COMPSCI 250: Fall 2023
Homework 2 Solution Key

David A. Mix Barrington , Ghazaleh Parvini

Due Date : Friday, October 6

(8 points) **Problem 2.1.1**

Let A be any set. What are the direct products $\emptyset \times A$ and $A \times \emptyset$? If x is any thing, what are the direct products $A \times \{x\}$ and $\{x\} \times A$? Justify your answers.

Solution:

$A \times \emptyset = \emptyset$ since there is no element in $\emptyset$ to form a pair.
$\emptyset \times A = \emptyset$ for the same reason as above.

$A \times \{x\} = \{(a, x) | a \in A\}$
$\{x\} \times A = \{(x, a) | a \in A\}$

(10 points) **Problem 2.1.5**

Let n be a natural and let $I(x)$ be a unary relation on the set $\{0, \ldots, n-1\}$. Let w be the binary string of length n that has 1 in position x whenever $I(x)$ is true and 0 in position x when $I(x)$ is false. (As in Java, we consider the positions of the letters in the string to be numbered starting from 0.) What is the string corresponding to the predicate $I(x)$ meaning "x is an even number" in the case where $n = 5$? The case where $n = 8$? If w is an arbitrary string and $I(x)$ the corresponding unary predicate, describe the set corresponding to the predicate in terms of w.

Solution:

n=5: 10101
n=8: 10101010

If w is an arbitrary string, $I(x)$ is the corresponding predicate is "x is a position that has a 1 in w". This makes the corresponding set $\{x : x \text{ is a position that has a 1 in } w\}$.

(12 points) **Problem 2.3.2**

Suppose that for any unary predicate P on a particular type T , you know that the proposition $(\exists x : P(x)) \leftrightarrow (\forall x : P(x))$ is true. What does this tell you about T? Justify your answer – state a property of T and explain why this proposition is always true if T has your property, and not always true if T does not have your property.

Solution:

SOLUTION 1. For any unary predicate P on a particular type T, we know that the proposition $(\exists x : P(x)) \leftrightarrow (\forall x : P(x)))$ is true. So there should be just one object in the particular Type T. Because the proposition shows that all the elements in the type of T have the same value with the predicate P. That means these elements are equal, if the particular type is a set type, we should just have one object in the particular type T. There may be an argument that these elements could also have the same value even though they are different, but the question said that whatever the predicate T is, the proposition is always true. Thus it sound reasonable that if we just one object of Type T. Now we can easily show that the proposition is always true if T just has one object. If T does not have such property, it's not always possible that we can infer that for all the x, $P(x)$ is true by the condition that there exists one x such that $P(x)$ is true.

SOLUTION 2. If $\exists x : P(x) \leftrightarrow \forall x : P(x)$ is true then T needs to be a singleton set. For this direction, $\forall x : P(x) \rightarrow \exists x : P(x)$, we just need that T is non empty set. So, if P holds for all elements in T we can guarantee that there is one. For the other direction, $\exists x : P(x) \leftrightarrow \forall x : P(x)$, we need T to be singleton, so in that way if P holds for some element in T and there is just one, we can say that P holds for every element in T.

(12 points) **Problem 2.5.6**

Suppose that A is a language such that $\lambda \notin A$. Let w be a string of length k. Show that there exists a natural i such that for every natural $j > i$, every string in A^j is longer than k. Explain how this fact can be used to decide whether w is in A^*.

Solution:

A is a language such that $\lambda \notin A$. We want to show that $\exists i : \forall j : ((j > i) \rightarrow (\forall u : u \in A^j \rightarrow | u |> k))$. Let $i = k$ and j be an arbitrary number such that $j > k$. Now let u be an element of A^j. By the definition of concatenation we can write $u = u_1 u_2 \ldots u_j$, where for each $i, u_i \in A$. As $\lambda \notin A$, we know that $| u_i |\geq 1$, and therefore $| u |=| u_1 | + | u_2 | + \ldots + | u_j |\geq j$. As we know that $j > k$, we have that $| u |\geq j > k$, and we proved our statement.

