Selected solutions to *Discrete Mathematics and Functional Programming*

Thomas VanDrunen

August 13, 2013

This document is to provide a resource for students studying *Discrete Mathematics and Functional Programming* either on their own or in an academic course. The purpose is to aid student self-evaluation. Sections in this document are set to reflect book sections from which the exercises come. Accordingly, some sections are skipped here, either because the corresponding sections in the book have no exercises or no solutions are provided.

1 Set

1.3 Set notation

1.3.2. False. **1.3.4.** True. **1.3.6.** False. **1.3.8.** False. **1.3.10.** True.

1.11 Making your own operations

1.11.3.

```
fun add(Int(x), Int(y)) = Int(x + y)
  | add(Real(x), Real(y)) = Real(x + y)
  | add(Int(x), Real(y)) = Real(real(x) + y)
  | add(Real(x), Int(y)) = Real(x + real(y));
```

1.11.5.

```
fun replaceFries(Meal(e, Fries, b), s) = Meal(e, s, b)
  | replaceFries(Meal(e, s1, b), s2) = Meal(e, s1, b);
```

1.11.8

```
(* included here for reference *)
datatype rational = Fraction of int * int;
fun subtract(Fraction(a, b), Fraction(c, d)) =
     let val numerator = a * d - c * b;
         val denominator = b * d;
         val divisor = gcd(numerator, denominator);
      in Fraction(numerator div divisor, denominator div divisor)
      end;
```

1.12 Recursive functions

1.12.4

```
fun multiply(x, 0) = 0
  | multiply(x, y) = x + multiply(x, y-1);
```

]1.12.6

```
fun arithSum(0) = 0
  | arithSum(n) = n + arithSum(n-1) ;
```

2 List

2.1 Lists

2.1.1

$$\underbrace{[\ \underbrace{\underbrace{\mathtt{tl}(\underbrace{[\underbrace{5}_{\text{int}},\underbrace{12}_{\text{int}},\underbrace{6}_{\text{int}}]}_{\text{int list}})}_{\text{int list}} \mathbin{@} \underbrace{[\underbrace{8}_{\text{int}},\underbrace{9}_{\text{int}}]}_{\text{int list}}}_{\text{int list}}\ ]}_{\text{int list list}}$$

2.1.5

$$\underbrace{\underbrace{\mathtt{hd}(\underbrace{[\underbrace{12}_{\text{int}},\underbrace{5}_{\text{int}},\underbrace{6}_{\text{int}}]}_{\text{int list}})}_{\text{int}} :: \underbrace{[\underbrace{2}_{\text{int}},\underbrace{7}_{\text{int}}]}_{\text{int list}}}_{\text{int list}}$$

2.1.8

$$\underbrace{[\ \underbrace{[\underbrace{(\underbrace{2.3}_{\text{real}},\underbrace{5}_{\text{int}})}_{\text{(real * int)}},\underbrace{(\underbrace{8.1}_{\text{real}},\underbrace{6}_{\text{int}})}_{\text{(real * int)}}]}_{\text{(real * int) list}},\quad \underbrace{[]}_{\text{(real * int) list}}\ ]}_{\text{(real * int) list list}}$$

2.2 Functions on lists

2.2.4

```
fun count([]) = 0
    | count(a::rest) = 1 + count(rest);
```

2.2.5

```
fun findNth([], n) = ~1
  | findNth(a::rest, 0) = a
  | findNth(a::rest, n) = findNth(rest, n-1)
```

2.2.6

```
fun reverse([]) = []
  | reverse(a::rest) = reverse(rest) @ [a];
```

2.2.10

```
fun listify([]) = []
    | listify(a::rest) = [a] ::   listify(rest);
```

2.2.12

```
fun splitList([]) = ( [] , [] )
  | splitList( (a, b )::rest) =
    let
        val (x, y) = splitList(rest);
    in
        (  a::x , b::y)
    end;
```

