LVA 703070
Department of Computer Science
University of Innsbruck

Exercise 1

Let $A_m = \{a_1, \dots, a_m\}$ and $B_n = \{b_1, \dots, b_n\}$ for any $m, n \in \mathbb{N}$.

a) We call $f : A \to B$ a *constant function* if there is a $y \in B$ such that $f(x) = y$ for all $x \in A$. If $A, B \neq \emptyset$, when is a constant function $f : A \to B$ injective? When is it surjective?

b) For any $m \leq 2$ and $n \leq 2$, list the set $(B_n)^{A_m}$. That is: Give all functions of the form $f : A_m \to B_n$. Write them in a form similar to Slide 27 of the Week 3 lecture slides.

c) Which of these are injective, surjective, and bijective?

d) Can you say more generally what kind of functions there are if $m \in \{0, 1\}$ or $n \in \{0, 1\}$?

Remember: There are n^m functions in $(B_n)^{A_m}$. Do not forget the edge cases $m = 0$ or $n = 0$!

Solution:

a) Let A and B be non-empty sets and $f : A \to B$ a constant map, say $f(x) = y$ for all $x \in A$.

- If A is a singleton set (i.e. $|A| = 1$) then f is trivially injective since $|f^{-1}(y)| \leq |A| = 1$. Otherwise, if $x, x' \in A$ with $x \neq x'$, then $f(x) = y = f(x')$, which violates injectivity. Thus f is injective if and only if $|A| = 1$. (the possibility that $A = \emptyset$ will be handled in the next subexercise)
- If B is a singleton set (say $B = \{y\}$) then $\mathrm{ran}(f) = \{y\}$ since A is non-empty. Surjectivity demands that $\mathrm{ran}(f) = B$, which is then clearly the case if and only if $|B| = 1$.

b)

- For $m = 0$ or $n = 0$, remember that a function $f : A \to B$ is just a left-total and right-unique relation $f \subseteq A \times B$. If $m = 0$ or $n = 0$, clearly $A_m \times B_n = \emptyset$, so only the 'empty relation' $\emptyset$ is possible in principle.

  It remains to check whether $\emptyset$ is actually a function. It is clearly right-unique, but only left-total if $A = \emptyset$ (i.e. in our case $m = 0$). Thus, if $m = 0$ the only function in $(B_n)^{A_m}$ is the 'empty function' $\emptyset$, and if $m > 0$ and $n = 0$ there is no such function and we have $(B_n)^{A_m} = \emptyset$.

  Writing this 'empty function' down with the notation of Slide 27 is tricky; one could write it as $f : \emptyset \to B_n,\ f(x) = x$ (although the $f(x) = x$ is actually superfluous since there is only one function $\emptyset \to B_n$ anyway).
- For $n = 1$, we have only one element in the codomain B_n to map to, so the only function in $(B_n)^{A_m}$ is the constant function $f(x) = b_1$.
- For $m = 1$, we have one element a_1 in the domain to map and n elements in the codomain B_n to map it to. So for each $i \in [n]$, the constant function $f_i(x) = b_i$ is in $(B_n)^{A_m}$, and all elements of $(B_n)^{A_m}$ are of this form.
- For $m = n = 2$, the formula tells us that there are $2^2 = 4$ such functions. They can be defined as follows:

$$f_1(x) = b_1 \qquad f_2(x) = b_2$$

$$f_3(a_i) = b_i \qquad f_4(x) = \begin{cases} b_2 & \text{if } x = a_1 \\ b_1 & \text{otherwise} \end{cases}$$

c)
- If $m = 0$, the only function is the empty function $\emptyset$ and it is trivially injective, but only surjective (and thus bijective) if $n = 0$.
- If $n = 0$ and $m > 0$ there are no functions in $(B_n)^{A_m}$, as we have seen.
- If $n = 1$ the only function is the constant function $f(x) = b_1$. It is clearly surjective, but only injective if $m \leq 1$.
- If $m = 1$ and $n > 0$ the only functions are constant functions of the form $f_i(x) = b_i$. They are trivially injective, but only surjective if $n = 1$.
- If $m = n = 2$, there are the above functions f_1 to f_4. Of these, f_3 and f_4 are bijections and the other two are neither injective nor surjective.

d) This was already answered in b).

