function can have an inverse because it is cannot be injective.

---

4 Let $g : A \to B$ be a function. Under what condition(s) on g are the following statements true?

(a) $\forall b \in B.\ \text{Im}_g(\text{PreIm}_g(\{b\})) = \{b\}$;

(b) $\forall a \in A.\ \text{PreIm}_g(\text{Im}_g(\{a\})) = \{a\}$;

(c) $\exists b \in B.\ \text{PreIm}_g(\{b\}) = \varnothing$.

Solution:

(a) True for all functions $g : A \to B$, since $x \in \text{PreIm}_g(\{b\})$ if and only if $g(x) = b$.

(b) True for injective functions $g : A \to B$, since $\text{Im}_g(\{a\}) = \{g(a)\}$ and so $\text{PreIm}_g(\text{Im}_g(\{a\})) = \{a' \in A : g(a') = g(a)\} = \{a\}$.

(c) True for non-surjective functions $g : A \to B$, since the assertion $\text{PreIm}(\{b\}) = \varnothing$ is precisely the assertion that $\neg\exists a \in A.\ g(a) = b$.

---

5 Prove that if $f : [a] \to [b]$ is surjective then $a \geqslant b$.

Solution: By induction on a. If $a = 0$ then $[a] = \varnothing$, so for f to be surjective we need $[b] = \varnothing$, and hence $b = 0$. So $a \geqslant b$.

Suppose the assertion is true for a, and let $f : [a+1] \to [b]$ be surjective. Consider $f' : [a] \to [b]$ defined by $f'(x) = x$ for all $x \in [a]$. If f' is surjective then $a \geqslant b$ by the induction hypothesis, so certainly $a + 1 \geqslant b$. If f' is *not* surjective then $a + 1$ must be the only element of $[a+1]$ mapping to $f(a+1)$, so the function $f'' : [a] \to [b] \setminus \{f(a+1)\}$ defined by $f''(x) = f(x)$ is well-defined. Moreover f'' is surjective, since if $y \in [b] \setminus \{f(a+1)\}$ then $y = f(x)$ for some $x \in [a+1] \setminus \{a+1\} = [a]$, so $y = f''(x)$. By induction hypothesis again we have $a \geqslant b - 1$, and hence $a + 1 \geqslant b$.

---

6 Prove that $f : A \to B$ is injective if and only if $\forall b \in B.\ |\text{PreIm}_f(\{b\})| \leqslant 1$.

Solution: Suppose $f : A \to B$ is injective, and let $b \in B$ be arbitrary. If $\text{PreIm}_f(\{b\}) = \varnothing$ then we're fine, so suppose $\text{PreIm}_f(\{b\}) \neq \textit{varnothing}$ and let $a \in \text{PreIm}_f(\{b\})$. If $a' \in A$ with $a' \in \text{PreIm}_f(\{b\})$ then $f(a') = b = f(a)$, so by injectivity we have $a' = a$. Hence $\text{PreIm}_f(\{b\}) = \{a\}$. In any case, the cardinality of $\text{PreIm}_f(\{b\})$ is $\leqslant 1$.

Conversely, suppose $\forall b \in B.\ |\text{PreIm}_f(\{b\}) \leqslant 1$. Let $a, a' \in A$ be arbitrary and suppose $f(a) = f(a')$. Then $a, a' \in \text{PreIm}_f(\{f(a)\})$, so $a = a'$ since this set has only one element.

---

7 Two sets A and B are defined by:

$$A = \{n \in \mathbb{Z} : n \equiv 2 \bmod 3\} \quad \text{and} \quad B = \{n \in \mathbb{Z} : n \equiv 0 \bmod 7\}$$

Find a bijection from A to B and give an expression for its inverse.

Solution: Notice that $A = \{2 + 3k : k \in \mathbb{Z}\}$ and $B = \{7k : k \in \mathbb{Z}\}$. (Implicitly what we've just done is define bijections $\mathbb{Z} \to A$ and $\mathbb{Z} \to B$.) The idea is: identify $2 + 3k$ with $7k$. We can do this by expressing $n = 2 + 3k$ in terms of k and subbing into $7k$; and vice versa.

