

3.6 Cardinal Arithmetic

Section 2.5 counted finite sets, and Section 2.3 proved the laws of powers $m^{n+k} = m^n m^k$ and $(m^n)^k = m^{nk}$ by induction (Proposition 2.3.4). For finite sets these numbers count functions: Y^X has m^n elements when Y has m and X has n (Section 1.5, before Example (All functions between two small sets)). This section asks what is left of that arithmetic when the sets are infinite and all we have are bijections.

3.6.1 The plane and the line

A square has two dimensions and a segment has one. Surely the plane $\mathbb{R} \times \mathbb{R}$ has more points than the line? The injection $x \mapsto (x, 0)$ gives $|\mathbb{R}| \leq |\mathbb{R} \times \mathbb{R}|$, and it seems that the other half of the plane should be left over.

A second question. Is $\mathbb{N}^{\mathbb{N}}$, the set of sequences of natural numbers, bigger than $\mathbb{R}$? A real number in $[0, 1)$ is only a sequence of digits below 10, while a sequence in $\mathbb{N}^{\mathbb{N}}$ may use any natural number at every place, so $\mathbb{N}^{\mathbb{N}}$ looks bigger.

Guess both answers before reading on. The plane is a product, $\mathbb{N}^{\mathbb{N}}$ is a power, and the line will turn out to be a power too: a power of 2.

3.6.2 Adding sizes: disjoint unions

For finite sets that do not meet, Section 2.5 added sizes by taking the union (Proposition 2.5.5). So define the sum of two sets as their union? With $A = B = \{0\}$ we want two elements, and $A \cup B = \{0\}$ has one. The union counts the shared element once. The cure is to tag every element with the name of the set it came from, so that the two copies cannot overlap.

A disjoint union keeps a labeled copy of each set, so nothing is counted twice.

Definition 3.6.1. Disjoint Union

Let A and B be sets. Their **disjoint union** is

$$A \sqcup B := (A \times \{0\}) \cup (B \times \{1\}).$$

The maps $\iota_A: A \rightarrow A \sqcup B$, $\iota_A(a) := (a, 0)$, and $\iota_B: B \rightarrow A \sqcup B$, $\iota_B(b) := (b, 1)$, are the **inclusions**.

In words: every element of $A \sqcup B$ is $(a, 0)$ with $a \in A$ or $(b, 1)$ with $b \in B$, and **not both**, since $(a, 0) = (b, 1)$ would give $0 = 1$ by the characteristic property of pairs (Definition 1.4.1). By the same property each inclusion is injective, the two images are disjoint, and together they make up $A \sqcup B$. So a function on $A \sqcup B$ may be defined by giving its values on the two tagged parts separately: these are the two cases that cannot overlap, as in the proof of Proposition 3.1.5.

Example. Two copies of $\mathbb{N}$

Show that $|\mathbb{N} \sqcup \mathbb{N}| = |\mathbb{N}|$.

Solution. This is the merging of two lists from the proof of Proposition 3.1.5, now as a bijection. Let $e(n, 0) := 2n$ and $e(n, 1) := 2n + 1$, for $n \in \mathbb{N}$; by the unwinding above this

defines $e: \mathbb{N} \sqcup \mathbb{N} \rightarrow \mathbb{N}$. For the decoder, let $d(m) := (q, r)$, where $m = 2q + r$ with $q \in \mathbb{N}$ and $r \in \{0, 1\}$; the pair exists and is unique by the claim in that proof, and $(q, r) \in \mathbb{N} \sqcup \mathbb{N}$. Then $d(e(n, r)) = (n, r)$ by the uniqueness, and $e(d(m)) = 2q + r = m$. By Theorem 1.6.4, e is a bijection.

This is the first encoding of the section: e writes a pair as one number, and d reads it back. The method box comes with the next one.

Quick check.

- (a) With $a \neq b$, list the elements of $\{a, b\} \sqcup \{a\}$ and of $\{a, b\} \cup \{a\}$. (b) What is $\emptyset \sqcup B$?
 (c) If $A \cap B = \emptyset$, give a bijection $A \cup B \rightarrow A \sqcup B$.

