Solutions set for Exercise Group #1

CAS 701 Logic and Discrete Mathematics

Musa Al-hassy

« October 2017 »

Abstract

Students were required to submit solutions to 10 of the given 15 exercises posed by professor William Farmer. "Gallier" means the textbook *Logic for Computer Science: Foundations of Automatic Theorem Proving*, 2015.

The purpose of this assignment is to test one's background in general discrete mathematics. As such, there are varying degrees of rigour depending on one's comfort level and so these solutions also vary in rigour throughout the document.

- All exercises are worth 10 points each.
- Unlike Gallier, we are using *backwards composition*: $(g \circ f)\, x = g\,(f\, x)$.
- Notationally, I also use associative equivalence ' $\equiv$ ' in-place of conjunctive ' $\iff$ '.

This document renders its calculations using Maarten Fokkinga's calculation.sty LaTeX style file.

Contents

1 Calculating with sets

Show that, if A and B are sets, then

$$(A \cap B) \cup (A \cap \bar{B}) = A$$

Solution :: A set-theortic, or "point-free", solution takes the shape,

$$\begin{array}{ll} & (A \cap B) \cup (A \cap \bar{B}) \\ = & \quad \{ \text{ Distributivity of intersection over union } \} \\ & A \cap (B \cup \bar{B}) \\ = & \quad \{ \text{ Complements: Law of the excluded middle} \\ & \quad \text{Letting } \mathbf{U} \text{ denote the ambient } U\text{niversal set } \} \\ & A \cap \mathbf{U} \\ = & \quad \{ \text{ Universal set is identity of intersection } \} \\ & A \end{array}$$

—Alternatively, a "point-wise" proof follows—

The principle of extensionality states that the two sets are identical exactly when an arbitrary element is in one set precisely when it is in the other. Let x be arbitrary, then calculate:

$$\begin{array}{ll} & x \in (A \cap B) \cup (A \cap \bar{B}) \\ = & \quad \{ \text{ Union: In one } \textit{or} \text{ the other } \} \\ & x \in (A \cap B) \quad \vee \quad x \in (A \cap \bar{B}) \\ = & \quad \{ \text{ Intersection: In one } \textit{and} \text{ the other } \} \\ & (x \in A \ \wedge \ x \in B) \quad \vee \quad \left(x \in A \ \wedge \ x \in \bar{B}\right) \\ = & \quad \{ \text{ Negation: } \textit{Not} \text{ in the set } \} \\ & (x \in A \ \wedge \ x \in B) \quad \vee \quad (x \in A \ \wedge \ x \notin B) \\ = & \quad \{ \text{ And Distributes over Or: } p \wedge (q \vee r) \ \equiv \ (p \wedge q) \vee (p \wedge r) \ \} \\ & x \in A \quad \wedge \quad (x \in B \ \vee \ x \notin B) \\ = & \quad \{ \text{ Law of the Excluded Middle: It is or it isn't. } \} \\ & x \in A \quad \wedge \quad \mathsf{true} \\ = & \quad \{ \text{ Identity of conjunction: } p \wedge \mathsf{true} \ \equiv \ p \ \} \\ & x \in A \end{array}$$

Therefore, by extensional, we have shown the two sets to be identical.

2 One or the other, but not both!

Let $A \backslash B$ denote the difference of A and B and $A \Delta B$ denote the symmetric difference of A and B. Show $A \Delta B = (A \backslash B) \cup (B \backslash A)$.

Solution :: The principle of extensionality states that the two sets are identical exactly when an arbitrary element is in one set precisely when it is in the other. Let x be arbitrary, then calculate from the *complicated* side to the *simpler* side:

$$
\begin{array}{ll}
 & x \in (A \backslash B) \cup (B \backslash A) \\
= & \quad \{ \text{ Union: In one } \textit{or} \text{ the other } \} \\
 & x \in (A \backslash B) \ \vee \ x \in (B \backslash A) \\
= & \quad \{ \text{ Difference: In the first, } \textit{but not} \text{ in the second } \} \\
 & (x \in A \ \wedge \ x \notin B) \quad \vee \quad (x \in B \ \wedge \ x \notin A) \\
= & \quad \{ \text{ Phrase as a conditional for readability; } \mathsf{if}\ b\ \mathsf{then}\ t\ \mathsf{else}\ f\ \mathsf{fi} \ \equiv \ (b \wedge t) \ \vee \ (\neg b \wedge f) \ \} \\
 & \mathsf{if}\ x \in A\ \mathsf{then}\ x \notin B\ \mathsf{else}\ x \in B\ \mathsf{fi} \\
= & \quad \{ \text{ Conditionals: } \mathsf{if}\ b\ \mathsf{then}\ t\ \mathsf{else}\ f\ \mathsf{fi} \quad \equiv \quad (b \implies t) \ \wedge \ (\neg b \implies f) \ \} \\
 & (x \notin A \ \Rightarrow \ x \in B) \quad \wedge \quad (x \in A \ \Rightarrow \ x \notin B) \\
= & \quad \{ \text{ Implication, } p \implies q \ \equiv \ \neg p \vee q, \text{ and Double Negation, } \neg\neg p \ \equiv \ p \ \} \\
 & (x \in A \ \vee \ x \in B) \quad \wedge \quad (x \notin A \ \vee \ x \notin B) \\
= & \quad \{ \text{ De Morgan: Negations turn ors to ands, and vice versa } \} \\
 & (x \in A \ \vee \ x \in B) \quad \wedge \quad \neg\, (x \in A \ \wedge \ x \in B) \\
= & \quad \{ \text{ Symmetric difference: In one or the other, but not both } \} \\
 & x \in A \Delta B
\end{array}
$$

3 Injections are precisely the post-invertibles

Gallier's Exercise 2.1.1.a

> If there exists a function $g : B \to A$ such that $g \circ f = \mathsf{Id}$, then $f : A \to B$ is injective. If $f : A \to B$ is injective and $A \neq \emptyset$, then there exists a function $g : B \to A$ with $g \circ f = \mathsf{Id}$.