So define $f : A \to B$ by $f(n) = 7 \cdot \frac{n-2}{3}$, and define $F : B \to A$ by $F(m) = \frac{m}{7} \cdot 3 + 2$. You need to check that these functions are well-defined and their composites are identities.

---

8 Find a subset $A \subseteq \mathbb{R}$ for which the function $f : A \to \mathbb{R}$ given by $f(x) = x^2 - 3x + 2$ is injective. (Bonus points if A is *maximal*, i.e. if $A \subsetneq B \subseteq \mathbb{R}$ then $\widehat{f} : B \to \mathbb{R}$ given by $\widehat{f}(x) = x^2 - 3x + 2$ is *not* injective.)

Solution: We can write $x^2 - 3x + 2 = (x - \frac{3}{2})^2 + k$ for some constant k (whose value doesn't matter [why?]). Let $A = \{x \in \mathbb{R} : x \geqslant \frac{3}{2}\}$. Then $\widehat{f} : A \to \mathbb{R}$ given by $\widehat{f}(x) = x^2 - 3x + 2$ is injective, since $x \geqslant \frac{3}{2}$ if and only if $x - \frac{3}{2} \geqslant 0$, and every real number has a unique nonnegative square root. And A is maximal: if $B \supsetneq A$ then there is some $b \in B$ with $b < \frac{3}{2}$, and then $f(b) = f(3 - b)$. (You can check this.)

Solutions to advanced questions

For these problems I've left a few more gaps than usual are left for you to fill in.

A1 A function $g : A \to B$ is *inflationary* if $g(x) > x$ for all $x \in A$ (where $A, B \subseteq \mathbb{R}$).

Prove that there exists an inflationary bijection $g : \mathbb{Z} \to \mathbb{Z}$, but that there does not exist an inflationary bijection $\mathbb{N} \to \mathbb{N}$. Does there exist an inflationary bijection $\mathbb{Z} \to \mathbb{N}$?

Solution: The function $g : \mathbb{Z} \to \mathbb{Z}$ defined by $g(n) = n + 1$ for all $n \in \mathbb{Z}$ is inflationary, since $n + 1 > n$ for all n. No inflationary bijection $f : \mathbb{N} \to \mathbb{N}$ can exist since if $n \in \mathbb{N}$ then $f(n) > n \geqslant 1$, so $1 \notin \mathrm{Im}_f(\mathbb{N})$ and f fails surjectivity. There does exist an inflationary bijection $h : \mathbb{Z} \to \mathbb{N}$: for example, define $h(n) = 2n$ if $n \in \mathbb{N}$, and $h(n) = 1 - 2n$ if $n \in \mathbb{Z} \setminus \mathbb{N}$. (The positive integers get mapped to even naturals (and certainly $2n > n$ if $n > 0$), and the negative integers get placed in the odd positions.)

A2 A function $h : \mathbb{Z} \to \mathbb{Z}$ is *periodic* if there exists $m \in \mathbb{N}$ such that $\forall x \in \mathbb{Z}.\ h(x + m) = h(x)$. Prove that the set of periodic functions $\mathbb{Z} \to \mathbb{Z}$ is countable.

Solution: Let P_m denote the set of all m-periodic functions $\mathbb{Z} \to \mathbb{Z}$, i.e. those for which $h(x + m) = h(x)$ for all $x \in \mathbb{Z}$. Any function $h \in P$ is determined uniquely by the values of

$h(1), \cdots, h(m-1), h(m)$. Indeed, if $t \in \mathbb{Z}$ then there is a unique $k \in [m]$ with $t \equiv k \bmod m$, and it is easy to prove by induction that if $t \equiv k \bmod m$ then $h(t) = h(k)$.

So there is a bijection $F : P_m \to \mathbb{Z}^m$ given by $F(h) = (h(1), h(2), \cdots, h(m))$. (You can check the details.) But $\mathbb{Z}^m$ is a finite product of countable sets, so is countable; and hence the set of all periodic functions, which is equal to $\bigcup_{m \in \mathbb{N}} P_m$, is a countable union of countable sets, so is countable.