3 Proposition

3.3 Boolean values

3.3.4

```
fun turnToInts([]) = []
  | turnToInts(true::rest) = 1::turnToInts(rest)
  | turnToInts(false::rest) = 0::turnToInts(rest);
```

3.4 Logical equivalence

3.4.5

$$
\begin{array}{lll}
p \wedge (\sim q \vee (p \wedge \sim p)) & & \\
\equiv & p \wedge (\sim q \vee F & \text{Negation} \\
\equiv & p \wedge \sim q & \text{Identity}
\end{array}
$$

3.4.6

$$
\begin{array}{lll}
(q \wedge p) \vee \sim (p \vee \sim q) & & \\
\equiv & (q \wedge p) \vee (\sim p \wedge q) & \text{DeMorgan's and double negative} \\
\equiv & q \wedge (p \vee \sim p) & \text{Distributive (and commutative)} \\
\equiv & q \wedge T & \text{Negation} \\
\equiv & q & \text{Identity}
\end{array}
$$

3.4.7

$$
\begin{array}{lll}
((q \wedge (p \wedge (p \vee q))) \vee (q \wedge \sim p)) \wedge \sim q & & \\
\equiv & ((q \wedge p) \vee (q \wedge \sim p)) \wedge \sim q & \text{Absorption} \\
\equiv & (q \wedge (p \vee \sim p)) \wedge \sim q & \text{Distributivity} \\
\equiv & (q \wedge T) \wedge \sim q & \text{Negation} \\
\equiv & q \wedge \sim q & \text{Identity} \\
\equiv & F & \text{Negation}
\end{array}
$$

4 Proof

4.2 Subset proofs

4.2.1.

Proof. Suppose $a \in A$. *[By generalization, $a \in A$ or $a \in B$.]* By definition of union, $a \in A \cup B$. Therefore, by definition of subset, $A \subseteq A \cup B$. □

4.2.8.

Proof (long version). Suppose $x \in A \times (B - C)$. By definition of Cartesian product, $x = (a, d)$ for some $a \in A$ and $d \in B - C$. By definition of difference, $d \in B$ and $d \notin C$.

By definition of Cartesian product, $(a, d) \in A \times B$. Also by definition of Cartesian product, this time used negatively, $(a, d) \notin A \times C$.

[That is, we rewrite $d \notin C$. as $\sim (d \in C)$. By generalization, $\sim (d \in C \wedge a \in A)$. By definition of Cartesian product, $\sim ((a, d) \in A \times C)$. This can be rewritten as $(a, d) \notin A \times C$.]

By definition of difference, $(a, d) \in (A \times B) - (A \times C)$. By substitution, $x \in (A \times B) - (A \times C)$. Therefore, by definition of subset, $A \times (B - C) \subseteq (A \times B) - (A \times C)$. □

Proof (short version). Suppose $(a, d) \in A \times (B - C)$. By definition of Cartesian product, $a \in A$ and $d \in B - C$.

By definition of difference, $d \in B$ and $d \notin C$. By definition of Cartesian product, $(a, d) \in A \times B$ and $(a, d) \notin A \times C$.

By definition of difference, $(a, d) \in (A \times B) - (A \times C)$. Therefore, by definition of subset, $A \times (B - C) \subseteq (A \times B) - (A \times C)$. □

5 Relation

5.3 Image, inverse, and composition

Ex 5.3.5.

Proof. Suppose R is a relation over A and suppose $(a, b) \in R$.

Further suppose $x \in \mathcal{I}_R(b)$. By definition of image, $(b, x) \in R$. By definition of composition $(a, x) \in R \circ R$. By definition of image again, $x \in \mathcal{I}_{R \circ R}(b)$. Therefore, by definition of subset, $\mathcal{I}_R(b) \subseteq \mathcal{I}_{R \circ R}(a)$. □

Ex 5.3.7.

Proof. Suppose R is a relation over A and that $(a, b) \in R$.

[Note that $(a, b) \in R$ implies that both a and b must be elements of A.]