Solution :: Assume $g \circ f = \mathsf{Id}$, we show $f\,x = f\,y \;\Rightarrow\; x = y$,

$$\begin{array}{ll} & f\,x = f\,y \\ \Longrightarrow & \quad \{ \text{ Leibniz rule: Substituting equals for equals } \} \\ & g\,(f\,x) = g\,(f\,y) \\ = & \quad \{ \text{ Assumption } g \circ f = \mathsf{Id} \ \} \\ & x = y \end{array}$$

For the second part,

- For singleton sets, we use the partial-function unwrap to extract the singleton's element: $\mathsf{unwrap}\,(\{x\}) = x$.
- f is injective implies that its preimages are at-most singletons; in-particular, $a, a' \in f^{-1}\{b\} \;\equiv\; a = a'$
- $A \neq \emptyset$ precisely when there is some $a_0 \in A$.
- **Define** $g : B \to A : b \;\mapsto\; \mathsf{if}\ f^{-1}\{b\} \neq \emptyset\ \mathsf{then\ unwrap}\left(f^{-1}\{b\}\right)\ \mathsf{else}\ a_0\ \mathsf{fi}$

The definition of g sends elements to their only pre-image if it exists, and to the picked out point a_0 if they have no image at all —e.g., when f is not surjective.

It remains to prove the desired property,

$$\begin{array}{ll} & (g \circ f)\,x \\ = & \quad \{ \text{ Definitions } \} \\ & \mathsf{if}\ f^{-1}\{f\,x\} \neq \emptyset\ \mathsf{then\ unwrap}\left(f^{-1}\{f\,x\}\right)\ \mathsf{else}\ a_0\ \mathsf{fi} \\ = & \quad \{ \text{ Set theory } \} \\ & \mathsf{if}\ \{f\,x\} \neq \emptyset\ \mathsf{then\ unwrap}\,(\{f\,x\})\ \mathsf{else}\ a_0\ \mathsf{fi} \\ = & \quad \{ \text{ Set theory and conditionals } \} \\ & \mathsf{unwrap}\,(\{f\,x\}) \\ = & \quad \{ \text{ Specficiation of } \mathsf{unwrap} \ \} \\ & f\,x \end{array}$$

That was nice :-)

4 Surjections are precisely the pre-invertibles

Gallier's Exercise 2.1.1.b,

> A function f is surjective if and only if there exists a function $g : B \to A$ such that $f \circ g = \mathsf{Id}$.

Solution :: For the 'if' direction, assume $f \circ g = \mathsf{Id}$ then for any given y we set $x = g\,y$ then we have $f\,x = y$ and so f is surjective.

For the 'only if' direction:

- For non-empty sets, we use the partial-function for *choice* ϵ from sets to elements, having the membership-property $(\epsilon A) \in A$.
  - Intuitively such a function simply *selects* an element from the non-empty set A; we do not care which one as long as the result is from that set.
  - Such a function exists by the axiom of choice.
- That f is surjective means that its preimages are necessarily non-empty.
- **Define** $g : B \to A : b \mapsto \epsilon\left(f^{-1}\{b\}\right)$

It remains to prove the necessary property,

$$
\begin{array}{ll}
 & (f \circ g)\,x \\
= & \quad \{\ \text{Definitions}\ \} \\
 & f\ \left(\epsilon\left(f^{-1}\{x\}\right)\right) \\
= & \quad \{\ \text{Observe,} \\
 & \quad \left[\begin{array}{ll}
 & \epsilon\left(f^{-1}\{x\}\right)\ \in\ f^{-1}\{x\} \qquad \text{—This is the focal property of } \textit{choice} \\
= & \quad \{\ \text{Definition of preimage}\ \} \\
 & f\ \left(\epsilon\left(f^{-1}\{x\}\right)\right)\ \in\ \{x\} \\
= & \quad \{\ \text{Singleton membership}\ \} \\
 & f\ \left(\epsilon\left(f^{-1}\{x\}\right)\right)\ =\ x
\end{array}\right] \\
 & \quad \} \\
 & x \\
= & \quad \{\ \text{Definition}\ \} \\
 & \mathsf{Id}\,x
\end{array}
$$

That was nicer than I thought! :-)

5 Bijections are precisely the two-sides invertibles, the isos

Gallier's Exercise 2.1.1.c,

> A function $f : A \to B$ is bijective if and only if there is a function f^{-1} called its *inverse* such that $f \circ f^{-1} = \mathsf{Id}$ and $f^{-1} \circ f = \mathsf{Id}$.

