Math 25a Homework 2 Solutions part 1

Ivan Corwin and Alison Miller.

1 Injections, surjections, bijections

(1) Prove that the composition of two injective functions is an injective function and that the composition of two surjective functions is a surjective function.

Solution. Suppose f and g are injections. $f \circ g(x) = f \circ g(y) \Rightarrow g(x) = g(y) \Rightarrow x = y$, so $f \circ g$ is an injection.

Suppose f and g are surjections. Consider $c \in \text{Img}(g)$. $\exists b$ s.t. $g(b) = c$ and subsequently a s.t. $f(a) = b$. Then $f \circ g(a) = c$, so $f \circ g$ is a surjection.

□

(2) Let $f : A \to B$ be a function. Show that the following are equivalent.

(a) There exists a function $g : B \to A$ such that $g(f(x)) = x$ for all $x \in X$ and $f(g(y)) = y$ for all $y \in Y$.

(b) f is a bijection.

Solution.

$\Rightarrow$: Suppose $f(x) = f(y)$. Then $x = g(f(x)) = g(f(y)) = y$, so f is injective. Take any y. $f(g(y)) = y$, so there $\exists x$ s.t. $f(x) = y$. So f is surjective. Therefore, f is bijective.

$\Leftarrow$: Take $g(y) =$ the element in$f^{-1}(y)$ for $y \in B$. Since f is a bijection, we know that $f^{-1}(y)$ exists and consists of exactly one element, so g is well-defined. Then $g(f(x)) = x$ and $f(g(y)) = y$ follows. □

(3) Let $f : \mathbb{R} \to \mathbb{R}$ be a function. We say that f is *strictly increasing* if $f(x) < f(y)$ whenever $x < y$.

(a) Show that if f is strictly increasing, it is an injection. Must it be a surjection?

(b) Suppose f is a bijection and $f(0) = 0$ and $f(1) = 1$. Does it follow that f is strictly increasing?

Solution.

- Suppose $f(x) = f(y)$ and $x \neq y$, then WLOG $x > y$. But by definition of strictly increasing, $f(x) > f(y)$, a contradiction. So $x = y$, and f is an injection. It does not have to be a surjection, however, as exemplified by

$$f(x) = \begin{cases} x - 1 & x \leq 0 \\ x & x > 0 \end{cases}$$

.

- No. Consider

$$f(x) = \begin{cases} 1/x & x \neq 0 \\ 0 & x = 0 \end{cases}$$

□

(5) Give an explicit bijection between each of the following sets (see Rudin page 31 for the notation):
(a) $[1, 2]$ and $[3, 7]$
(b) $(0, 1)$ and $(0, \infty)$
(c) $[0, 1]$ and $[0, 1)$
(d) $\mathbb{R} \times \mathbb{R}$ and $\mathbb{R}$ *(Hint: see decimal expansions ...)*

Solution.

(a) Let $X = [1, 2]$, $Y = [3, 7]$. Consider $f : X \to Y$, $f(x) = 4x - 1$.

(b) $(0, 1)$ and $(0, \infty)$ Let $X = (0, 1)$, $Y = (0, \infty)$. Consider $f : X \to Y$, $f(x) = 2\sin(\pi x)/(1 - \cos(\pi x))$. In fact, f takes every point with positive abscissa on the unit circle centered around $(0, 1)$, and maps it to the intersection of the line through the point and $(0, 2)$ and the x-axis.

(c) $[0, 1]$ and $[0, 1)$ Let $X = [0, 1]$, $Y = [0, 1)$. Take a countable subset $\{x_i\}$ of X with $x_1 = 1$ (letting $x_i = 1/i$, for example). Let f take x_i to x_{i+1}, and x to x $\forall x \notin \{x_i\}$.

(d) $\mathbf{R} \times \mathbf{R}$ and $\mathbf{R}$ We know that there is a bijection from $(0, 1)$ to $\mathbf{R}$ by taking $f(x) = \tan((x - 1/2)\pi)$. It then suffices to supply a bijection from $(0, 1) \times (0, 1)$ to $(0, 1)$. To do this, we first consider each element in $(0, 1)$ as a decimal, using an infinite sequence of 0's instead of 9's when applicable. Then we divide $x \in (0, 1)$, $x = 0.x_1x_2x_3\ldots$ into pieces $x = 0.X_1X_2X_3\ldots$, where each piece starts from the end of the previous piece and ends when it encounters a non-9 digit (which exists by our construction of the decimals). Therefore, for each pair $(x, y) \in (0, 1) \times (0, 1)$, we can split x and y into $0.X_1X_2X_3\ldots$ and $0.Y_1Y_2Y_3\ldots$. Then construct $z = 0.X_1Y_1X_2Y_2\ldots$. This is a bijection since it cannot end in repeating 9's, and it is a reversible process. □