Suppose $x \in \mathcal{I}_R(b)$. By definition of image, $(b, x) \in \mathcal{I}_R(b)$. Since $(a, b) \in R$, we have $(a, x) \in R \circ R$ by definition of composition. Moreover $x \in \mathcal{I}_{R \circ R}(a)$ by definition of image.

Therefore $\mathcal{I}_R(b) \subseteq \mathcal{I}_{R \circ R}(a)$ by definition of subset. □

Ex 5.3.10.

Proof. First suppose $(x, y) \in i_B \circ R$. By definition of function composition, there exists $b \in B$ such that $(x, b) \in R$ and $(b, y) \in i_B$.

By definition of the identity relation, $b = y$. By substitution, $(x, y) \in R$. Hence $i_B \circ R \subseteq R$ by definition of subset.

Next suppose $(x, y) \in R$. By how R is defined, we know $x \in A$ and $y \in B$.

By definition of the identity relation, $(y, y) \in i_B$. By definition of composition, $(x, y) \in i_B \circ R$. Hence $R \subseteq i_B \circ R$.

Therefore, by definition of set equality, $i_B \circ R = R$. □

5.4 Properties of relations

Ex 5.4.6.

Proof. Suppose $x \in \mathbb{Z}$. By arithmetic, $x - x = 0 = 0 \cdot 2$, and so $x - x$ is even by definition. So $(x, x) \in R$ by how R is defined. Therefore R is reflexive by definition. □

Ex 5.4.7.

Proof. Suppose $x, y \in \mathbb{Z}$ such that $(x, y) \in R$. By how R is definited, $x - y$ is even. By definition of even, there exists $c \in \mathbb{Z}$ such that $x - y = 2 \cdot c$. By arithmetic, $y - x = 2 \cdot {}^{-}c$, which is even by definition. $(y, x) \in R$ by how R is defined. Therefore R is symmetric by definition. $\square$

Ex 5.4.8.

Proof. Suppose $x, y, z \in \mathbb{Z}$ such that $(x, y), (y, z) \in R$. By how R is defined, $x - y$ and $y - z$ are even. By definition of even, there exist $c, d \in \mathbb{Z}$ such that $x - y = 2 \cdot c$ and $y - z = 2 \cdot d$. By arithmetic and algebra,

$$\begin{aligned} x - z &= x + (y - y) - z \\ &= x - y + y - x \\ &= 2 \cdot c + 2 \cdot d \\ &= 2 \cdot (c + d) \end{aligned}$$

Since $c + d \in \mathbb{Z}$, $x - z$ is even by definition, and $(x, z) \in R$ by how R is defined. Therefore, R is transitive by definition. $\square$

Let R and S be relations on a set X and let $A \subseteq X$.

Ex 5.4.21.

Proof. Suppose R and S are both reflexive. Suppose $x \in X$. By definition of reflexive, $(x, x) \in R$ and $(x, x) \in S$. By definition of intersection, $(x, x) \in R \cap S$. Therefore $R \cap S$ is reflexive by definition. $\square$

Ex 5.4.23.

Proof. Suppose R and S are both symmetric. Suppose further that $(x, y) \in (S \circ R) \cup (R \circ S)$.

By definition of union, $(x, y) \in S \circ R$ or $(x, y) \in R \circ S$.

Case 1: Suppose $(x, y) \in S \circ R$. Then there exists $z \in X$ such that $(x, z) \in R$ and $(z, y) \in S$. Since R and S are symmetric, $(z, x) \in R$ and $(y, z) \in S$, by definition of symmetric. By definition of composition, $(y, z) \in R \circ S$. Hence $(y, z) \in (S \circ R) \cup (R \circ S)$ by definition of union.

Case 2: Similar to case 1, just interchange S and R.

Either way, $(y, z) \in (S \circ R) \cup (R \circ S)$, and so $(S \circ R) \cup (R \circ S)$ is symmetric by definition □

Ex 5.4.25.