Solution ::

$$
\begin{array}{ll}
 & f \text{ bijective} \\
= & \quad \{ \text{ Definitions } \} \\
 & f \text{ injective and surjective} \\
= & \quad \{ \text{ The results of the previous exerices } \} \\
 & \exists g, h. \quad f \circ h = \mathsf{Id} \ \wedge \ g \circ f = \mathsf{Id} \\
= & \quad \{ \text{ Exercise: Associative operations necessarily have unique inverses. } \} \\
 & \exists g, h. \quad f \circ h = \mathsf{Id} \ \wedge \ g \circ f = \mathsf{Id} \ \wedge \ h = g \\
= & \quad \{ \text{ One-point rule and dummy-renaming} \\
 & \quad \text{`}f^{-1}\text{' is only a } \textit{name} \text{ here. } \} \\
 & \exists f^{-1}. \quad f \circ f^{-1} = \mathsf{Id} \ \wedge \ f^{-1} \circ f = \mathsf{Id}
\end{array}
$$

Neato!

6 Pointfree formulation of transitivity

Gallier's Exercise 2.1.3,

> Given a relation R on a set A, prove that R is transitive if and only if R^2 is a subset of R.

Solution ::

$$
\begin{array}{ll}
 & R \text{ transitive} \\
= & \quad \{ \text{ Definition } \} \\
 & \forall x, y, z. \quad x \, R \, y \ \wedge \ y \, R \, z \ \Rightarrow \ x \, R \, z \\
= & \quad \{ \text{ Quantifier nesting } \} \\
 & \forall x, z. \quad (\forall y. \quad x \, R \, y \ \wedge \ y \, R \, z \ \Rightarrow \ x \, R \, z) \\
= & \quad \{ \text{ Join-characterisation: Implications transform exists to foralls } \} \\
 & \forall x, z. \quad (\exists y. \quad x \, R \, y \ \wedge \ y \, R \, z) \ \Rightarrow \ x \, R \, z \\
= & \quad \{ \text{ Relational Composition } \} \\
 & \forall x, z. \quad x \, R^2 \, z \ \Rightarrow \ x \, R \, z \\
= & \quad \{ \text{ Subset Containment } \} \\
 & R^2 \subseteq R
\end{array}
$$

7 [Reflexive,] [Symmetric,] Transitive Closure

Gallier's Exercise 2.1.5,

> Prove that $R^+ = \bigcup_{n \geq 1} R^n$ is the smallest transitive relation on A containing R, and $R^* = \bigcup_{n \geq 0} R^n$ is the smallest reflexive and transitive relation on A containing R. Prove that for any relation R on a set A, $(R \cup R^{-1})^*$ is the least equivalence relation containing R.

Solution :: The phrase

$$\text{“}\bar{x} \text{ is the least } P\text{-solution containing } x\text{”}$$

is usually realised as three small digestible proof obligations:

- *Solution*: $P\,\bar{x}$
- *Containment*: $x \leq \bar{x}$
- *Least*: $\forall y.\quad P\,y \;\wedge\; x \leq y \;\Rightarrow\; \bar{x} \leq y$

However, these can be combined into one *universal characterisation*:

$$\forall y.\qquad P\,y \;\wedge\; x \leq y \quad\equiv\quad \bar{x} \leq y$$

When possible, I personally prefer proving one thing even though it's a bit more complex, rather than three items. Of-course, when I'm at a loss, I'd rather use the three guiding obligations instead.

For the first part,

$$\begin{array}{ll}
& R^+ \;\subseteq\; T \\
\equiv & \quad \{\ \text{Definitions}\ \} \\
& \bigcup_{n\geq 1} R^n \;\subseteq\; T \\
\equiv & \quad \{\ \text{Join-characterisation: Union is the least upper bound.}\ \} \\
& \forall n \geq 1.\qquad R^n \;\subseteq\; T \\
\equiv & \quad \{\ \text{For `}\Rightarrow\text{', we instantiate } n \text{ to be 1.} \\
& \quad\ \text{For `}\Leftarrow\text{', we observe, for arbitrary } n, \\
& \quad\ \left[\begin{array}{ll}
& R^n \;\subseteq\; T \\
\Leftarrow & \quad \{\ \text{Strengthening: Adding a new constraint} \\
& \qquad\ \text{and transitivity of inclusion}\ \} \\
& R^n \;\subseteq\; T^n \quad\wedge\quad T^n \;\subseteq\; T \\
\Leftarrow & \quad \{\ \text{Monotonicity of relational product}\ \} \\
& R \;\subseteq\; T \qquad\wedge\quad T^n \;\subseteq\; T \\
= & \quad \{\ T^n \;\subseteq\; T \text{ follows by induction from the case } n = 2\ \} \\
& R \;\subseteq\; T \qquad\wedge\quad T^2 \;\subseteq\; T
\end{array}\right] \\
& \quad\ \}\\
& R \;\subseteq\; T \quad\wedge\quad T^2 \subseteq T \\
\equiv & \quad \{\ \text{Pointfree definitions}\ \} \\
& R \;\subseteq\; T \quad\wedge\quad T \text{ transitive}
\end{array}$$