2 Fields, rational and irrational numbers

(1) Given $x \in \mathbb{R}$ with $x > 0$ and an integer $k \geq 2$, define $a_0, a_1, \ldots$ recursively by setting $a_0 = \lfloor x \rfloor$ (this means the largest integer which is less than or equal to x) and a_n to be the largest integer such that

$$a_0 + \frac{a_1}{k} + \frac{a_2}{k^2} + \cdots + \frac{a_n}{k^n} \leq x$$

(a) Show that $0 \leq a_i \leq k - 1$ for each $i \geq 1$.
(b) Let $r_n = a_0 + \frac{a_1}{k} + \ldots \frac{a_n}{k^n}$. Show that $\sup\{r_0, r_1, \ldots\} = x$.
(Note: The expression $r = a_0 + \frac{a_1}{k} + \frac{a_2}{k^2} + \ldots$ is called the base-k expansion of $x \in \mathbb{R}$. If $k = 10$, this is the decimal expansion of x. The next part of the problem shows that the base-k expansion of x is almost unique.)
(c) Show that if we have sequences $a_0, a_1, \ldots$ and $b_0, b_1, \ldots$ such that
(I) $0 \leq a_i \leq k - 1$ and $0 \leq b_i \leq k - 1$

(II) $a_0 + \frac{a_1}{k} + \frac{a_2}{k^2} + \cdots = b_0 + \frac{b_1}{k} + \frac{b_2}{k^2} + \ldots$

(III) for each $N > 0$ there exists and $n > N$ and $m > N$ such that $a_n \neq k-1$ and $b_m \neq k-1$ then $a_i = b_i$ for all i.

(Hint: This last condition just says that neither sequence ends with an infinite sequence of $(k-1)$'s. You may need to use the fact that if $0 \leq |x| < 1$, then $1 + x + x^2 \cdots = \frac{1}{1-x}$.)

Solution.

(a) Since

$$a_0 + \frac{a_1}{k} + \frac{a_2}{k^2} + \ldots + \frac{a_n}{k^n} \leq x$$

Taking $a_{n+1} = 0$ gives

$$a_0 + \frac{a_1}{k} + \frac{a_2}{k^2} + \ldots + \frac{a_{n+1}}{k^{n+1}} \leq x$$

and since we are picking the largest possible a_{n+1}, $a_{n+1} \geq 0$. Suppose $a_{n+1} > k-1$. Then $\frac{a_{n+1}}{k^{n+1}} \geq \frac{1}{k^n}$. So for a_n we could have picked a_n+1 instead, since that gives an extra contribution of $\frac{1}{k^n}$. So $a_{n+1} \leq k-1$.

(b) Clearly $x \geq r_n \forall n$. Now, we just need to make sure there does not $\exists x' < x$ s.t. $x' \geq r_n \forall n$. Take n large enough s.t. $\frac{1}{k^n} \leq x - x'$. Therefore, adding 1 to a_n would still satisfy our inequality in the construction of a_n, which is a contradiction since we picked the largest possible a_n.

(c) Consider

$$t_n = \frac{a_n}{k^n} + \frac{a_{n+1}}{k^{n+1}} + \ldots$$

. An unattainable upper bound of of t_n occurs when all of the a_i equal $k-1$, which gives $\frac{k-1}{k^n}(1 + \frac{1}{k} + \frac{1}{k^2} + \ldots) = \frac{1}{k^{n-1}}$. We define $\{s_n\}$ similarly, with b_n in place of a_n as they occur. We take the smallest i s.t. $a_i \neq b_i$. WLOG, $a_i < b_i$. Then $\frac{a_i}{k^i} + t_{i+1} = \frac{b_i}{k^i} + s_{i+1}$. However, $\frac{b_i}{k^i} - \frac{a_i}{k_i} \geq \frac{1}{k^i}$ and $t_{i+1} - s_{i+1} < \frac{1}{k^{i+1-1}} - 0 = \frac{1}{k^i}$, a contradiction. So $a_i = b_i \forall i$. □

(2) Use the elementary order axioms to prove the following properities:

(a) If $a \leq b$ and $c \leq d$, then $a + c \leq b + d$.

(b) If $x, y \geq 0$ and $x^2 > y^2$, then $x > y$.

(c) $\mathbb{R}$ is not bounded above.

Solution.

(a) Since $a \leq b$ it follows that $a + c \leq b + c$. Similarly since $c \leq d$ it follows that $c + b \leq d + b$. Transitivity implies then that $a + c \leq b + c \leq b + d$ and therefore $a + c \leq b + d$.

(b) Assume from the point of contradiction that $x \leq y$. Therefore $0 \leq x \leq y$. Then since $y - x \geq 0$ and $x \geq 0$ it follows that $x(y - x) \geq 0$, or that $xy \geq x^2$. Similarly since $x \leq y$ and $y \geq 0$, $xy \leq y^2$. Therefore $x^2 \leq xy \leq y^2$ which implies $x^2 \leq y^2$, a contradiction. Thus $x > y$.

(c) Assume from the point of contradiction that $\mathbf{R}$ is bounded from above. Therefore it has a supremum $a \in \mathbf{R}$. $\mathbf{R}$ also contains a positive element (such as 1) and hence by ordering (first part of the question), $a + 1 > a$. Yet $a + 1 \in \mathbf{R}$ by closure under addition. Therefore a is not the supremum, a contradiction.

