Quiz (Week 3)

Properties for Functions

Question 1

A substitution cipher is a method of hiding a message by substituting each character of the message with a different character in a way that can be reversed. The following is a simple subtitution cipher implemented in Haskell that substitutes each letter in the alphabet with the corresponding letter in the reversed alphabet, so `A` becomes `Z`, `B` becomes `Y`, and `M` becomes `N`.

Haskell

```haskell
encipher :: String -> String
encipher =
  let
    table = table' 'A' 'Z' ++ table' 'a' 'z'
    table' a z = zip [a..z] (reverse [a..z])
  in
    map $ \x -> case lookup x table of
      Just y  -> y
      Nothing -> x
```

Select all the properties that this function satisfies (assuming ASCII strings).

1. ✓ `all (not . isAlpha) xs ==> encipher xs == xs`
2. ✓ `encipher (encipher xs) == xs`
3. ✓ `length xs == length (encipher xs)`
4. ✗ `encipher (map f xs) == map f (encipher xs)`
5. ✓ `encipher (a ++ b) == encipher a ++ encipher b`
6. ✓ `(encipher $ map toUpper x) == (map toUpper $ encipher x)`
7. ✗ `not (null x) ==> 26 - ord (head x) == ord (head (encipher x))`

Property 1 is true, as this cipher does not affect any characters except alphabetical ones.

This cipher is an *involution*, that is, it is its own inverse. This makes property 2 true.

Property 3 is also true, as the ciphertext is always the same length as the plaintext in a substitution cipher. This property is also true of `map` itself and the implementation here is simply a partially applied `map`.

Property 4 does not hold, for example when `f` is the `succ` function.

Property 5 is true, as concatenating two ciphered strings is the same as ciphering their concatenation.

Property 6 holds as case is preserved across ciphering (capital letters are changed to other capital letters, and lowercase letters are changed to other lowercase letters).

Property 7 is false, as the difference in ASCII codes can be very different from 26, for example, the space character is left unaltered by ROT13 and so the difference may be zero.

Question 2

Here is a function that fairly merges ordered lists, e.g. `merge [2,4,6,7] [1,2,3,4] == [1,2,2,3,4,4,6,7]`.

```
merge :: (Ord a) => [a] -> [a] -> [a]
merge (x:xs) (y:ys) | x < y     = x:merge xs (y:ys)
                    | otherwise = y:merge (x:xs) ys
merge xs [] = xs
merge [] ys = ys
```

Select all the properties that this function satisfies.

1. ✓ `length (merge a b) == length a + length b`
2. ✗ `merge (map f a) (map f b) == map f (merge a b)`
3. ✓ `sort (merge a b) == sort (a ++ b)`
4. ✗ `merge a b == sort (a ++ b)`
5. ✓ `merge (sort a) (sort b) == sort (merge a b)`
6. ✗ `merge (filter f a) (filter f b) == filter f (merge a b)`

Property 1 is true, as the `merge` always contains all elements from the input list.

Property 2 is false, for example if `f` is the absolute value function `abs`, then any lists involving both negative and positive numbers will result in different orderings.

Property 3 is true, as a merge contains all the elements of both lists, as does a concatenation, and `sort` canonicalises their order.

Property 4 is false, for example when `a` is `[3,1]` and `b` is `[2,3]`.

Property 5 is true, as given two sorted lists (`sort a` and `sort b`), `merge` should produce a sorted list containing all of the elements of the original lists. Even if the input lists are not sorted, all elements will still be contained in the output, so `sort`-ing `merge a b` will produce the same result.

Property 6 is false, for example when `a` is `[3,1]` and `b` is `[2,3]`, and `f` is `(/= 3)`. The two filtered lists are `[1]` and `[2]`, resulting in a merge of `[1,2]` whereas merging first would result in the list `[2,1]`.

Question 3

The following code converts Haskell `Int` values to and from strings containing their hexadecimal representation (as a sequences of characters from the set { `'0'`, `'1'`, `'2'`, `'3'`, `'4'`, `'5'`, `'6'`, `'7'`, `'8'`, `'9'`, `'A'`, `'B'`, `'C'`, `'D'`, `'E'`, `'F'` }.

```
toHex :: Int -> String
toHex 0 = ""
toHex n =
  let
    (d,r) = n `divMod` 16
  in
    toHex d ++ ["0123456789ABCDEF" !! r]

fromHex :: String -> Int
fromHex = fst . foldr eachChar (0,1)
  where
    eachChar c (sum, m) =
      case elemIndex (toUpper c) "0123456789ABCDEF" of
        Just i  -> (sum + i * m, m * 16)
        Nothing -> (sum        , m * 16)
```

Select all properties that these functions satisfy.