A3 Let Σ be a countably infinite set. Let Σ^* be the set of finite strings whose symbols come from Σ, and Σ^∞ be the set of infinite strings whose symbols come from Σ. Prove that Σ^* is countable but Σ^∞ is uncountable.

Solution: There is a bijection $\Sigma^* \to \bigcup_{n \in \mathbb{N} \cup \{0\}} \Sigma^n$, since Σ^n is just the set of strings of length n (which is finite) and every $w \in \Sigma^*$ has some finite length. But each Σ^n is a finite product of countable sets, so is countable, and so Σ^* is a countable union of countable sets, so is countable.

However Σ^∞ is uncountable: indeed, if $\sigma, \tau \in \Sigma$ are two distinct elements, then there is a bijection $\{\sigma, \tau\}^{\mathbb{N}} \to \{0, 1\}^{\mathbb{N}}$ given by replacing σ by 0 and τ by 1 in the string, and we know the latter set is uncountable, hence so is $\{\sigma, \tau\}^{\mathbb{N}}$; but $\{\sigma, \tau\}^{\mathbb{N}} \subseteq \Sigma^\infty$, so Σ^∞ is also uncountable.

A4 A real number x is *algebraic* if x is a root of a polynomial with integer coefficients, i.e. if there exists $k \in \mathbb{N}$ and integers $a_0, a_1, \cdots, a_k$ such that

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_k x^k = 0$$

Prove that the set of algebraic real numbers is countably infinite.

Solution: Every polynomial with integer coefficients can be written uniquely as

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_k x^k = a_k (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_k)$$

where $\alpha_1, \cdots, \alpha_k \in \mathbb{R}$ are the roots of the polynomial and $\alpha_1 \leqslant \alpha_2 \leqslant \cdots \leqslant \alpha_k$.

Let A_k be the set of roots of polynomials of degree k.

$$f_k : [k] \times \mathbb{Z}^{k+1} \to A_k$$

given by $f_k(i, a_0, a_1, \cdots, a_k) = \alpha_i$, where

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_k x^k = a_k (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_k)$$

(That is, $f_k(i, a_0, a_1, \cdots, a_k)$ is the ith largest root of the polynomial whose coefficients are $a_0, a_1, \cdots, a_k$.)

But $[k] \times \mathbb{Z}^{k+1}$ is a finite product of (finite or) countable sets, so is countable, and hence A_k is countable; and the set of all algebraic real numbers is $\bigcup_{k \in \mathbb{N}} A_k$, which is a countable union of countable sets, so is countable.

A5 Let X be a set such that, for all $f : X \to X$, the following holds:

$$\forall x \in X.\ \exists n \in \mathbb{N}.\ f^n(x) = x \quad \Rightarrow \quad \exists n \in \mathbb{N}.\ \forall x \in X.\ f^n(x) = x$$

where $f^n = \underbrace{f \circ f \circ \cdots \circ f}_{n \text{ times}}$. Prove that X is finite.

Solution: Intuitively, this is saying that if for every element there is some finite iteration of f that gets us back to where we started, then there is some particular number such that iterating that many times works for all x. (And sure, in the finite case, just take the lcm of all the lengths of iterations.)

We prove the contrapositive. That is, if X is infinite then there is a function $f : X \to X$ such that $\forall x \in X.\ \exists n \in \mathbb{N}.\ f^n(x) = x$ holds but $\exists n \in \mathbb{N}.\ \forall x \in X.\ f^n(x) = x$ fails.