□

(3) (a) Prove that there is exactly one way to make $\mathbb{Q}$ into an ordered field.

Hint: Assume that there is another order $x \prec y$ on $\mathbb{Q}$ satisfying the axioms for an ordered field and show that $x \prec y$ if and only if $x < y$.

(b) Let p be prime. Show that the field $\mathbb{Z}/p\mathbb{Z}$ cannot be made into an ordered field. Show that $\mathbb{C}$ cannot be made into an ordered field.

Solution.

We know that $0 \prec 1$, from which $a \prec a + 1 \forall a \in \mathbf{Z}$. By transitivity $a \prec b$ iff $a < b$, so $a \prec 0 \Leftrightarrow a < 0 \Leftrightarrow 1/a \prec 0 \Leftrightarrow 1/a < 0$ (since $(1/a)a = 1$). This gives us $b/a \prec 0 \Leftrightarrow b/a < 0 \forall \{a, b\}$. So $a/b \prec c/d \Leftrightarrow (ad - bc)/(bd) \prec 0 \Leftrightarrow (ad - bc)/(bd) < 0 \Leftrightarrow a/b < c/d$.

$\mathbf{Z}/p\mathbf{Z}$: Suppose it can be made into an ordered field. Then $0 < 1$. Adding 1 to both sides gives $1 < 2$. Continuing on, $0 < 1 < 2 \ldots p = 0$, a contradiction.

$\mathbf{C}$: Suppose it can be made into an ordered field. Then $i > 0$ or $i < 0$. In either case, $i^2 > 0$. But $i^2 = -1 < 0$, a contradiction. □

(4) (a) Show that $\sqrt{2} + \sqrt{3}$ is irrational.

(b) If a and b is irrational, must $a + b$ be irrational?

Solution.

(a)

$$\begin{aligned} \sqrt{2} + \sqrt{3} \in \mathbf{Q} &\Rightarrow 2 + 3 + 2\sqrt{6} \in \mathbf{Q} \\ &\Leftrightarrow 5 + 2\sqrt{6} \in \mathbf{Q} \\ &\Leftrightarrow \sqrt{6} \in \mathbf{Q} \end{aligned}$$

Suppose $\sqrt{6} = m/n$, $(m, n) = 1$. Then $6n^2 = m^2$, so $2|m$. But then $m = 2m'$, so $3n^2 = 2m'^2$, and $2|n$, a contradiction since $(m, n) = 1$. So the original number is not rational.

(b) No. Consider $-\sqrt{2} + \sqrt{2} = 0$. Both numbers are irrational, but their sum is rational. □

(5) Show that between any two distinct real numbers x, y, there is an irrational number.

Solution. Note that $\sqrt{2} \notin \mathbf{Q}$. Without loss of generality, take $x < y$ both real. Then there exists a $q \in \mathbf{Q}$ such that $x < q < y$, and furthermore a q' such that $x < q < q' < y$. Since $q' - q > 0$, $\sqrt{2}/(q' - q)$ exists as is in $\mathbf{R}$. Therefore there exists an $n \in \mathbf{N}$ such that $n > \sqrt{2}/(q' - q)$. Thus $x < q < q + \sqrt{2}/n < q' < y$. However $q + \sqrt{2}/n \notin \mathbf{Q}$ and therefore between any two distinct reals there exists an irrational. □

(6) Rudin pg 22 q. 6 (This is an exercise to verify that indices behave how you would expect them to behave. That is, you know how indices work when they are integers, what about when they are rational and real numbers?)

Solution.

(a) We note that for $m', n' \in \mathbf{N}$, $(b^{m'})^{n'} = (b^{n'})^{m'} = b^{n'm'}$. This follows from the definition of exponentiation to an integral power. Now, let $x = (b^m)^{\frac{1}{n}}$ and $y = (b^p)^{\frac{1}{q}}$. Then, $x^n = b^m$ and $y^q = b^p$, and remembering that $mq = np$, we get $x^{nq} = b^{mq} = b^{np} = y^{nq}$. Then, $x^{nq} - y^{nq} = (x-y)(x^{nq-1} + x^{nq-2}y + \cdots + xy^{nq-2} + y^{nq-1})$, and as the second term in the product is strictly positive, we must have $x = y$.

(b) For $x, y > 0$, $(xy)^{\frac{1}{n}} = x^{\frac{1}{n}} y^{\frac{1}{n}}$. Indeed, we simply note that by the commutative and associative properties we have $\left[x^{\frac{1}{n}} y^{\frac{1}{n}}\right]^n = \left[x^{\frac{1}{n}}\right]^n \left[y^{\frac{1}{n}}\right]^n = xy$.

Then, say $r = \frac{m}{n}$ and $s = \frac{m'}{n}$ (we can choose a common denominator, as all representatives are equivalent by (a)). Then, $b^r b^s = b^{\frac{m}{n}} b^{\frac{m'}{n}} = (b^m)^{\frac{1}{n}} (b^{m'})^{\frac{1}{n}} = \left[b^m b^{m'}\right]^{\frac{1}{n}} = \left[b^{m+m'}\right]^{\frac{1}{n}} = b^{\frac{m+m'}{n}} = b^{r+s}$.