Exercise 2
Let $f : A \to B$ and $g : B \to C$ be functions.

a) Show: If f and g are surjective then $g \circ f$ is surjective.
b) Show: If f and g are injective then $g \circ f$ is injective.
c) Refute: If f and $g \circ f$ are injective, then g is injective.
d) Show: If f is bijective and $g \circ f$ is injective, then g is injective.
e) True or false? If g and $g \circ f$ are surjective, then f is surjective.

Solution:

a) Let $z \in C$ be arbitrary. Then by surjectivity of g there exists a $y \in B$ with $f(y) = z$ and by surjectivity of f there exists a $x \in A$ with $f(x) = y$. Thus $(g \circ f)(x) = z$.

b) Let $x, x' \in A$ with $(g \circ f)(x) = (g \circ f)(x')$. Then $g(f(x)) = g(f(x'))$ and by injectivity of g we have $f(x) = f(x')$ and by injectivity of f we have $x = x'$.

c) g can violate injectivity on an element that is not in the image of f. For example, if $A = B = C = \mathbb{N}$ and $f(n) = n + 1$ and $g(0) = 0$ and $g(n) = n - 1$ for $n \geq 1$, then f is injective and g is not. But $f \circ g = \mathrm{id}_{\mathbb{N}}$, which is injective.

   A simpler finite counterexample also exists: $A = C = \{0\}$ and $B = \{0, 1\}$ with $f(x) = x$ and $g(x) = 0$.

d) Let $y, y' \in B$ with $g(y) = g(y')$. By surjectivity of f, obtain $x, x' \in A$ with $f(x) = y$ and $f(x') = y'$. We thus have $g(f(x)) = g(f(x'))$, i.e. $(g \circ f)(x) = (g \circ f)(x')$. By injectivity of $g \circ f$, it follows that $x = x'$, and thus also $f(x) = f(x')$, i.e. $y = y'$.

   There is also a shorter proof: since f is bijective, so is f^{-1}. From this and the fact that $g \circ f$ is injective, we can conclude that also $g \circ f \circ f^{-1}$ is injective using b). But $g \circ f \circ f^{-1} = g \circ \mathrm{id}_B = g$.

e) False. To achieve surjectivity of $g \circ f$, we need to hit everything in C at least once, but we do not necessarily have to hit everything in B to achieve that.

   Let e.g. $A = C = \{0\}$ and $B = \{0, 1\}$ and $f(x) = x$ and $g(x) = x$. Clearly g is surjective and f is not. But $g \circ f = \mathrm{id}_{\{0\}}$ is surjective.

Exercise 3
Let R, S be well-founded relations. For each of the following statements, give a justification for why it holds or a counterexample if it does not.

a) $R \cup S$ is well-founded.

b) RS is well-founded.

c) R^+ is well-founded.

d) R^* is well-founded.

Solution:

a) False. The relations $R = \{(n-1, n) \mid n \in \mathbb{Z},\ n \text{ odd}\}$ and $S = \{(n-1, n) \mid n \in \mathbb{Z},\ n \text{ even}\}$ are well-founded since they do not even contain chains of length 2: we can only go from n to $n-1$, but then we cannot continue.

However, $R \cup S = \{(n-1, n) \mid n \in \mathbb{Z}\}$ has the infinite descending chain $0, -1, -2, \ldots$.

b) False. With R and S as in a), we have $RS = \{(n-2, n) \mid n \text{ even}\}$, so RS has an infinite descending chain $0, -2, -4, -6, \ldots$.

c) True. If we had an infinite descending chain $x_0, x_1, x_2, \ldots$ in R^+ then we could 'flatten' it and get an infinite descending chain on R:

At the beginning, we have $(x_1, x_0) \in R^+$. That means there exist $x_{0,0}, \ldots, x_{0,k}$ for some $k > 0$ with $x_{0,k}\ R\ x_{0,k-1} R \ldots R\ x_{0,1}\ R\ x_{0,0}$ and $x_{0,1} = x_0$ and $x_{0,k} = x_1$. We can repeat this for $(x_2, x_1) \in R^+$ and $(x_3, x_2) \in R^+$ etc. and chain them all together to obtain one big infinite chain.

d) False (unless R is defined over the empty set, in which case $R^* = \emptyset$). If R is a relation over a non-empty set, R^* is obviously not irreflexive. But well-founded relations must be irreflexive: if $(x, x) \in S$ for some relation S then S has the infinite descending chain $x, x, x, \ldots$.