For the second part,

$$
\begin{array}{ll}
& R^* \subseteq T \\
\equiv & \quad \{ \text{ Definitions } \} \\
& \bigcup_{n\geq 0} R^n \subseteq T \\
\equiv & \quad \{ \text{ Split-off one term from the quantification} \\
& \quad \text{—Similar to unfolding a loop } \} \\
& R^0 \cup \bigcup_{n\geq 1} R^n \subseteq T \\
\equiv & \quad \{ \text{ Relational Exponentation: } R^0 = \mathsf{Id} \\
& \quad \text{and Join-characterisation: Union is the least upper bound. } \} \\
& \bigcup_{n\geq 1} R^n \subseteq T \quad \wedge \quad \mathsf{Id} \subseteq T \\
\equiv & \quad \{ \text{ Previous calculation } \} \\
& R \subseteq T \quad \wedge \quad T \text{ transitive} \quad \wedge \quad \mathsf{Id} \subseteq T \\
\equiv & \quad \{ \text{ Pointfree definitions } \} \\
& R \subseteq T \quad \wedge \quad T \text{ transitive and reflexive}
\end{array}
$$

For the final part,

- Since $(R \cup R^{-1})^{-1} = R^{-1-1} \cup R^{-1} = R \cup R^{-1}$ we have that $R \cup R^{-1}$ is symmetric.
- Taking $R, T := R \cup R^{-1}, (R \cup R^{-1})^*$ in the previous part we obtain:
  - $R \subseteq (R \cup R^{-1})^*$
  - $(R \cup R^{-1})^*$ is transitive and reflexive, and so, by the previous item, it is an equivalence relation.
- It remains to show that it is the *least* such equivalence relation:
  - If T is an equivalence, then it is transitive and reflexive and so, by the previous part, it contains $R \cup R^{-1}$.

8 Injections are closed under composition

Prove that if f and g are injective functions, then their composition is injective, but the converse is false.

Solution :: Assume f, g are injective, then we show $(g \circ f)\, x = (g \circ f)\, y \;\Rightarrow\; x = y$,

$$\begin{array}{rl} & (g \circ f)\, x = (g \circ f)\, y \\ = & \quad \{ \text{ Definitions } \} \\ & g\ (f\ x) = g\ (f\ y) \\ \Longrightarrow & \quad \{ \ g \text{ injective } \} \\ & f\, x = f\, y \\ \Longrightarrow & \quad \{ \ f \text{ injective } \} \\ & x = y \end{array}$$

Cool.
Now to show the converse does *not* hold, it suffices to find a counterexample:

- Let $\mathbf{1} = \{0\}$ be any singleton set whose only element is named '0'.
- Let $\mathbf{2} = \{0, 1\}$ be any set of two (distinct) elements, say their names are '0' and '1'.
- Let $f : \mathbf{1} \to \mathbf{2} : 0 \mapsto 0$ be the function that embeds $\mathbf{1}$ into $\mathbf{2}$.
  - This is injective since $f\, x = f\, y \implies x = y$ is true since all $x = y = 0$.
- Let g be the only function to $\mathbf{1}$; i.e., $g : x \mapsto 0$.
  - This is *not* injective since $g\, 0 = 0 = g\, 1$ even thought $0 \neq 1$ in $\mathbf{2}$.
- Now the composition $g \circ f : \mathbf{1} \to \mathbf{1}$ is injective —it is distinctness preserving since there are no distinct points in $\mathbf{1}$ — but it is not the case that both f *and* g are injective.

9 Surjections are closed under composition

Prove that, if f and g are surjective functions, then their composition is surjective, but the converse is false.

Solution :: A "point-free" proof takes the shape:

$$
\begin{array}{ll}
 & f, g \text{ surjective} \\
= & \quad \{ \text{ Past exercise: Surjections are precisely the pre-invertibles } \} \\
 & \exists f', g'. \quad f \circ f' = \mathsf{Id} \ \wedge \ g \circ g' = \mathsf{Id} \\
\Longrightarrow & \quad \{ \text{ The context yields} \\
 & \quad \left\lceil \begin{array}{ll}
 & (g \circ f) \circ (f' \circ g') \\
= & \quad \{ \text{ Associtivity of composition } \} \\
 & g \circ (f \circ f') \circ g' \\
= & \quad \{ \text{ Left-conjunct from context } \} \\
 & g \circ \mathsf{Id} \circ g' \\
= & \quad \{ \text{ Identity of composition is } \mathsf{Id} \ \} \\
 & g \circ g' \\
= & \quad \{ \text{ Right-conjunct from context } \} \\
 & \mathsf{Id}
\end{array} \right. \\
 & \quad \} \\
 & \exists f', g'. \quad (g \circ f) \circ (f' \circ g') = \mathsf{Id} \\
\Longrightarrow & \quad \{ \text{ Witness introduction and superflous quantifier elimination } \} \\
 & \exists h'. \quad (g \circ f) \circ h' = \mathsf{Id} \\
= & \quad \{ \text{ Past exercise: Surjections are precisely the pre-invertibles } \} \\
 & (g \circ f) \text{ surjective}
\end{array}
$$

—Alternate "point-wise" proof follows—

If f, g are surjective, then we show that any y has $(g \circ f)$-preimage x as follows.

- Since g is surjective, y has at least one preimage, say, x_g. —$g(x_g) = y$
- Since f is surjective, x_f has at least one preimage, say, x_f. —$f(x_f) = x_g$
- Let $x = x_f$, then: $(g \circ f)(x_f) = g\,(f\,(x_f)) = g\,(x_g) = y$.