(c) We note that for fixed n, $x \mapsto x^n$ is a strictly increasing map on the positive reals (for $x > y$, $x^n - y^n = (x-y)(x^{n-1} + x^{n-2}y + \ldots + y^{n-1} > 0)$. That is, for $x_1, x_2 > 0$, we have $x_1 > x_2 \Leftrightarrow x_1^n > x_2^n$. Then, it follows that $x \mapsto x^{\frac{1}{n}}$ must also be a strictly increasing map on the positive reals.

Also note that for fixed $b > 1$, $n \mapsto b^n$ is an increasing map on the integers (by an easy induction).

Then, given $b > 1$, and $q_1, q_2 \in \mathbb{Q}$, with $q_1 > q_2$, we can write $q_1 = \frac{m_1}{n}$ and $q_2 = \frac{m_2}{n}$, $m_1 > m_2$, and we see that $b^{q_1} = (b^{m_1})^{\frac{1}{n}} > (b^{m_2})^{\frac{1}{n}} = b^{q_2}$. So, for $b > 1$, $q \mapsto b^q$ is a strictly increasing function on the rationals.

Now, for $r \in \mathbb{Q}$, let $S = \sup B(r) = \sup\{b^t | t \in \mathbb{Q}, t \leq r\}$. We observe that $b^r \in B(r)$, so $S \geq b^r$. But, for $b^t \in B(r) \setminus \{b^r\}$, we have $t < r$, so $b^t < b^r$, and so in fact $S = b^r$.

(d) We use the definition given in (c) along with the result of (a) for rationals:

$$\begin{aligned} b^x b^y &= \sup\{b^t | t \in \mathbb{Q}, t \leq x\} \sup\{b^t | t \in \mathbb{Q}, t \leq y\} \\ &= \sup\{b^{t_1} b^{t_2} | t_1, t_2 \in \mathbb{Q}, t_1 \leq x, t_2 \leq y\} \\ &= \sup\{b^{t_1+t_2} | t_1, t_2 \in \mathbb{Q}, t_1 \leq x, t_2 \leq y\} \\ &= \sup\{b^{t_1+t_2} | t_1 + t_2 \in \mathbb{Q}, t_1 + t_2 \leq x + y\} = b^{x+y} \end{aligned}$$

There are two steps of this argument that need further justification: the first is the step from the first to the second line (combining the two supremums). Let X, Y be two sets of positive rationals having finite upper bounds and denote $XY = \{xy | x \in X, y \in Y\}$. Then, we claim $\sup X \sup Y = \sup XY$. Note that $xy < x \sup Y < \sup X \sup Y$ (as all quantities involved are positive), so $\sup XY \leq \sup X \sup Y$. Suppose for contradiction that $\sup XY = t < \sup X \sup Y$. Let $\delta = \sup X \sup Y - t$, and take $q \in (t, \sup X \sup Y - \frac{\delta}{2}) \cap \mathbb{Q}$. Then, take $0 < h < \frac{\delta}{2 \sup Y}$ and $q_x \in (\sup X - h, \sup X) \cap \mathbb{Q}$. Then, $\frac{\sup X \sup Y - \frac{\delta}{2}}{\sup_X - h} > \frac{q}{q_x}$

must be an upper bound for Y. But, $\frac{\sup X \sup Y - \frac{\delta}{2}}{\sup X - h} < \frac{\sup X \sup Y - \frac{\delta}{2}}{\sup X - \frac{\delta}{2 \sup Y}} = \sup Y$. This yields a contradiction, proving our claim.

The second, is substantially more subtle than it seems, and I don't think that anyone got this part of the problem. is that, in order to pass from the next-to-last equation to the last, we would like to show that any rational number $t \leq x + y$ can in fact be expressed as the sum of two rational numbers t_1, t_2, where $t_1 \leq x$, $t_2 \leq y$. Unfortunately, this need not be true. It is true, however, than any rational number $t < x + y$ can be expressed as a sum $t_1 + t_2$ where $t_1 < x_1$, $t_2 < x_2$. This is a consequence of the definition of $x + y$ via Dedekind cuts, but it can also be shown as follows: $t - y < x$ and the rationals are dense in the reals, so we can take t_1 to be any rational number with $t - y < t_1 < x$. Then let $t_2 = t - t_1$, which is rational because rationals are closed under subtraction. Also $t_2 = t - t_1, t - (t - y) = y$. So we have expressed $t = t_1 + t_2$ in the desired way.