Proof. Suppose $a \in A$. Since R is reflexive, $(a, a) \in R$. By definition of image, $a \in \mathcal{I}_R(A)$. Therefore $A \subseteq \mathcal{I}_R(A)$ by definition of subset. □

6 Equivalence relations

Ex 5.5.4.

Proof. Suppose R is reflexive and for all $a, b, c \in A$, if $(a, b) \in R$ and $(b, c) \in R$, then $(c, a) \in R$.

Reflexivity: Given.

Symmetry: Suppose $x, y \in A$ such that $(x, y) \in R$. Since R is reflexive, $(y, y) \in R$. By the assumed property [*taking* $a = x$, $b = y$ *and* $c = y$], $(y, x) \in R$. Hence R is symmetric by definition.

Transitivity: Suppose $x, y, z \in A$ such that $(x, y) \in R$ an $(y, z) \in R$. By the assumed property, $(z, x) \in R$. By symmetry (proven in the previous part of this proof), $(x, z) \in R$. Hence R is transitive by definition.

Therefore R is an equivalence relation by definition. □

Ex 5.5.6.

Proof. Suppose R is an equivalence relation and $(a, b) \in R$. Then suppose $x \in \mathcal{I}_R(a)$. By definition of image, $(a, x) \in R$. By definition of symmetry, $(b, a) \in R$. By definition of transitivity, $(b, x) \in R$. By definition of image $x \in \mathcal{I}_R(b)$. Hence by definition of subset, $\mathcal{I}_R(a) \subseteq \mathcal{I}_R(b)$.

Next suppose $x \in \mathcal{I}_R(b)$. By definition of image, $(b, x) \in R$. By definition of transitivity, $(a, x) \in R$. Hence by definition of subset, $\mathcal{I}_R(b) \subseteq \mathcal{I}_R(a)$.

Therefore, by definition of set equality, $\mathcal{I}_R(a) = \mathcal{I}_R(b)$. □

6.7 Transitive closure

Ex 5.7.2.

Proof. Suppose R is a relation on A.

[$R \cup i_A$ is reflexive:] Suppose $a \in A$. $(a, a) \in i_A$ by definition of identity relation. $(a, a) \in R \cup i_A$ by definition of union. Hence $R \cup i_A$ is reflexive by definition.

[$R \subseteq R \cup i_A$:] Suppose $(a, b) \in R$. Then $(a, b) \in R \cup i_A$ by definition of uniion. Hence $R \subseteq R \cup i_A$. (Alternately, we could have cited Exercise 4.2.1. Or, if I wasn't so mean, I could let you just say "by definition of union.")

[$R \cup i_A$ is the smallest such relation:] Suppose S is a reflexive relation such that $R \subseteq S$. Suppose further $(a, b) \in R \cup i_A$. By definition of union, $(a, b) \in R$ or $(a, b) \in i_A$.

Case 1: Suppose $(a, b) \in R$. Then $(a, b) \in S$ by definition of subset (since we supposed $R \subseteq S$).

Case 2: Suppose $(a, b) \in i_A$. Then, by definition of identity relation, $a = b$. $(a, a) \in S$ by definition of reflexive (since we suppose S is reflexive). $(a, b) \in S$ by substitution.

Either way, $(a, b) \in S$ and hence $R \cup i_A \subseteq S$ by definition of subset.

Therefore, $R \cup i_A$ is the reflexive closure of R. □

7 Function

7.4 Images and inverse images

Ex 7.4.1.

Suppose $A, b \subseteq X$. Further suppose $y \in F(A \cap B)$.

By definition of image, there exists $x \in A \cap B$ such that $f(x) = y$. By definition of intersection, $x \in A$ and $x \in B$. By definition of image, $y \in F(A)$ and $y \in F(B)$. By definition of intersection again, $y \in F(A) \cap F(B)$.

Therefore, by definition of subset, $F(A \cap B) \subseteq F(A) \cap F(B)$. □

Ex 7.4.3.

Attempted proof. Suppose $A, B \in X$. Further suppose $y \in F(A - B)$.