Now let w be a string of length k, and $A^* = A^0 \cup A^1 \cup A^2 \cup \ldots$. To decide if $w \in A^*$ we need to show that $w \in A^j$ for some j. We just proved that for $j > k$, a string u in A^j is going to be longer than k. So we just need to check if $w \in A^j$ for $j = 0, 1, \ldots, k$, and we can list all the strings of length k for each A^j, given that A is a finite set. If A is not a finite set, we can still test whether w is in A^* by brute force search, because we only need to consider a string x as part of the concatenation if it is no longer than w, and only finitely many elements of A are the same length as or shorter than w.

(14 points) **Problem 2.6.3**

Heinlein's second puzzle has the same form as in Problem 2.6.2. Here you get to figure out what the intended conclusion is to be, and prove it as above:

- Everything, not absolutely ugly, may be kept in a drawing room;
- Nothing, that is encrusted with salt, is ever quite dry;
- Nothing should be kept in a drawing room, unless it is free from damp;
- Time-traveling machines are always kept near the sea;
- Nothing, that is what you expect it to be, can be absolutely ugly;
- Whatever is kept near the sea gets encrusted with salt.

Solution: We will use the following predicates for this problem:

$$AU(x) x \text{ is absolutely ugly} \tag{1}$$
$$DR(x) x \text{ can be kept in a drawing room} \tag{2}$$
$$ES(x) x \text{ is encrusted with salt} \tag{3}$$
$$QD(x) x \text{ is quite dry / is free from damp} \tag{4}$$
$$TM(x) x \text{ is a time traveling machine} \tag{5}$$
$$NS(x) x \text{ is kept near the sea} \tag{6}$$
$$EB(x) x \text{ is what you expect it to be} \tag{7}$$

Which will then give us the following translation:

$$\forall x : \neg AU(x) \to DR(x) \quad = \forall x : \neg DR(x) \to AU(x) \tag{8}$$
$$\neg\exists x : ES(x) \land QD(x) \quad = \forall x : ES(x) \to \neg QD(x) \tag{9}$$
$$\neg\exists x : DR(x) \land \neg QD(x) \quad = \forall x : DR(x) \to QD(x) \quad = \forall x : \neg QD(x) \to \neg DR(x) \tag{10}$$
$$\forall x : TM(x) \to NS(x) \tag{11}$$
$$\neg\exists x : EB(x) \land AU(x) \quad = \forall x : AU(x) \to \neg EB(x) \tag{12}$$
$$\forall x : NS(x) \to ES(x) \tag{13}$$

The result is "Time traveling machines are not what you expect." ($\forall x : TM(x) \to \neg EB(x)$), which can be found through multiple applications of modus ponens:

$$TM(t) \quad \text{something } (t) \text{ is a time machine} \tag{14}$$
$$NS(t) \quad \text{MP, from (7), (4)} \tag{15}$$
$$ES(t) \quad \text{MP, from (8), (6)} \tag{16}$$
$$\neg QD(t) \quad \text{MP, from (9), (2)} \tag{17}$$
$$\neg DR(t) \quad \text{MP, from (10), (3)} \tag{18}$$
$$AU(t) \quad \text{MP, from (11), (1)} \tag{19}$$
$$\neg EB(t) \quad \text{MP, from (12), (5)} \tag{20}$$
$$TM(t) \to \neg EB(t) \quad \text{MP, from (7), (13)} \tag{21}$$

(10 points) **Problem 2.8.1**

Let $A = \{1, 2\}$ and $B = \{x, y\}$. There are exactly sixteen different possible relations from A to B. List them. How many are total? How many are well-defined? How many are functions? How many are neither well-defined nor total?

Solution:

We have $A = \{1, 2\}$ and $B = \{x, y\}$. So, $A \times B = \{(1, x), (1, y), (2, x), (2, y)\}$. Any relation from A to B will be a subset of AB, that's why we have 16 possible relations, listed below:

$$\begin{gathered}
R_0 = \\
R_1 = \{(1, x)\} \\
R_2 = \{(1, y)\} \\
R_3 = \{(2, x)\} \\
R_4 = \{(2, y)\} \\
R_5 = \{(1, x), (1, y)\} \\
R_6 = \{(1, x), (2, x)\} \\
R_7 = \{(1, x), (2, y)\} \\
R_8 = \{(1, y), (2, x)\} \\
R_9 = \{(1, y), (2, y)\} \\
R_{10} = \{(2, x), (2, y)\} \\
R_{11} = \{(1, x), (1, y), (2, x)\} \\
R_{12} = \{(1, x), (1, y), (2, y)\} \\
R_{13} = \{(1, y), (2, x), (2, y)\} \\
R_{14} = \{(1, x), (2, x), (2, y)\} \\
R_{15} = \{(1, x), (1, y), (2, x), (2, y)\}
\end{gathered}$$

There are 9 total relations: $R_6, R_7, R_8, R_9, R_{11}, R_{12}, R_{13}, R_{14}, R_{15}$.