Unfortunately, if x and y are irrational and $x + y$ is irrational, it is impossible to write $x + y = t_1 + t_2$ where $t_1 \leq x$, $t_2 \leq y$. So we know that the set $\{t_1 t_2 \mid t_1 < x, t_2 < y, t_1, t_2 \in \mathbb{Q}\}$ is either the set of all rational numbers $\leq x + y$ or the set of all rational numbers $< x + y$. In the first case, our argument goes through, so we just have to show that the second case doesn't make a difference, by the following series of technical lemmas (see the note on lemmas after problem 3.5. In my writeup I've put the most technical bits to the end to make sure you get the main ideas, but this method of saying "oops... there's this annoying special case... let's tack on a lemma at the end to deal with it" is generally not the best way to organize a proof):

Lemma. *The greatest lower bound (infimum) of the set $S = \{b^t \mid t > 0, t \in \mathbb{Q}\}$ is equal to 1.*

Proof. We know from the previous part that $t \mapsto b^t$ is an increasing function. Hence for $t > 0$, $b^t > b^0 = 1$, so 1 is a lower bound. Hence S is bounded below, and $\inf(S)$ exists. Suppose by way of contradiction that $\inf(S) > 1$. Then $\inf(S)^2 > \inf(S)$ is not a lower bound for S, and we can find a rational $t > 0$ such that $b^t < \inf(S)^2$. Because t is rational, we can use part b) to write $b^t = (b^{\frac{t}{2}})^2 < \inf(S)^2$. By 2.2a), $b^{\frac{t}{2}} < \inf(S)$, but $\frac{t}{2}$ is positive rational, so $b^{\frac{t}{2}} \in S$, contradicting the definition of $\inf(S)$. Hence the only possibility is that $\inf(S) = 1$. □

Lemma. *For r a rational number, the supremums $\sup\{b^t \mid t < r, t \in \mathbb{Q}\}$ and $\sup\{b^t \mid t \leq r, t \in \mathbb{Q}\}$ are both equal to b^r.*

Proof. We already know (by part c) that the second supremum equals b^r, so we need only deal with the first one, which is bounded above by b^r for the same reason. Hence we need only show that for any real $M < b^r$, M is not an upper bound for $\{b^t \mid t < r, t \in \mathbb{Q}\}$. Indeed, for such an M, $\frac{b^r}{M} > 0$, so by the previous lemma we can find an $s \in \mathbb{Q}$, $s > 0$, such that $b^s < \frac{b^r}{M}$. Since r, s are both rational, we can apply part b) to deduce $b^{r-s} = \frac{b^r}{b^s} > M$. But $r - s$ is rational and less than r, so $b^{r-s} \in \{b^t \mid t < r, t \in \mathbb{Q}\}$. Hence M is not an upper bound. □

So, returning to our problem, if $\{t_1 t_2 \mid t_1 < x, t_2 < y, t_1, t_2 \in \mathbb{Q}\}$ is the set of all rational numbers $< x + y$, either $x + y$ is irrational, in which case this is the same as the set of all

rationals $\leq x+y$, or $x+y$ is rational, in which case the previous lemma shows that we can change the $<$ sign to a $\leq$ sign with no difference to the supremum in question. □

Problem 2.1. *Rudin pg. 22, Exercise 7 (It's long, so I won't reproduce it here)*

Solution.

(a) Note that $b^1 - 1 \geq 1(b-1)$ (in fact we have equality). Then, assuming that $b^{n-1} - 1 \geq (n-1)(b-1)$, we have:

$$b^n - 1 = b(b^{n-1} - 1) + (b-1) \geq b(n-1)(b-1) + (b-1) \geq (b-1)(n-1) + (b-1) = n(b-1)$$

Thus, by induction we have that for any positive integer n, $b^n - 1 \geq n(b-1)$.

(b) Applying part (a) to $b^{\frac{1}{n}}$ (in place of b), we get $b - 1 = (b^{\frac{1}{n}})^n - 1 \geq n(b^{\frac{1}{n}} - 1)$.

(c) Note that $b - 1 \geq n(b^{\frac{1}{n}-1} - 1)$ can be re-arranged as $b^{\frac{1}{n}} \leq 1 + \frac{b-1}{n}$. Rewriting $n > \frac{b-1}{t-1}$, we can get $t - 1 > \frac{b-1}{n}$ and $t > \frac{b-1}{n} + 1$. These inequalities combine to give us $b^{\frac{1}{n}} < t$.

(d) Take $t = y \cdot b^{-w} > 1$. Then, for $n > \frac{b-1}{t-1}$ we get $b^{\frac{1}{n}} < t$. Then, $b^{w+\frac{1}{n}} = b^w b^{\frac{1}{n}} < tb^w = y$.

(e) Take $t = \frac{b^w}{y} > 1$. Then, for $n > \frac{b-1}{t-1}$ we get $b^{\frac{1}{n}} < t = \frac{b^w}{y}$ and so $b^{-\frac{1}{n}} > yb^{-w}$. Then, $b^{w-\frac{1}{n}} = b^w b^{-\frac{1}{n}} > y$.

(f) Let $A = \{w : b^w < y\}$, and $x = \sup A$. Say $b^x > y$, then by (e) we have $b^{x-\frac{1}{n}} > y$ for some n. So, $x - \frac{1}{n} \notin A$, and so is an upper bound of A less than x, violating the definition of x as the least upper bound. Say $b^x < y$, then by (d) we have $b^{x+\frac{1}{n}} < y$ for some n. So, $x + \frac{1}{n} \in A$, and so x is not an upper bound of A, violating the definition of x as the least upper bound. Thus, we must have $b^x = y$.