By definition of image, there exists $x \in A - B$ such that $f(x) = y$. By definition of difference, $x \in A$ and $x \notin B$.

By definition of image, $y \in F(A)$. Also by definition of image, used negatively, $y \notin F(B)$, right?

NO! Just because $x \notin B$ and $f(x) = y$ does not mean that there isn't some other element in B that also hits y. Thus here is our counterexample:

$$X = \{x, b\}; A = \{x\}; B = \{b\}; Y = \{y\}; f = \{(x, y), (b, y)\}$$
$$F(A - B) = F(\{x\} - \{b\}) = F(\{x\}) = \{y\}$$
$$F(A) - F(B) = F(\{x\}) - F(\{b\}) = \{y\} - \{y\} = \emptyset$$

7.4.4.

Suppose $A \subseteq B \subseteq X$.

First suppose $y \in F(B)$. By definition of image, there exists $x \in B$ such that $f(x) = y$.

Now, either $x \in A$ of $x \notin A$ by the negation law. *[How did we come up with that? We looked ahead and noticed that we want either $y \in F(B-A)$ or $y \in F(A)$ and saw how that would depend on $x \in A$ or $x \notin A$.]*

Case 1: Suppose $x \in A$. Then, by definition of image, $y \in F(A)$. By definition of union, $y \in F(B - A) \cup F(A)$.

Case 2: Suppose $x \notin A$. Then, by definition of difference, $x \in B - A$, and by definition of image, $y \in F(B - A)$. By definition of union, $y \in F(B - A) \cup F(A)$.

Either way, $y \in F(B - A) \cup F(A)$ and hence $F(B) \subseteq F(B - A) \cup F(A)$ by definition of subset.

Next suppose $y \in F(B-A) \cup F(A)$. By definition of union, $y \in F(B-A)$ or $y \in F(A)$.

Case 1: Suppose $y \in F(B - A)$. By definition of image, there exists $x \in B - A$ such that $f(x) = y$. By definition of difference, $x \in B$. So $y \in F(B)$ by definition of image.

Case 2: Suppose $y \in F(A)$. By definition of image, there exists $x \in A$ such that $f(x) = y$. By definition of subset, $x \in B$. So $y \in F(B)$ by definition of image.

Either way, $y \in F(B)$, and hence $F(B-A) \cup F(A) \subseteq F(B)$ by definition of subset.

Therefore, by definition of set equality, $F(B) = F(B - A) \cup F(A)$. $\square$

Ex 7.4.6.

Proof. Suppose $A \subseteq B \subseteq Y$. Further suppose $x \in F^{-1}(A)$.

By definition of inverse image, there exists $y \in A$ such that $f(x) = y$. By definition of subset, $y \in B$. By definition of inverse image again, $x \in F^{-1}(B)$.

Therefore, by definition of subset, $F^{-1}(A) \subseteq F^{-1}(B)$. $\square$

In the proof above, we could also do without the variable y. It's simply another name for that same mathematical object that we call $f(x)$:

Proof. Suppose $A \subseteq B \subseteq Y$. Further suppose $x \in F^{-1}(A)$.

By definition of inverse image, $f(x) \in A$. By definition of subset, $f(x) \in B$. By definition of inverse image again, $x \in F^{-1}(B)$.

Therefore, by definition of subset, $F^{-1}(A) \subseteq F^{-1}(B)$. $\square$

Ex 7.4.7.

Proof. Suppose $A, B \in Y$.

First suppose $x \in F^{-1}(A \cup B)$. By definition of inverse image, $f(x) \in A \cup B$. By definition of union, $f(x) \in A$ and $f(x) \in B$.

Case 1: Suppose $f(x) in A$. By definition of image, $x \in F^{-1}(A)$. By definition of union, $x \in F^{-1}(A) \cup F^{-1}(B)$.

Case 2: Similarly, if $f(x) \in B$, $x \in F^{-1}(A) \cup F^{-1}(B)$.