For the second part of the problem, —using the *exact* same setup as in the previous question—

- Let $\mathbf{1} = \{0\}$ be any singleton set whose only element is named '0'.
- Let $\mathbf{2} = \{0, 1\}$ be any set of two (distinct) elements, say their names are '0' and '1'.
- Let $f : \mathbf{1} \to \mathbf{2} : 0 \mapsto 0$ be the function that embeds $\mathbf{1}$ into $\mathbf{2}$.
  - This is *not* surjective since '1' in $\mathbf{2}$ has no f preimage.
- Let g be the only function to $\mathbf{1}$; i.e., $g : x \mapsto 0$.
  - This is surjective since the only point of $\mathbf{1}$ has all of the function's source as preimage.
- Now the composition $g \circ f : \mathbf{1} \to \mathbf{1}$ is surjective since $(g \circ f)\,0 = 0$, but it is not the case that both f *and* g are surjective.

Sweet, the same setup works for two problems ;-)

10 Baffling Bijections

Determine which of the following functions are bijective from $\mathbb{R}$ to $\mathbb{R}$:

a. $f(x) = -3 \cdot x + 4$

b. $f(x) = -3 \cdot x^2 + 7$

c. $f(x) = (x + 1)/(x + 2)$

d. $f(x) = x^5 + 1$

Solution ::
A "high-level" solution to this problem-set may be:

> The first is a linear function over the reals and so invertible, the second is bounded above by 7 and so necessarily not surjective, the third is undefined at -2 and so not even a total function, the last is strictly monotonic whence injective and it takes positives to positives and negatives to negatives and is clearly continuous so it must be then surjective. Hence only the first and last are bijections.

—A more involved, methodical, approach follows—

Recall that a function f is a bijection exactly when there is a function g that allows us to solve equations involving f, and vice versa:

$$\forall x, y. \qquad f(x) = y \quad \equiv \quad x = g(y)$$

We are given f in each case, so let us attempt to solve this equivalence with the aim of finding g —this is the usual method one learns in high school to check if a function is invertible.

10.1 Part a

$$\begin{aligned}
& f(x) = y \\
\equiv \quad & \{ \text{ Givens } \} \\
& -3 \cdot x + 4 = y \\
\equiv \quad & \{ \text{ Arithmetic —subtraction } \} \\
& -3 \cdot x = y - 4 \\
\equiv \quad & \{ \text{ Arithmetic —non-zero division } \} \\
& x = \tfrac{y-4}{-3} \\
\equiv \quad & \{ \text{ Define } g(y) = \tfrac{y-4}{-3} \} \\
& x = g(y)
\end{aligned}$$

Hence, we have *calculated* an inverse for the given f and so it is a bijection.

10.2 Part b

Given $f(x) = -3 \cdot x^2 + 7$, we calculate:

$$\begin{aligned}
& f(x) = y \\
\equiv & \quad \{ \text{ Givens } \} \\
& -3 \cdot x^2 + 7 = y \\
\equiv & \quad \{ \text{ Arithmetic —subtraction } \} \\
& -3 \cdot x^2 = y - 7 \\
\equiv & \quad \{ \text{ Arithmetic —non-zero division } \} \\
& x^2 = \tfrac{y-4}{-3}
\end{aligned}$$

- It is no longer clear how to proceed since squaring is not invertible on the real number line:

$$x^2 = y^2 \;\equiv\; x \in \{+y, -y\}$$

- Bijections are necessarily injective, so if we find f to be non-injective then it must be non-bijective.
- Taking $x \in \{+1, -1\}$ we find $f(+1) = 4 = f(-1)$ but $+1 \neq -1$ and so f is not injective.

Hence, f is not bijective.

10.3 Part c

Given $f(x) = (x + 1)/(x + 2)$, we calculate:

$$\begin{aligned}
& f(x) = y \\
\equiv & \quad \{ \text{ Givens } \} \\
& (x + 1)/(x + 2) = y \\
\equiv & \quad \{ \text{ Arithmetic —non-zero division, } \textit{supposing } x \neq -2 \ \} \\
& x + 1 = y \cdot x + 2 \cdot y \\
\equiv & \quad \{ \text{ Arithmetic —Subtraction } \} \\
& x - y \cdot x = 2 \cdot y - 1 \\
\equiv & \quad \{ \text{ Arithmetic —Factoring } \} \\
& x \cdot (1 - y) = 2 \cdot y - 1 \\
\equiv & \quad \{ \text{ Arithmetic —non-zero division, } \textit{supposing } y \neq 1 \ \} \\
& x = (2 \cdot y - 1)/(1 - y) \\
\equiv & \quad \{ \text{ Define } g(y) = (2 \cdot y - 1)/(1 - y) \ \} \\
& x = g(y)
\end{aligned}$$

Hence, we have *calculated* an inverse for the given *f*. However, along the way we had to assume constraints on the source x and target y values, thereby establishing a bijection $\mathbb{R}\backslash\{-2\} \to \mathbb{R}\backslash\{1\}$.

Hence, f is a bijection on the restricted source and target, but is *not* a $\mathbb{R} \to \mathbb{R}$ bijection —indeed, what is the 'inverse' of $f(-2)$?

10.4 Part d

Given $f(x) = x^5 + 1$, we calculate:

$$\begin{aligned} & f(x) = y \\ \equiv & \quad \{ \text{ Givens } \} \\ & x^5 + 1 = y \\ \equiv & \quad \{ \text{ Arithmetic —subtraction } \} \\ & x^5 = y - 1 \end{aligned}$$

It is no longer clear how to continue this calculation.