(g) We will show that $x \mapsto b^x$ is an increasing function on $\mathbb{R}$ for $b > 1$. Given $x_1 < x_2$, say $b^{x_1} = \sup B(x_1)$ where $B(x_1) = \{b^q | q < r_1, q \in \mathbb{Q}\}$ and $b^{x_2} = \sup B(x_2)$ where $B(x_2) = \{b^q | q < r_2, q \in \mathbb{Q}\}$. As $B(x_1) \subset B(x_2)$, we have that $b^{x_1} \leq b^{x_2}$. Thus, our map is non-decreasing.

To see that equality does not hold, we assume that contrary – that $b^{x_1} = b^{x_2}$, with $x_1 < x_2$. Then, take $q_1 < q_2$, with $q_1, q_2 \in (x_1, x_2) \cap \mathbb{Q}$. We must have $b^{q_1} = b^{q_2}$ (as the map is non-decreasing, and $b^{x_1} = b^{x_2}$). But, we note from the argument of (6c) that $q \mapsto b^q$ is an increasing function on $\mathbb{Q}$ for $b > 1$, so $b^{q_1} < b^{q_2}$. This yields a contradiction, and so we see that $x \mapsto b^x$ is indeed increasing for $b > 1$.

As this map is strictly increasing, the value of x in (f) must be unique, for if there were an x' with $b^{x'} = y$, then we could have neither $x' > x$ nor $x' < x$. □

3 Combinatorics and Countability

(1) Verify that
(a) $\text{Card}(\mathbf{N}) = Card(\mathbf{N}^2)$

Solution. Let $\nu : \mathbf{N}^2 \to \mathbf{N}$ be given by $\nu(n,m) = \frac{(n+m)(n+m+1)}{2} + m$. Noting that $\frac{(k+1)(k+2)}{2} - \frac{k(k+1)}{2} = k+1$, we see that the sets $S_k = \{\frac{k(k+1)}{2} + n | 0 \leq n \leq k\} = \{\nu(n,m) | n+m = k\}$ form a disjoint partition of $\mathbf{N}$. So, ν is surjective, and moreover injective for two pairs (n,m), (n',m') with $n+m = n'+m'$ map to the same value if and only if $m = m'$, in which case they're the same pair. So ν is a bijection between $\mathbf{N}$ and $\mathbf{N}^2$, and $\text{Card}(\mathbf{N}) = \text{Card}(\mathbf{N}^2)$. Graphically, ν looks like this:

$$\begin{array}{cccc} 0 & 1 & 3 & 6 & \dots \\ 2 & 4 & 7 & \dots & \\ 5 & 8 & \dots & & \\ 9 & \dots & & \ddots & \end{array}$$

□

(b) $\text{Card}(\{0,1\}^{\mathbf{N}}) = \text{Card}(\mathbb{R})$

Solution. We've already shown that $\text{Card}(\mathbb{R}) = \text{Card}((0,1))$ (via the bijection $f(x) = \tan((x - 1/2)\pi)$): hence we may as well show that $\text{Card}(\{0,1\}^{\mathbf{N}}) = \text{Card}((0,1))$. Trying to explicitly construct a bijection would be somewhat unpleasant, so we will instead resort to the Schroeder-Bernstein theorem (otherwise known as Problem 1.6 on the last problem set) and construct injections each way.

We'll construct our injections with base-k expansions (as in Problem 2.1). For the injection $(0,1) \to \{0,1\}^{\mathbf{N}}$, we use base 2: for $x \in (0,1)$, x has the base-2 expansion $x = \frac{a_1}{2} + \frac{a_2}{2^2} + \frac{a_3}{2^3} + \dots$ (a_0 is always 0). We can view the sequence of digits $a_1, a_2, a_3, \dots$ as a member of $(0,1)^{\mathbf{N}}$ (it is associated with the function $n \mapsto a_n$. Hence the function f that takes x to the sequence of digits in its expansion maps $(0,1)$ to $(0,1)^{\mathbf{N}}$. This sequence is injective by problem 2b), since we can uniquely recover x from its base-2 expansion.

For an injection in the other direction, from $\{0,1\}^{\mathbf{N}} \to (0,1)$, we use base 3. Let x be an element of $\{0,1\}^{\mathbf{N}}$, which we can think of as a sequence $x_1, x_2, x_3, \dots$ of elements of $\{0,1\}$. Then we define our function $g : \{0,1\}^{\mathbf{N}} \to (0,1)$ by the base-3 expansion

$$f(x) = \frac{x_1 + 1}{3} + \frac{x_2}{3} + \frac{x_3}{3^2} + \frac{x_4}{3^2} + \dots .$$

where $a_0 = 0$, $a_1 = x_1 + 1$, and $a_n = x_n$ for $n > 1$. The function g actually maps $\{0,1\}^{\mathbf{N}}$ into the interval $(0,1)$ because for any $x \in \{0,1\}^{\mathbf{N}}$,

$$0 < \frac{1}{3} = \frac{1}{3} + \frac{0}{3^2} + \frac{0}{3^3} + \dots \leq g(x) \leq \frac{2}{3} + \frac{1}{3^2} + \frac{1}{3^3} + \dots = \frac{5}{6} < 1.$$

Additionally, for $n > 1$, $a_n = x_n \neq 2$, so we may apply 1c) to deduce that g is injective.