Either way, $x \in F^{-1}(A) \cup F^{-1}(B)$ and so $F^{-1}(A \cup B) \subseteq F^{-1}(A) \cup F^{-1}(B)$ by definition of subset.

Next suppose $x \in F^{-1}(A) \cup F^{-1}(B)$. By definition of union, $x \in F^{-1}(A)$ or $x \in F^{-1}(B)$.

Case 1: Suppose $x \in F^{-1}(A)$. By definition of inverse image, $f(x) \in A$. By definition of union, $f(x) \in A \cup B$. By definition of inverse image again, $x \in F^{-1}(A \cup B)$.

Case 2: Similarly, if $x \in F^{-1}(B)$, $x \in F^{-1}(A \cup B)$. Either way, $x \in F^{-1}(A \cup B)$ and so $F^{-1}(A) \cup F^{-1}(B) \subseteq F^{-1}(A \cup B)$.

Therefore, by definition of set equality, $F^{-1}(A \cup B) = F^{-1}(A) \cup F^{-1}(B)$. $\square$

7.6 Function properties

7.6.4.

Proof. Suppose $A \subseteq X$ and f is one-to-one. Further suppose $x \in F^{-1}(F(A))$. By definition of inverse image, $f(x) \in F(A)$.

*[By definition if image, $x \in A$, right? **NO!** At least, not immediately. From what we have said so far, we know that something in A maps to $f(x)$, but we don't yet know that x is that something. In other words, we need to use the definition of one-to-one—and use it correctly.]*

By definition of image, there exists some $a \in A$ such that $f(a) = f(x)$. Then by definition of one-to-one, $a = x$. So $x \in A$ by substitution.

Therefore $F^{-1}(F(A)) \subseteq A$ by definition of subset. $\square$

Ex 7.6.5.

Proof. Suppose $A \subseteq Y$ and f is onto. Further suppose $y \in A$.

By definition of onto, there exists $x \in X$ such that $f(x) = y$. By definition of inverse image, $x \in F^{-1}(A)$. By definition of image, $y \in F(F^{-1}(A))$.

Therefore, by definition of subset, $A \subseteq F(F^{-1}(A))$. $\square$

Ex 7.8.4.

Proof. Suppose $f : A \to B$ and $g : B \to C$ are both onto.

[Now, we want to prove "ontoness." Of which function? $g \circ f$. How do we prove ontoness? We pick something from the codomain of the function we're proving to be onto and show that it is hit. What is the codomain of $g \circ f$? C.]

Further suppose $c \in C$. *[We need to come up with something in the domain of $g \circ f$ that hits c. The domain is A. We will use the fact that f and g are both onto.]* By definition of not, there exists $b \in B$ such that $g(b) = c$. Similarly there exists $a \in A$ such that $f(a) = b$. Now,

$$\begin{aligned} g \circ f(a) &= g(f(a)) && \text{by definition of function composition} \\ &= g(b) && \text{by substitution} \\ &= c && \text{by substitution} \end{aligned}$$

Therefore $g \circ f$ is onto by definition. $\square$

Ex 7.8.8.

Proof. Suppose $f : A \to B$, $g : A \to B$, $h : B \to C$, h is onto, and $h \circ f = h \circ g$.

[This is a proof of function equality. Remember those? The two functions we're showing to be equal are f and g. How do we prove two functions are equal? We pick an element in their (mutual) domain and show that the two functions map it to the same thing. What is the domain of f and g? A.]

Suppose $a \in A$. *[We need to show $f(a) = g(a)$.]* Then

$$\begin{aligned} h(f(a)) &= h \circ f(a) && \text{by definition of function composition} \\ &= h \circ g(a) && \text{by definition of function equality, since } h \circ f = h \circ g \\ &= h(g(a)) && \text{by definition of function composition} \end{aligned}$$

Since $h(f(a)) = h(g(a))$, we then have that $f(a) = g(a)$ by definition of onto (because h is onto). Therefore, by definition of function equality, $f = g$. $\square$