We could proceed by resorting to testing values for f and observing it to be injective at least. However, we would need to make infinitely many such checks —we do not have such time; a finite proof would be preferable.

We know that a bijection is precisely a function that is surjective and injective, so let us aim to tackle these two goals.

For injectivity, we aim to show $f(x) = f(y) \implies x = y$:

$$\begin{aligned} & f(x) = f(y) \\ \equiv & \quad \{ \text{ Givens } \} \\ & x^5 + 1 = x^y + 1 \\ \equiv & \quad \{ \text{ Arithmetic —subtraction } \} \\ & x^5 = y^5 \\ \implies & \quad \{ \text{ Claim: Exponentiation is injective on the reals. } \} \\ & x = y \end{aligned}$$

It remains to proof our claim: Let a be an arbitrary real,

$$\begin{aligned} & \text{exponentiation (by } a\text{) is injective on the reals} \\ \equiv & \quad \{ \text{ Givens } \} \\ & x^a = y^a \implies x = y \\ \equiv & \quad \{ \text{ Contraposition: } p \implies q \quad \equiv \quad \neg q \implies \neg p \ \} \\ & x \neq y \implies x^a \neq y^a \\ \Leftarrow & \quad \{ \text{ Strengthening the assumption, weakening the conclusion } \} \\ & x < y \implies x^a < y^a \\ \equiv & \quad \{ \text{ This is strict monotony of exponentiation —c.f. calculus } \} \\ & \mathsf{true} \end{aligned}$$

It remains to show that f is surjective: Given y, we search for a preimage x,

$$\begin{aligned} & f(x) = y \\ \equiv & \quad \{ \text{ Givens and Arithmetic } \} \\ & x^5 + 1 - y = 0 \end{aligned}$$

The fundamental theorem of algebra says that a polynomial of degree n must have n complex roots. Since non-real complex roots come in conjugate pairs, we are ensured at least one real root. So we satisfy this equation by *selecting* such a real root, call it ω_y.

Hence, given any y there exists some $x = \omega_y$ with $x^5 + 1 - y = 0$; i.e., $f(x) = y$. Therefore, f is surjective.

We have show that f is both surjective and injective and so, by definition, it is bijective.

11 $\mathbb{Q}$ is equivalence classes of $\mathbb{Z} \times (\mathbb{Z} - \{0\})$

Let R be a relation on $\mathbb{Z} \times (\mathbb{Z} - \{0\})$ be a relation such that $(a, b)\, R\, (c, d) \;\equiv\; a \cdot d = b \cdot c$. Show that R is an equivalence relation. What is the equivalence class of $(1, 2)$? Give an interpretation of the equivalence classes of R.

Solution :: An *equivalence relation* is a relation that models what it means for one item to be 'similar' to another. There are three properties that must be proven:

Reflexitivity Everything is 'similar' to itself —$(a, b)\, R\, (a, b)$

$$
\begin{array}{ll}
 & (a, b)\, R\, (a, b) \\
= & \quad \{ \text{ Definitions } \} \\
 & a \cdot b = b \cdot a \\
= & \quad \{ \text{ Symmetry of multiplication } \} \\
 & \mathsf{true}
\end{array}
$$

Symmetry If one thing is 'similar' to another, then the other is similar to it —$(a, b)\, R\, (c, d) \quad \equiv \quad (c, d)\, R\, (a, b)$

$$
\begin{array}{ll}
 & (a, b)\, R\, (c, d) \\
= & \quad \{ \text{ Definitions } \} \\
 & a \cdot d = b \cdot c \\
= & \quad \{ \text{ Symmetry of multiplication and equality } \} \\
 & c \cdot b = d \cdot a \\
= & \quad \{ \text{ Definitions } \} \\
 & (c, d)\, R\, (a, b)
\end{array}
$$

Transitivity If one thing is 'similar' to another which itself is 'similar' to a third, then the first is 'similar' to the third —$(a, b)\, R\, (c, d) \;\wedge\; (c, d)\, R\, (e, f) \quad \Rightarrow \quad (a, b)\, R\, (e, f)$

$$
\begin{array}{ll}
 & (a, b)\, R\, (c, d) \quad \wedge \quad (c, d)\, R\, (e, f) \\
= & \quad \{ \text{ Definitions } \} \\
 & a \cdot d = b \cdot c \quad \wedge \quad c \cdot f = e \cdot d \\
\Longrightarrow & \quad \{ \text{ Using this context we calculate} \\
 & \quad \left[\begin{array}{ll}
 & a \cdot d \cdot f \\
= & \quad \{ \text{ Left conjunct from context } \} \\
 & b \cdot c \cdot f \\
= & \quad \{ \text{ Right conjunct from context } \} \\
 & b \cdot e \cdot d
\end{array} \right] \\
 & \quad \text{Now we multiplicatively cancel non-zero } d \;\; \} \\
 & a \cdot f = b \cdot e \\
= & \quad \{ \text{ Definitions } \} \\
 & (a, b)\, R\, (e, f)
\end{array}
$$