There are 9 well-defined relations: $R_0, R_1, R_2, R_3, R_4, R_6, R_7, R_8, R_9$.

There are 4 functions: R_6, R_7, R_8, R_9.

There are 2 neither well-defined nor total relations: R_5, R_{10}.

(10 points) **Problem 2.9.3**

Let $f : A \to B$ and $g : B \to C$ be functions such that $g \circ f$ is a bijection. Prove that f must be one-to-one and that g must be onto. Give an example showing that it is possible for neither f nor g to be a bijection.

Solution:

A function f is one-to-one if it's never true that two different arguments map to the same result:

$$\neg\exists x : \exists y : \exists z : (x \neq y) \wedge (f(x) = z) \wedge (f(y) = z)$$

A function f is onto if every element of the range is "hit" by some input:

$$\forall y : \exists x : f(x) = y$$

$g \circ f$ is a bijection, so it's both onto and one-to-one:

$$\forall c \exists a : (g \circ f)(a) = c$$
$$\neg \exists a \exists b \exists c : (a \neq b) \wedge ((g \circ f)(a) = c) \wedge ((g \circ f)(b) = c).$$

To show f is one-to-one, we must show that $\forall a \forall a' \forall b : ((f(a) = b) \wedge (f(a') = b)) \to (a = a')$. Let a and a' be arbitrary elements of A, let b be an arbitrary element of B, and assume $(f(a) = b) \wedge (f(a') = b)$. Then $(g \circ f)(a) = g(b) = (g \circ f)(a')$, so as $g \circ f$ is one-to-one, we can specify the one-to-one property of $g \circ f$ on a, a', and c, to get that $a = a'$. By generalization, f is one-to-one.

To show g is onto, we must show $\forall c \exists b : g(b) = c$. As $(g \circ f)$ is onto, we know that $\forall c \exists a : (g \circ f)(a) = c$. Let c be an arbitrary element of C. Then by specification, $\exists a : (g \circ f)(a) = c$. We can specify this a, let $b = f(a)$, and then we have that $g(b) = c$ as desired.

As an example in which $g \circ f$ is a bijection but neither of f or g are bijections, let $A = \{a\}$, $B = \{b_1, b_2\}$, $C = \{c\}$. Then define $f(a) = b_1$, $g(b_1) = c$, $g(b_2) = c$. Here f is not onto and g is not one-to-one, but the composition $g \circ f$ is a bijection.

(12 points) **Problem 2.9.7**

Let A be a set and f a bijection from A to itself. We say that f **fixes** an element x of A if $f(x) = x$.

(a) Write a quantified statement, with variables ranging over A, that says "there is exactly one element of A that f does not fix."

(b) Prove that if A has more than one element, the statement of part (a) leads to a contradiction. That is, if f does not fix x, and there is another element in A besides x, then there is some other element that f does not fix.

Solution:

(a) $\exists x : [f(x) \neq x \wedge \neg \exists y : (x \neq y \wedge f(y) \neq y)]$
Equivalently, $\exists x : [f(x) \neq x \wedge \forall y : (x = y \vee f(y) = y)]$

(b) Assuming $\exists x : [f(x) \neq x \wedge \forall y : (x = y \vee f(y) = y)]$

- By Instantiation, choose x such that $f(x) \neq x \wedge \forall y : (x = y \vee f(y) = y)$.
- By left separation, $f(x) = x$. Let $z = f(x)$.
- Since f is injective and $f(x) = z$, $f(z) \neq z$.
- The statement $x \neq z$ and $f(z) \neq z$ contradict $\forall y : (x = y \vee f(y) = y)$ (from right separation of the first line). In other words, z is another element of f (in addition to x) that does not fix, which contradicts the assumption that there is exactly one element of A that f does not fix.