So we have constructed injections $f : (0,1) \to \{0,1\}^{\mathbf{N}}$ and $g : \{0,1\}^{\mathbf{N}} \to (0,1)$, and by Schroeder-Bernstein, $\text{Card}(\{0,1\}^{\mathbf{N}}) = \text{Card}((0,1)) = \text{Card}(\mathbb{R})$. □

(2) Let A, B, X be sets with $Card(A) = Card(B)$. Then show that $\text{Card}(A^X) = \text{Card}(B^X)$ and $Card(X^A) = Card(X^B)$.

(Hint: Recall that A^B is the set of all functions from B to A.)

Solution. First of all, we begin with a bit of terminology. If we have functions $f : A \to B$, and $g : B \to C$, the *composition* $g \circ f : A \to C$ is the function defined by $(g \circ f)(a) = g(f(a))$ for all $a \in A$. Also, we note that Problem 1.2 shows that if $f : A \to B$ is a bijection, there is a inverse function $g : B \to A$ such that $g \circ f$ is the identity function on A (that is, the function that sends $a \mapsto a$ for any $a \in A$), and $f \circ g$ is the identity on B. We note that compositions are associative: for any three functions $f : A \to B$, $g : B \to C$, $h : C \to D$, $(f \circ g) \circ h = f \circ (g \circ h)$, because for any $a \in A$,

$$((f \circ g) \circ h)(a) = (f \circ g)(h(a)) = f(g(h(a)) = f((g \circ h)(a)) = (f \circ (g \circ h))(a)$$

Now, because $\text{Card}(A) = \text{Card}(B)$, we can let $f : A \to B$ be a bijection, and let $g : B \to A$ be the corresponding inverse function. Then we define a function $F_1 : A^X \to B^X$ such that if $h : X \to A$ is an element of A^X, $F_1(h) = f \circ h$. Similarly, we can define a function $G_1 : B^X \to A^X$ that sends $j \mapsto g \circ j$. We claim that for any $h \in A^X$, $G_1(F_1(h)) = h$, and that for any $j \in B^X$, $F_1(G_1(h)) = h$. For the first equality:

$$G_1(F_1(h)) = f \circ (g \circ h) = (f \circ g) \circ h = h,$$

where the last step is because $f \circ g$ is the identity function, so composing with it does not affect h. By the exact same argument, $F_1(G_1(h)) = h$ for any $h \in B^X$, so F_1 and G_1 are inverses. So we can apply Problem 1.2 to see that F_1 is a bijection, and $\text{Card}(A^X) = \text{Card}(B^X)$.

We use a similar bijection to show that $\text{Card}(A^X) = \text{Card}(B^X)$: again, let $f : A \to B$ be a bijection, and $g : B \to A$ its inverse. This time we compose on the other side: for $h \in X^A$, let $F_2(h) = h \circ f \in Y^A$. Again, we can define an inverse G_2 such that $G_2(j) = j \circ g$ for $j \in Y^A$. We can show that F_2 and G_2 are in fact inverses by a formula argument analogous to the first part, so F_2 is a bijection $X^A \to X^B$, and we deduce that $\text{Card}(X^A) = \text{Card}(X^B)$.

□

(3) Let X be an infinite set.

(a) Show that for each positive integer n, there is a subset A_n of X with size n.

(c) Hence or otherwise show that any subset S of $\mathbb{N}$ is at most countable.

Solution. (a) We first note that X infinite implies X non-empty, so there is a subset of X with size 1. Now, we proceed by contradiction: Assume our claim is false. Then, there is some minimal n such that there is no subset of X with size n. Then, let A_{n-1} be a subset of size $n-1$. Consider $X \setminus A_{n-1}$. It must be empty, for otherwise we could take any element of it and adjoin it to A_{n-1} to form an n element subset of X. But then, $X = A_{n-1}$, and so X is finite. This yields a contradiction.
(b) Show that there is a countable subset of X. (Note: this implies that "countability" is the smallest possible infinite set.)

(Hint: Go look up the well-ordering theorem (equivalent to the axiom of choice).)

We invoke the well-ordering theorem (as equivalent to the axiom of choice). Let $<$ be an ordering on X, such that $(X, <)$ is well ordered.

Take any element $x_0 \in X$, and let $A_0 = \{x_0\}$. Then, for $n > 0$ recursively define $A_n = A_{n-1} \cup \{x_n\}$, where x_n is the least element in $X \setminus A_{n-1}$. Finally, let $A = \cup_{i=0}^{\infty} A_i$. The mapping $\phi : \mathbf{N} \to A$ given by $\phi(n) = x_n$ is a bijection, and so A is a countable subset of X. □(Note that this also proves the result of part (a), as well as giving an "explicit" construction for the A_n)

(c) Hence or otherwise show that any subset S of $\mathbb{N}$ is at most countable.
We have two cases:

(a) S is finite. Then it is at most countable.