Secondly,

$$
\begin{array}{ll}
& R\text{-equivalence class of } (1,2) \\
= & \quad \{ \text{ Definitions } \} \\
& \{(a,b) \,|\, (a,b)\, R\, (1,2) \ \wedge\ a \in \mathbb{Z} \ \wedge\ b \in \mathbb{Z} - \{0\}\} \\
= & \quad \{ \text{ Definitions } \} \\
& \{(a,b) \,|\, a \cdot 2 = b \cdot 1 \ \wedge\ a \in \mathbb{Z} \ \wedge\ b \in \mathbb{Z} - \{0\}\} \\
= & \quad \{ \text{ Arithmetic } \} \\
& \{(a,b) \,|\, a \cdot 2 = b \ \wedge\ a \in \mathbb{Z} \ \wedge\ b \in \mathbb{Z} - \{0\}\} \\
= & \quad \{ \text{ Set theory: One-point rule} \\
& \quad \text{“You can have any } b \text{ you want, provided it's } 2 \cdot a\text{”} \ \} \\
& \{(a, 2 \cdot a) \,|\, a \in \mathbb{Z} \ \wedge\ a \cdot 2 \in \mathbb{Z} - \{0\}\} \\
= & \quad \{ \text{ Set theory and arithmetic } \} \\
& \{(a, 2 \cdot a) \,|\, a \in \mathbb{Z} \ \wedge\ a \neq 0\}
\end{array}
$$

Hence, the equivalence class of (1,2) are all non-zero scalar multiples of that vector.

Thirdly, if we construe R as equating fractions, then (1,2) has its equivalence class being all fractions that reduce to it.

12 Countable domains admit uncountably many sequences

What is the cardinality of the function space $\mathbb{N} \to \mathbb{N}$?

Solution :: Recall that Cantor's Theorem says $\mathbb{N} \to \mathbf{2}$ is uncountable and $\mathbb{N}$ is “much larger” than $\mathbf{2}$, so it is reasonable to conjecture $\mathbb{N} \to \mathbb{N}$ is also uncountable.

We shall prove it to be uncountable by supposing there is an enumeration ϕ_i of these functions, then we shall construct a function —“by looking at the diagonal”— that cannot be in the enumeration thereby establishing a contradiction.

- Let $f : \mathbb{N} \to \mathbb{N}$ be defined by $f(n) = 1 + \phi_n(n)$.
- We claim that f is not in the enumeration; i.e., for all n, we do not have $f = \phi_n$.
  - Indeed were it that $f = \phi_n$ for some n, then we necessarily have $f(x) = \phi_n(x)$ for all x and in-particular $f(n) = \phi_n(n)$, but by definition of f we are led inexorably to $0 = 1$.

This is the common shape of proving uncountability —so-called “diagonal arguments”.

13 Finitistic Intuition for an arbortist

Let T_n be a full binary tree of height $n \geq 1$. What is the cardinality of the set of nodes in T_n? What is the cardinality of the set of paths in T_n?

Solution :: Recall,

Full binary tree Each node has exactly zero or two children.

- As a working definition, let us use unlabelled trees, in curried notation:

$$Tree \ ::= \ Leaf \mid Branch \, Tree \, Tree$$

  In computing, this is what one normally expects when seeing "binary tree".
- Warning! Terminology is subtle: This differs from a 'complete' binary tree.

Path A sequence of instructions $\langle d_0, \ldots, d_n \rangle$ that direct us from the root to a particular leaf, where the $d_i \in \{Left, Right\}$.

- At each direction, we either look at the left child tree or the right child tree.
- Incidentally, our working definition of paths is just that of *binary sequences* whose length is the depth of a node in the tree.

Size of a tree The number of its leaf nodes.

- *size Leaf = 1*
- *size (Branch l r) = size l + size r*

"One Off" For binary trees, the number of external nodes is exactly 1 more than the number of internal nodes.

- Sounds counter-intuitive! Let *innodes* count the number of internal nodes:
  - *innodes Leaf = 0*
  - *innodes (Branch l r) = 1 + innodes l + innodes r*
- Then a simple induction argument shows *size t = 1 + innodes t.*

Height of a tree Number of edges from the root node to the deepest leaf.

- The height of a tree measures how far away the furthest leaf is.
- *height Leaf = 0*
- *height (Branch l r) = 1 + (height l* ***max*** *height r)*

Fundamental fact of (full) Binary trees $\log_2(\mathsf{size}\, t) \leq \mathsf{height}\, t < \mathsf{size}\, t \leq 2^{\mathsf{height}\, t}$.

- Even though two trees of the same size needn't have the same height, the measures are closely related.
- A simple induction argument shows that $\mathsf{height}\, t < \mathsf{size}\, t \leq 2^{\mathsf{height}\, t}$.
- By taking base-2 logs of the second inclusion, and placing the first inclusion to the right, we obtain: $\log_2(\mathsf{size}\, t) \leq \mathsf{height}\, t < \mathsf{size}\, t$.
- Observe that the first inclusion in the theorem statement says *the height of a tree with n leaf nodes is at-least log(n).*

With these facts in-hand, we find

$$
\begin{aligned}
& \text{cardinality of nodes in } T_n \\
= \quad & \{ \text{ Partition nodes: Turn one complex counting problem into two simpler ones. } \} \\
& \text{cardinality of external nodes in } T_n \ + \ \text{cardinality of internal nodes in } T_n \\
= \quad & \{ \text{ Definitions } \} \\
& \mathsf{size}\, T_n + \mathsf{innodes}\, T_n \\
= \quad & \{ \text{ Theorem "One Off" and arithmetic } \} \\
& 2 \cdot \mathsf{size}\, T_n - 1 \\
= \quad & \{ \text{ Fundamental fact of binary trees and Big-O notation } \} \\
& O\left(2^{\mathsf{height}\, T_n}\right)
\end{aligned}
$$