In case you wonder where the argument from c) breaks down here: The argument from the previous subexercise does not work anymore because now $k = 0$ *is* possible, i.e. the $(x_{i+1}, x_i) \in R^*$ may simply be because $x_{i+1} = x_i$ and consist of zero steps. If this happens for all but finitely many i, our infinite chain in R^* will only have finite length after 'flattening' (most steps just 'disappear').

Bonus exercise

Let $f : A \to B$ be a function. We say that $g : B \to A$ is inverse to f if $g \circ f = \mathrm{id}_A$ and $f \circ g = \mathrm{id}_B$.

a) Show: If f is bijective then f^{-1} is bijective and $(f^{-1})^{-1} = f$.

b) Show: If g is inverse to f, then f is bijective and $g = f^{-1}$.

c) Is $g \circ f = \mathrm{id}_A$ alone sufficient for bijectivity of f?

d) Is $f \circ g = \mathrm{id}_B$ alone sufficient for bijectivity of f?

Only use the characteristic properties of f^{-1} from the lecture slides: if f is bijective, then (i) $f^{-1}(y) = x \leftrightarrow f(x) = y$, (ii) $f^{-1} \circ f = \mathrm{id}_A$, (iii) $f \circ f^{-1} = \mathrm{id}_B$.

Hint: Remember that $h_1, h_2 : X \to Y$ are equal if and only if $h_1(x) = h_2(x)$ for all $x \in X$.

Solution:

a)
- Surjectivity: Let $x \in A$ and define $y = f(x)$. Then $f^{-1}(y) = f^{-1}(f(x)) = x$.
- Injectivity: let $y, y' \in B$ with $f^{-1}(y) = f^{-1}(y')$. By surjectivity of f there exist $x, x' \in A$ with $f(x) = y$ and $f(x') = y'$ and thus $f^{-1}(f(x)) = f^{-1}(f(x'))$, which simplifies to $x = x'$.
- $(f^{-1})^{-1} = f$: First of all note that $(f^{-1})^{-1}$ is indeed a well-defined function because we just showed that f^{-1} is bijective. Now recall that two functions are equal if and only if, for any given input, they return the same output.

To show this, let $x \in A$ be arbitrary. We must now show that $(f^{-1})^{-1}(x) = f(x)$. With (i), this is equivalent to $x = f^{-1}(f(x))$, which is true due to (ii).

b) Note that, with the hint from the problem statement, g being inverse to f implies $g(f(x))$ and $f(g(y)) = y$ for any $x \in A$ and $y \in B$, so we can 'cancel' any adjacent f and g. Now:

- Surjectivity: Let $y \in B$. Then define $x = g(y)$. Then $f(x) = f(g(y)) = y$.
- Injectivity: Let $x, x' \in A$ with $f(x) = f(x')$. Then $g(f(x)) = g(f(x'))$, which simplifies to $x = x'$.
- $g = f^{-1}$: Two functions are equal if and only if they take the same values on all inputs. So let $y \in B$ be arbitrary. We want to show that $f^{-1}(y) = g(y)$. Using a), this is equivalent to $y = f(g(y))$, which follows from $f \circ g = \mathrm{id}_B$.

Note: It would also have sufficed to only prove the third property $g = f^{-1}$ here, since we already proved in b) that f^{-1} is bijective.

c) No. This is sufficient to show that f is injective, but it does not, in general, imply surjectivity. For instance, $f : \mathbb{N} \to \mathbb{N}, f(n) = n+1$ and $g : \mathbb{N} \to \mathbb{N}, g(n) = \max(0, n-1)$ satisfy $g \circ f = \mathrm{id}_{\mathbb{N}}$ but f is clearly not surjective.

d) No. This is sufficient to show that f is surjective, but it does not, in general, imply injectivity. Let us swap the situation from d): $f : \mathbb{N} \to \mathbb{N}, f(n) = \max(0, n-1)$ and $g : \mathbb{N} \to \mathbb{N}, g(n) = n+1$. Then we have $g \circ f = \mathrm{id}_{\mathbb{N}}$ but f is clearly not injective.