The Theory of Computation

Bernard M.E. Moret

Addison-Wesley-Longman, 1998

Solution Manual

Chapter 2, Problem 2.33

1. Assume we have two inverses for f, call them g and h. Consider the composition $f \cdot f^{-1}$, which is the identity on Ts: we would have, with $f^{-1} = g$, $f(f^{-1}(y)) = f(g(y))$ and with $f^{-1} = h$, $f(f^{-1}(y)) = f(h(y))$, for any $y \in T$. Since each is the identity, we would then have $f(g(y)) = f(h(y)) = y$, for any $y \in T$. Now apply f^{-1} to the first equality: we have $f^{-1}(f(g(y))) = f^{-1}(f(h(y)))$, or $(f^{-1} \cdot f)(g(y)) = (f^{-1} \cdot f)(h(y))$, for all $y \in T$; but $f^{-1} \cdot f$ is the identity on S, so that we have $g(y) = h(y)$, for all $y \in T$. Hence we have $g = h$, as desired.
2. Much the same manipulations as under (1) prove the result.
   We begin with the only if part. Let x and y be two elements of S. If we have $f(x) = f(y)$, then we can apply f^{-1} to each side to yield $f^{-1}(f(x)) = f^{-1}(f(y))$, or $(f^{-1} \cdot f)(x) = (f^{-1} \cdot f)(y)$; but $f^{-1} \cdot f$ is the identity on S, so that we have $x = y$, as desired. Hence f is injective. Now let z be any element of T and consider $y = f^{-1}(z)$. By definition, we must have $y \in S$. If we apply f to the equality above, we get $f(y) = f(f^{-1}(z))$ or $f(y) = (f \cdot f^{-1})(z)$; but $f \cdot f^{-1}$ is the identity on T, so that we have $f(y) = z$ and thus, for any $z \in T$, there exists a $y \in S$ (namely, $f^{-1}(z)$) with $f(y) = z$. Hence f is surjective. Being both injective and surjective, it is a bijection.
   Now for the if part. If f is a bijection, it is both injective and surjective. Thus, given any $z \in T$, there exists a $y \in S$ with $f(y) = z$. Moreover, we claim that this y is unique: if we have some $x \in S$ also with $f(x) = z$, it would violate the injectivity of f. Since the y is unique, we can legitimately define $f^{-1}(z) = y$. By construction, we then have $(f \cdot f^{-1})(z) = f(f^{-1}(z)) = f(y) = z$, so that $f \cdot f^{-1}$ is the identity on T, as desired. Consider now $(f^{-1} \cdot f)(x)$ for some $x \in S$; since we have $z = f(x) \in T$, our construction of f^{-1} ensures that there exists a unique $y \in S$ such that $f(y) = z$; but this y must then be our x, since our x has that property and since it must be unique. Thus we can

write $(f^{-1} \cdot f)(x) = f^{-1}(f(x)) - f^{-1}(z) = x$, showing that $f^{-1} \cdot f$ is the identity on S, as desired.

3. First we verify that $g^{-1} \cdot f^{-1}$ has the desired properties. Then we appeal to part (1) of this exercise, where we showed that the inverse must be unique, so that $g^{-1} \cdot f^{-1}$, which is *an* inverse, must be *the* inverse.
   We verify that $h \cdot h^{-1}$ is an identity: $h \cdot h^{-1} = (f \cdot g) \cdot (g^{-1} \cdot h^{-1})$, but composition of functions is associative, so that we can write

   $$h \cdot h^{-1} = (f \cdot g) \cdot (g^{-1} \cdot h^{-1}) = f \cdot (g \cdot g^{-1}) \cdot f^{-1} = f \cdot I \cdot f^{-1}$$

   where we used I to denote an identity function. But identity composed with any function is that function, so that we can further write

   $$h \cdot h^{-1} = f \cdot I \cdot f^{-1} = f \cdot f^{-1} = I$$

   as desired. We now verify that $h^{-1} \cdot h$ is also an identity:

   $$h^{-1} \cdot h = (g^{-1} \cdot f^{-1}) \cdot (f \cdot g) = g^{-1} \cdot (f^{-1} \cdot f) \cdot g = g^{-1} \cdot g = I$$

   as desired.