Then for the second part,

$$
\begin{aligned}
& \text{cardinality of paths in } T_n \\
= \quad & \{ \text{ above observation } \} \\
& \text{number of binary sequences whose lengths range over the depths of } T_n \\
\leq \quad & \{ \text{ the height of a tree is the maximum of the depths of its leaves } \} \\
& \text{number of binary sequences of length } \mathsf{height}\, T_n \\
= \quad & \{ \text{ We have } \mathsf{height}\, T_n \text{ many items, with 2 possible values for each item,} \\
& \quad \text{so we mutliply out to find the total } \} \\
& 2^{\mathsf{height}\, T_n}
\end{aligned}
$$

Hence, in both cases, the answer is $O\left(2^{\mathsf{height}\, T_n}\right)$.

14 Infinity does not confirm to intuition

Let T_∞ be a full binary tree of infinite height. What is the cardinality of the set of nodes in T_∞? What is the cardinality of the set of paths in T_∞?

Solution :: We have already presented a solution via a diagonal argument, so this time we solve one problem by *reducing* it to an already known problem.

Recall that a full binary tree is a tree where each node has exactly zero or two children. That it has infinite height means that the number of edges from the root to a leaf is countably infinite.

For the first part,

1. We can label the nodes and then count the number of nodes.
2. Label each node with a binary sequence that indicates how one may arrive at it by taking *Left* or *Right* whenever one encounters a fork. This labelling is clearly unique and so the cardinality of the nodes is that of the labels.
   - That is, we have named our nodes, uniquely, by the elements of $\mathsf{List}\,\mathbf{2}$.
   - These are *finite* lists; not *infinite* streams. I.e., $\mathsf{List}\,X = \bigcup_{n:\mathbb{N}}(\mathbf{n} \to X)$.
3. Now each level has countably many labels and we have countably many levels, and it is not difficult to show that the countable union of countable sets is again countable.
   - That is, $\mathsf{List}\,X$ is countable whenever X is countable.
4. Hence, we have countably many labels in total and so countably many node in T_∞.

Let us calculate the second part,

$$
\begin{array}{ll}
 & \text{cardinality of paths in } T_\infty \\
= & \quad \{ \text{ definition of paths } \} \\
 & \text{cardinality of binary sequences whose lengths vary over the depths in } T_\infty \\
= & \quad \{ \text{ We are told that } T_\infty \text{ has countably many depths ;} \\
 & \quad \text{ let } \mathbf{2} \text{ denote the type of binary instructions for a path } \} \\
 & \text{cardinality of } \mathbb{N} \to \mathbf{2} \\
= & \quad \{ \text{ “Definition” of Power set: } \mathbb{P}(X) = (X \to \mathbf{2}) \\
 & \quad \text{ Subsets correspond to the } \textit{true}\text{-preimages of the functions. } \} \\
 & \text{cardinality of } \mathbb{P}\,(\mathbb{N}) \\
= & \quad \{ \text{ Cantor's Theorem } \} \\
 & \text{cardinality of } \mathbb{R}
\end{array}
$$

Hence, there are uncountably many paths in T_∞.

(The last step is proven as theorem 17 here.)

15 Quadratics over the integers have countably many real solutions

Show that the set of real numbers that are solutions of quadratic equations of the form $a \cdot x^2 + b \cdot x + c = 0$, where $a,\ b,\ c$ are integers, is countable

Solution ::

- Recall that the "Division Algorithm" for numbers holds for polynomials as well, in the form: for any f, g there're *unique* q, r with $f = g \cdot q + r$ where $0 \leq \mathsf{deg}\, r < \mathsf{deg}\, f$.
- *Theorem:* A polynomial of degree n has at-most n roots.
  - Proof by induction on n using the division algorithm.
- Hence, polynomials have countably many roots.

Solution ::

$$
\begin{aligned}
& \{x \in \mathbb{R} \mid a \cdot x^2 + b \cdot x + c = 0 \ \wedge\ a, b, c \in \mathbb{Z}\} \\
\cong \quad & \{ \text{ A polynomial is identified by its coefficients,} \\
& \quad \text{So let's tag the solution with the coefficients to make things easier} \\
& \quad \text{—Indeed the sets are "obviously" isomorphic. } \} \\
& \{(x, a, b, c) \in \mathbb{R} \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \mid a \cdot x^2 + b \cdot x + c = 0\} \\
\cong \quad & \{ \ x \text{ can be any real as long as its one of the two solutions to} \\
& \quad \text{the quadratic, it can be atmost two values, so we make that clear. } \} \\
& \{(x, a, b, c) \in \mathbf{2} \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \mid \mathsf{true}\} \\
= \quad & \{ \text{ Set theory } \} \\
& \mathbf{2} \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \\
\cong \quad & \{ \text{ The product of countable sets is again countable. } \}
\end{aligned}
$$

Hence, we have shown our original set to be isomorphic to $\mathbf{2} \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$. However, the finite product of countable sets is again countable[1] and so the cardinality of our original problem is countable.

[1] Indeed if C_i are countable, then $\Pi_{i \leq n} C_i \hookrightarrow \Pi_{i \leq n} \mathbb{N} \hookrightarrow \mathbb{N}$, where the last injection follows by the representation of numbers by their prime decomposition upto the first n primes.