(12 points) **Problem 3.1.7**

A **Perfect number** is a natural that is the sum of all its proper divisors. For example, $6 = 1 + 2 + 3$ and $28 = 1 + 2 + 4 + 7 + 14$. Prove that if $2^n - 1$ is prime, then $(2^n - 1)2^{n-1}$ is a perfect number. (A prime of the form $2^n - 1$ is called a **Mersenne prime**. Every perfect number known is of the form given here, but it is unknown whether there are any others.)

Solution:

For clarity, we let $p = 2^n - 1$ be the Mersenne prime, and let $x = (2^n - 1)2^{n-1}$. The fundamental theorem of Arithmetic gives us that there is a unique prime factorization for every number. We see for x, that this will be $x = 2 * 2 * \cdots * 2 * p = 2^{n-1} * p$. We now consider the proper divisors.

We first note that the proper divisors of x will include all the divisors of 2^{n-1} , and 2^{n-1} . We also see that all other proper divisors must differ these other divisors by product of p and some power of 2. We thus have that the proper divisors of x will be all the divisors of 2^{n-1} , $2^n - 1$,and $p * 2x$ for every x such that $x < n - 1$.
We first consider the sum every proper divisor which is not divisible by p. We see that we have $1 + 2 + 4 + \cdots + 2n - 1 = 2^n - 1$. We then see by definition of p ,that $p = 2n - 1$, and thus the sum of every divisor which is not a divisor of p is p.
We now consider the sum of ever proper divisor which is divisible by p. We see that we have $p + 2p + \cdots + 2^{n-1}p = p(1 + 2 + \cdots + 2^{n-2}) = p(2^{n-1} - 1) = p2^{n-1} - p$.

Combining these two sums, we have $p * 2^{n-1} - p + p = p * 2^{n-1}$, which is exactly the value of x. Because n was an arbitrary number, we know that for every n such that 2^{n-1} is prime, we know $(2^n - 1)2^{n-1}$ is a perfect number.

Extra credit:

(10 points) **Problem 2.10.6**

There is only one partial order possible on the set $\{a\}$, because $R(a, a)$ must be true. On the set $\{a, b\}$, there are three possible partial orders, as $R(a, a)$ and $R(b, b)$ must both be true and either zero or one of $R(a, b)$ and $R(b, a)$ can be true. List all the possible partial orders on the set $\{a, b, c\}$. (**Hint:** There are nineteen of them.) How many are linear orders?

Solution:

The following are the 19 partial orders over $\{a, b, c\}$:

(a) $R(a, a), R(b, b), R(c, c)$

(b) $R(a, a), R(b, b), R(c, c), R(a, b)$

(c) $R(a, a), R(b, b), R(c, c), R(b, a)$

(d) $R(a, a), R(b, b), R(c, c), R(b, c)$

(e) $R(a, a), R(b, b), R(c, c), R(c, b)$

(f) $R(a,a), R(b,b), R(c,c), R(a,c)$

(g) $R(a,a), R(b,b), R(c,c), R(c,a)$

(h) $R(a,a), R(b,b), R(c,c), R(a,b), R(a,c)$

(i) $R(a,a), R(b,b), R(c,c), R(a,b), R(a,c), R(b,c)$

(j) $R(a,a), R(b,b), R(c,c), R(a,b), R(a,c), R(c,b)$

(k) $R(a,a), R(b,b), R(c,c), R(a,b), R(c,a), R(c,b)$

(l) $R(a,a), R(b,b), R(c,c), R(b,a), R(b,c)$

(m) $R(a,a), R(b,b), R(c,c), R(b,a), R(b,c), R(a,c)$

(n) $R(a,a), R(b,b), R(c,c), R(b,a), R(b,c), R(c,a)$

(o) $R(a,a), R(b,b), R(c,c), R(b,a), R(c,a)$

(p) $R(a,a), R(b,b), R(c,c), R(b,c), R(a,c)$

(q) $R(a,a), R(b,b), R(c,c), R(c,b), R(c,a)$

(r) $R(a,a), R(b,b), R(c,c), R(b,a), R(c,b), R(c,a)$

(s) $R(a,a), R(b,b), R(c,c), R(a,b), R(c,b)$
Six of them are linear orders (9, 10, 11, 13, 14, 18).