If X is infinite then it contains a countably infinite subset $X_0 = \{x_n : n \in \mathbb{N}\}$ say. We'll construct a function f that induces loops of arbitrarily large finite size in X_0. To this end, define $f : X \to X$ so that:

- $f(x) = x$ for all $x \in X - X_0$;
- On X_0: send $x_1 \to x_1$, $x_2 \to x_3 \to x_2$, $x_4 \to x_5 \to x_6 \to x_7 \to x_4$, and more generally

$$x_{2^k} \to x_{2^k+1} \to \cdots \to x_{2^k+(2^k-2)} \to x_{2^k+(2^k-1)} \to x_{2^k}$$

More precisely,

$$f(x_n) = \begin{cases} x_{n+1} & \text{if } 2^k \leqslant n < 2^{k+1} - 1 \\ x_{2^k} & \text{if } n = 2^{k+1} - 1 \end{cases}$$

By construction, for any element x there is some finite iteration f^n of f such that $f^n(x) = x$. But no n works for all x: indeed, given n, take k such that $2^k > n$, then $f^n(x_{2^k}) = x_{2^k+n} \neq x$.

A6 Let S be a collection of pairwise disjoint intervals of $\mathbb{R}$ of positive length. That is,

$$S = \{(a_i, b_i) \subseteq \mathbb{R} : i \in I\}$$

with $a_i < b_i$ for all i, and if $i \neq j$ then $(a_i, b_i) \cap (a_j, b_j) = \varnothing$. Prove that S is countable. *(For clarity, $(a, b) = \{x \in \mathbb{R} : a < x < b\}$, not the ordered pair.)*

Solution: There is an injection $f : S \to \mathbb{Q}$ by defining $f(a_i, b_i) = q$ for some arbitrarily (but fixed) chosen $q \in \mathbb{Q}$ with $a_i < q < b_i$. But $\mathbb{Q}$ is countable, hence so is S.

A7 The *successor* of a set x is the set $x^+ = x \cup \{x\}$. Define $\bar{n}$ for $n \in \mathbb{N} \cup \{0\}$ as follows:

$$\overline{0} = \varnothing \quad \text{and} \quad \overline{n+1} = \overline{n}^+ \text{ for all } n \in \mathbb{N} \cup \{0\}$$

For example, $\bar{1} = \varnothing \cup \{\varnothing\} = \{\varnothing\}$ and $\bar{2} = \bar{1} \cup \{\bar{1}\} = \{\varnothing, \{\varnothing\}\}$. Prove that $|\bar{n}| = n$ for all $n \in \mathbb{N} \cup \{0\}$.

Solution: By induction on n. By definition $\bar{0} = \varnothing$, so $|\bar{0}| = |\varnothing| = 0$. Suppose $|\bar{n}| = n$. Now $n \bar{+} 1 = \bar{n} \cup \{\bar{n}\}$. Since $\bar{n} \notin \bar{n}$, we have $\bar{n} \cap \{\bar{n}\} = \varnothing$, and hence

$$|n \bar{+} 1| = |\bar{n} \cup \{\bar{n}\}| = |\bar{n}| + |\{\bar{n}\}| = n + 1$$

where the second $=$ sign follows from the fact that $|A \cup B| = |A| + |B|$ if A, B are disjoint finite sets, and the third $=$ sign follows from the induction hypothesis.

A8 Does there exist a set S such that $|\mathbb{N}| < |S| < |\mathcal{P}(\mathbb{N})|$? *(Don't spend too much time on this.)*

Solution: This was a trick question since it's impossible (from our foundational viewpoint) to answer this question. That is, in the standard set of axioms of set theory, this is (provably) unprovable. There is a set called ω_1 such that $|\mathbb{N}| < |\omega_1|$ and no S satisfies $|\mathbb{N}| < |S| < |\omega_1|$; so the question becomes: is $|\mathcal{P}(\mathbb{N})| = |\omega_1|$? An answer of 'yes' is called the *continuum hypothesis*. The continuum hypothesis is independent, that is, it is known that neither answer ('yes' or 'no') leads to a contradiction.

One consequence of this independence is that, even if we assume the continuum hypothesis is false, it would be impossible to explicitly define a function $f : \omega_1 \to \mathcal{P}(\mathbb{N})$ which is injective but not surjective.

If this piques your interest and/or blows your mind in a good way, consider studying set theory in the future (21-329, 21-602, 21-702).