MA2441.03

Problem Set No. 4. (Solutions)

Dept. of Mathematics (Atkinson College)

1. Prove that the composition of two 1-1 correspondences is a 1-1 correspondence.

Reminder. There are **three** issues to address.

Proof. Let $f : A \to B$ and $g : B \to C$ be 1-1 correspondences. We need to show that $f \circ g : A \to C$, or (what amounts to the same thing) $g \cdot f : A \to C$ is a 1-1 correspondence.†

total: Let $x \in A$. By assumption, $f(x)$ is defined (we can write $f(x) \downarrow$), i.e., $f(x) = y$, *for some* y, and thus (by assumption) $g(y) \downarrow$.

1-1: Knowing that $g \cdot f$ is total, we need only show

$$(g \cdot f)(x) = (g \cdot f)(y) \text{ implies } x = y \tag{1}$$

The hypothesis translates to $g(f(x)) = g(f(y))$, hence $f(x) = g(y)$ since g is 1-1 and total. Finally, $x = y$, since f is 1-1 and total.

onto: Must show that for any $c \in C$, $(g \cdot f)(x) = c$ has an x-solution. Well, by assumption, there is a b such that $g(b) = c$. Take x (possible, by assumption) such that $f(x) = b$. □

2. (a) Prove that if a *total* relation R on a set A is *symmetric* and *transitive*, then it is also *reflexive*.

(b) By an appropriate example show that the assumption on totalness is *essential*.

Proof. (a) Take any $a \in A$. To show aRa. **By totalness**, there is a $b \in A$ such that aRb. By symmetry, bRa as well. By transitivity, aRa. □

Answer. (b) This, of course, is open-ended. Here is a simple counterexample over $A = \{1, 2\}$: $R = \{\langle 1, 1\rangle\}$. Transitive and symmetric, but not reflexive (not total, of course). □

3. Let S denote the set of strings over $\Sigma = \{1, 2, 3, +, \times, (,)\}$ defined as the *closure* of $\mathcal{I} = \{1, 2, 3\}$ under the operations $x, y \mapsto (x + y)$ and $x, y \mapsto (x \times y)$ for all strings x and y.

---

† $f \circ g = g \cdot f$ by definition. The former is relational, the latter is functional composition. Thus, $(g \cdot f)(x) = g(f(x))$.

(a) Prove that every string x in S has equal numbers of "(" and ")" symbols in it.
(b) Prove the following claim for every $x \in S$: If $x = y * z$—where "$*$" denotes *concatenation*—and iff $\varepsilon \neq y \neq x$, then y contains *more* "("-symbols than ")"-symbols.

Proof. (a) Induction on S. Each $x \in \mathcal{I}$ has the property (0 left brackets and 0 right brackets in any of the strings 1, 2 or 3).

I.S (induction step). Show that if x, y have the property, so do the results of each of the two operations. So, let x have m left and m right brackets and y have n left and n right brackets. Then $(x + y)$ and $(x \times y)$ each have $m + n + 1$ left and $m + n + 1$ right brackets. □

Proof. (b) *Basis*: Since *no initial object* (here a 1 a 2 or a 3) has *nonempty* proper prefixes, the claim is vacuously satisfied (i.e., there's nothing to prove).

For the induction *steps* [**there are two, since there are two formation rules or "operations": One that takes two strings x and y and forms $(x+y)$, the other forming $(x \times y)$**] assume the claim to be true for strings x, y of S and prove it true for $(x + y)$ and $(x \times y)$ (I omit the latter).

We consider all the "nonempty proper prefix"-cases:

Case of "("-prefix: Trivial.

Case of "$(C$"-prefix, where C is a nonempty proper prefix of x. By the *induction hypothesis* on x, C has more "(" than it has ")", so adding the extra one up in front does not hurt.

Case of "$(x$"-prefix: Since x is in S, it has an *equal* number of "(" and ")" by part (a). Adding a "(" up in front, the "(" have it!

Case of "$(x +$"-prefix: Adding a "+" does not change the conclusion of the previous case.

Case of "$(x + C$"-prefix, where C denotes a nonempty proper prefix of y this time. Now the numbers of the left/right brackets in x balance out (part (a)), while C has more "(" than ") *by the induction hypothesis*. So adding the "(" up in front does not hurt.

Finally, case of "$(x + y$"-prefix: The brackets in x and y balance out (by part (a)), so the "(" have it, due to the "(" up in front. □

4. Let S be the set of strings over $\Sigma = \{0, 1\}$ obtained as the *closure* of $\mathcal{I} = \{01\}$† under a single operation on strings: $x \mapsto 0x1$ for all strings x.

Prove that $S = \{0^n 1^n : n \geq 1\}$, where v^n for a string v means $\underbrace{v * \cdots * v}_{n \text{ copies of } v}$ for any $n > 1$.

† This is *not* a typo. $\mathcal{I}$ contains a single string: 01.

Reminder. There are **two** directions ($\subseteq$ and $\supseteq$).

Proof. ($\subseteq$) Induction on S. The (only) initial object 01 is in $\{0^n 1^n : n \geq 1\}$. Done.

I.S. Let $x \in \{0^n 1^n : n \geq 1\}$. Thus, $x = 0^k 1^k$ for some $k \geq 1$. The result of the only operation is $0x1$. That is, $0^{k+1}1^{k+1}$ which is still in $\{0^n 1^n : n \geq 1\}$.

($\supseteq$) Since $S = \{x : x \text{ is } (\mathcal{I}, F)\text{-derived}\}$ we simply need to exhibit a derivation for the arbitrary $0^k 1^k$ $(k \geq 1)$.

Such is "$01, 0^2 1^2, \ldots, 0^k 1^k$".† □

† Alternatively, one can do induction on k for ($\supseteq$), not using the result "closure = set of derived objects".