(b) S is infinite. Then, by (2b) we know that there is a countable subset $X \subset S$. So, we know that there is a bijection $\phi : \mathbf{N} \to X$, and composing with the inclusion map $\iota_X : X \to S$, we get $\iota_X \circ \phi : \mathbf{N} \to S$ is an injection. Also, as $S \subset \mathbf{N}$, the inclusion map $\iota_S : S \to \mathbf{N}$ gives an injection into $\mathbf{N}$. So, we have bijections both ways, and by Schroeder-Bernstein, S is countable.

(4) Let S be a non-empty set. Show that the following are equivalent:
(a) S is at most countable (see Rudin p. 25 for a definition).
(b) there exists an injection $f : S \to \mathbb{N}$.
(c) there exists a surjection $g : \mathbb{N} \to S$.
Now define a surjective map from $\mathbb{N} \to \mathbb{Q}$ and hence show that the rational numbers are countable.

Solution. For (a) $\Rightarrow$ (b), we note that is S is at most countable, then one of the following holds:

(a) There exists a bijection $\phi : S \to A_n$, where $A_0 = \emptyset$, and $A_n = \{0, \dots, n-1\}$. Now, note that the inclusion map, $\iota : A_n \to \mathbf{N}$, is an injection, and so $f = \iota \circ \phi$ is our desired injection.

(b) There exists a bijection $\phi : S \to \mathbf{N}$. Then, ϕ is injective, and gives our desired injection.

For (b) $\Rightarrow$ (c), we note that in general given an injection $f : A \to B$, we can construct a surjection $g : B \to A$. Specifically, pick some $a_0 \in A$, and for $b \in B$ define

$$g(b) = \begin{cases} \text{the unique element of } f^{-1}(b) & b \in f(A) \\ a_0 & b \in B \setminus f(A) \end{cases}$$

We note that this is well-defined (for $b \in f(A)$, $f^{-1}(b)$ will be non-empty, and as f is an injection, it will contain at most one element), and is surjective as, for $g(f(a)) = a$ for any $a \in A$.

For (c) $\Rightarrow$ (a), we let $A_s = g^{-1}(s)$ for each element $s \in S$ (we note that the A_s are non-empty as g is surjective, and disjoint as g is a function). Then, by the axiom of choice, we can create a function $h : S \mapsto \mathbf{N}$ such that $g(s) \in A_S$, so h is an injection. Then, we have a bijection between S and $h(S) \subset \mathbf{N}$, and so by the above lemma, S is at most countable.

Finally, we note that ν^{-1} in our proof of (1) gives a bijection $\mathbf{N} \to \mathbf{N}^2$, and that we have a surjection $\mathbf{N}^2 \to \mathbf{Q}$ given by $(m, n) \mapsto \begin{cases} (-1)^{\lfloor \log_2 m \rfloor} \frac{m}{n} & n \neq 0 \\ 0 & n = 0 \end{cases}$ (we can always get both even and odd fractions by repeatedly multiplying both numerator and denominator by 2). Composing, we get a surjection $\mathbf{N} \to \mathbf{Q}$, establishing that $\mathbf{Q}$ is countable. □

(5) Let X be an uncountable set and Y a countable subset of X. Show that $Card(X \setminus Y) = Card(X)$.
(Hint: first show $Card(X \cup Y) = Card(X)$.)

As suggested by the hint, we first show a lemma. (If you're unfamiliar with the term, a "lemma" is a preliminary result that is used to prove something more important. When you are writing up solutions, stating intermediate results as lemmas and proving them first can be a good way to organize your write-up and make the graders happy.)

Lemma. *Let X be an infinite set and Y a countable set disjoint from X. Then,* $\mathrm{Card}(X \cup Y) = \mathrm{Card}(X)$.

Proof. X is infinite, so we can take $E \subset X$ countable. Then, we know that we can create a bijection, $\varphi : E \to E \cup Y$, as they are both countable. Then, define $\phi : X \to X \cup Y$ by:

$$\phi(x) = \begin{cases} x & x \notin E \\ \varphi(x) & x \in E \end{cases}$$

We see that this is injective, as φ is injective, the inclusion map is injective, and $\varphi(E) \cap (X \setminus E) = (E \cup Y) \cap (X \setminus E) = \emptyset$. We also see that it is surjective, as all elements of $X \setminus E$ are in the image of the inclusion map, and all elements of $E \cup Y$ are in the image of φ. Thus, ϕ provides a bijection between $X \cup Y$ and X.

□

Problem 3.1. *Let X an uncountable set and Y a countable subset of X. Show that* $\mathrm{Card}(X \setminus Y) = \mathrm{Card}(X)$.

Solution. Assume the contrary. Let $X' = X \setminus Y$. We note that X' is infinite, for if it were finite, then X would be the union of a countable (Y) and an a finite set (X'), and thus countable. Then, we apply the previous lemma to X' and Y, and get $\mathrm{Card}(X) = \mathrm{Card}(X' \cup Y) = \mathrm{Card}(X') = \mathrm{Card}(X \setminus Y)$. □