1. ✗ `` all (`elem` "0123456789") s ==> read s <= fromHex s ``
2. ✓ `i >= 0 ==> fromHex (toHex i) == i`
3. ✓ `i > 0 ==> length (toHex i) <= length (show i)`
4. ✓ `` all (`elem` "0123456789ABCDEF") s ==> fromHex s == fromHex ('0':s) ``
5. ✗ `` all (`elem` "0123456789ABCDEF") s ==> toHex (fromHex s) == s ``

Property 1 is false as `read` will throw an exception when given the empty list for `s`.

Property 2 is true as converting to a hexadecimal string and then back should result in the same number.

Property 3 is true, as for *positive* (i.e. nonzero) integers the `toHex` representation will never be longer than the decimal string representation.

Property 4 is true, as adding leading zeroes to a hexadecimal number does not change its value.

Property 5 is false as while `toHex` is injective (there is a unique string for every number), `fromHex` is not, even if the strings are restricted to hexadecimal digits. For example, adding any number of leading zeroes onto the binary string will result in the same number from `fromBinary`, so a counterexample to this property can easily be found with `s = "01"`.

Question 4

The following function removes adjacent duplicates from a list.

```
dedup :: (Eq a) => [a] -> [a]
dedup (x:y:xs) | x == y     = dedup (y:xs)
               | otherwise = x : dedup (y:xs)
dedup xs = xs
```

Assume the presence of the following `sorted` predicate:

```
sorted :: (Ord a) => [a] -> Bool
sorted (x:y:xs) = x <= y && sorted (y:xs)
sorted xs       = True
```

Select all properties that `dedup` satisfies.

1. ✓ `sorted xs ==> sorted (dedup xs)`
2. ✓ ``(x `elem` xs) == (x `elem` dedup xs)``
3. ✓ `sorted xs ==> dedup (dedup xs) == dedup xs`
4. ✓ `sorted xs ==> dedup xs == nub xs`
5. ✗ `sorted xs && sorted ys ==> dedup xs ++ dedup ys == dedup (xs ++ ys)`
6. ✗ `sorted xs ==> length (dedup xs) < length xs`

Property 1 is true as dedup will remove elements without otherwise reording the list.

Property 2 is true as `dedup` will not remove the last of any given value in the list.

Property 3 is true as removing adjacent duplicates shouldn't find any more adjacent duplicates the second time around.

Property 4 is true as for sorted lists, removing adjacent duplicates and removing all duplicates are identical.

Property 5 is false, as can be seen when both `xs` and `ys` are just the singleton list `[1]`.

Property 6 is false as a list that already has no duplicates will not get any shorter.

Functions for Properties

Question 5

Here are a set of properties that the function `foo` must satisfy:

```
foo :: [a] -> (a -> b) -> [b]
foo = undefined -- see below

prop_1 :: [Int] -> Bool
prop_1 xs = foo xs id == xs

prop_2 :: [Int] -> (Int -> Int) -> (Int -> Int) -> Bool
prop_2 xs f g = foo (foo xs f) g == foo xs (g . f)
```

Choose an implementation for `foo` that satisfies the above properties, and type-checks:

1. ✗

```
foo xs f = []
```

2. ✗

```
foo xs f = xs
```

3. ✗

```
foo [] f = []
foo (x:xs) f = foo xs f
```

4. ✗

```
foo [] f = []
foo (x:xs) f = x : foo xs f
```

5. ✓

```
foo [] f = []
foo (x:xs) f = f x : foo xs f
```

These are the standard laws (*functor* laws) that `map` has to obey. And, indeed, the correct answer is a `map` implementation.

Note that it is actually impossible to write a terminating function that typechecks and obeys those properties *without* correctly implementing `map`. Try to write an incorrect, terminating `map` that is well-typed and obeys those laws! You will find it is impossible. Later on in the course we will discuss why this is so and how we can exploit it to write better programs.

Question 6

```
bar :: [Int] -> [Int]
bar = undefined

prop_1 :: [Int] -> Bool
prop_1 xs = bar (bar xs) == xs

prop_2 :: [Int] -> Bool
prop_2 xs = length xs == length (bar xs)

prop_3 :: [Int] -> (Int -> Int) -> Bool
prop_3 xs f = bar (map f xs) == map f (bar xs)
```

Choose all implementations for `bar` that satisfy the above properties, and type-check:

1. ✗

```
bar []     = []
bar (x:xs) = xs ++ [x]
```

2. ✗

```
bar []     = []
bar (x:xs) =      bar (filter (<=x) xs)
```

```
            ++ x : bar (filter (> x) xs)
```

3. ✓

```
bar = foldr (:) []
```

4. ✓

```
bar xs = go xs []
  where go []     acc = acc
        go (x:xs) acc = go xs (x:acc)
```

5. ✗

```
bar xs = nub xs
```

6. ✓

```
bar = foldl (flip (:)) []
```

The first property says the function has to be an *involution*, that is, applying it twice should have the same effect as not applying it at all. Property 2 says that the number of elements must remain the same. And property 3 says that `bar` must commute with `map`: This effectively means that we cannot depend on the value of elements of the list or change the values of the elements of the list as this would allow the function given to `map` to be crafted to break this property.

Thus, we must permute the elements of the given list without altering them or changing their quantity, and we must choose the output permutation without inspecting the input values. Thus, the two reverse implementations in 4 and 6, and the identity function in 3 are all correct implementations.

The rotation function in 1 breaks idempotence property 1. The remove duplicates function in 5 breaks the length property in 2. The quicksort function in 2 breaks property 3, as the map function could change the relative ordering of the elements.

Question 7

```
baz :: [[Integer]] -> [Integer]
baz = undefined

prop_1 :: [[Integer]] -> [[Integer]] -> Bool
```

```
prop_1 xs ys = baz xs ++ baz ys == baz (xs ++ ys)

prop_2 :: [[Integer]] -> Bool
prop_2 xs = baz xs == reverse (baz (reverse $ map reverse xs))

prop_3 :: [Integer] -> [[Integer]] -> Bool
prop_3 x xs = take (length x) (baz (x:xs)) == x
```

Choose a law-abiding definition for `baz`, that type checks:

1. ✗

```
baz []     = [0]
baz (x:xs) = x ++ baz xs
```

2. ✗

```
baz xs = []
```

3. ✗

```
baz []     = []
baz (x:xs) = 1 : baz xs
```

4. ✓

```
baz = foldr (++) []
```

This has to be the `concat` function (option 4).

The game is almost given away by the first property alone. However `prop_1` by itself allows for a function that merely returns an empty list (option 2) or a function that returns a list of the same total elements as input lists combined (option 3), however `prop_3` rules these out for us. Option 1 includes an off-by-one error, as the identity of `++` is is `[]`, and thus would break `prop_1` for even empty lists.

The `prop_2` property is not really needed here, and is included as a bit of a red herring.

Question 8

Here is a definition of a function `fun`, and properties for another function `nuf`:

```
xor :: Bool -> Bool -> Bool
xor False x = x
xor True  x = not x

fun :: [Bool] -> [Bool]
fun []             = []
fun [x]            = []
fun (x : y : xs) = (y `xor` x) : fun (y : xs)

nuf :: [Bool] -> Bool -> [Bool]
nuf = undefined

prop_1 :: [Bool] -> Bool -> Bool
prop_1 xs x = nuf (fun (x:xs)) x == (x:xs)

prop_2 :: [Bool] -> Bool -> Bool
prop_2 xs x = fun (nuf xs x) == xs
```

Choose a definition for `nuf` that type checks and satisfies the given properties:

1. ✗

```
nuf [] i = [i]
nuf (x:xs) i = (i `xor` x) : nuf xs (i `xor` x)
```

2. ✓

```
nuf xs i = scanl xor i xs
```

3. ✗

```
nuf [] i = []
nuf (x:xs) i = (i `xor` x) : nuf xs (i `xor` x)
```

4. ✗

```
nuf [] i = []
nuf (x:xs) i = (i `xor` x) : nuf xs i
```

5. ✗

```
nuf xs i = i : scanl (\v x -> v `xor` x) i xs
```

The `fun` function is essentially a differential decoding function, encoding when a value changes between true and false. Then, `nuf` is described by our properties as its inverse operation (given the initial boolean value), i.e., a differential encoding function.

If we run `fun [False,True,True,False,True]` we will get the differential encoding `[True,False,True,True]`. Trying each possible implementation:

```
*> nuf1 [True,False,True,True] False
[True,True,True,False,True]
*> nuf2 [True,False,True,True] False
[False,True,True,False,True]
*> nuf3 [True,False,True,True] False
[True,True,True,False,True]
*> nuf4 [True,False,True,True] False
[True,False,False,True,False]
*> nuf5 [True,False,True,True] False
[False,False,True,True,False,True]
```

As can be seen, only `nuf2` gives a correct answer that gets us back to our starting point.

Submission is already closed for this quiz. You can click here to check your submission (if any).