Solution.

- (a) $\{a, b\} \sqcup \{a\} = \{(a, 0), (b, 0), (a, 1)\}$, three elements; $\{a, b\} \cup \{a\} = \{a, b\}$, two. (b) $\emptyset \sqcup B = B \times \{1\}$, since $\emptyset \times \{0\} = \emptyset$; and $b \mapsto (b, 1)$ is a bijection $B \rightarrow \emptyset \sqcup B$. (c) Send x to $(x, 0)$ if $x \in A$ and to $(x, 1)$ if $x \in B$. The cases do not overlap, since $A \cap B = \emptyset$, so this is a function. Its inverse sends $(a, 0) \mapsto a$ and $(b, 1) \mapsto b$.

Warning. No subtraction. For numbers, $m + k = n + k$ gives $m = n$. For sets, $|\{0\} \sqcup \mathbb{N}| = |\emptyset \sqcup \mathbb{N}|$ although $|\{0\}| \neq |\emptyset|$: the map sending $(0, 0) \mapsto 0$ and $(n, 1) \mapsto n + 1$ is a bijection $\{0\} \sqcup \mathbb{N} \rightarrow \mathbb{N}$, and $(n, 1) \mapsto n$ is a bijection $\emptyset \sqcup \mathbb{N} \rightarrow \mathbb{N}$ (Exercise B4 (a) has the details). Every law below is proved by a bijection, never borrowed from the numbers.

3.6.3 Multiplying, raising to powers, and comparing

Products $A \times B$ (Definition 1.4.2) and sets of functions Y^X (Section 1.5) are the other two operations. If A has m elements and B has n , then $A \times B$ has mn elements and B^A has n^m , as Exercise C2 of Section 2.5 counts. The base is written on the line and the exponent is the domain: Y^X is the set of functions **from** X **to** Y .

Before any law, we check that the three operations see only sizes.

Proposition 3.6.1. Sums, Products and Powers Respect Size

Let A, A', B, B' be sets with $|A| = |A'|$ and $|B| = |B'|$. Then

- (a) $|A \sqcup B| = |A' \sqcup B'|$;
 (b) $|A \times B| = |A' \times B'|$;
 (c) $|A^B| = |A'^{B'}|$.

Idea. Carry each element across along the bijections: on each tagged part for (a), on each coordinate for (b), and for (c) by composing a function with the bijections on both sides. The inverses carry everything back.

Proof. Let $\alpha: A \rightarrow A'$ and $\beta: B \rightarrow B'$ be bijections, with two-sided inverses α^{-1} and β^{-1} (Theorem 1.6.4).

- (a) Send $(a, 0) \mapsto (\alpha(a), 0)$ and $(b, 1) \mapsto (\beta(b), 1)$; this is a function by the two-part rule after Definition 3.6.1. The same rule with α^{-1} and β^{-1} undoes it on each part, so it is a two-sided inverse.
- (b) Send $(a, b) \mapsto (\alpha(a), \beta(b))$. The map $(a', b') \mapsto (\alpha^{-1}(a'), \beta^{-1}(b'))$ is a two-sided inverse, by Definition 1.4.1.
- (c) For $f \in A^B$, the composite $\alpha \circ f \circ \beta^{-1}$ is a function $B' \rightarrow A'$. Let $\Theta(f) := \alpha \circ f \circ \beta^{-1}$ and $\Lambda(g) := \alpha^{-1} \circ g \circ \beta$ for $g \in A'^{B'}$. By Proposition 1.5.3 and $\alpha^{-1} \circ \alpha = \text{id}_A$, $\beta^{-1} \circ \beta = \text{id}_B$,

$$\Lambda(\Theta(f)) = (\alpha^{-1} \circ \alpha) \circ f \circ (\beta^{-1} \circ \beta) = f,$$

and $\Theta(\Lambda(g)) = g$ in the same way. In each part, Theorem 1.6.4 gives a bijection. ■

Remark. The proposition lets us replace either set by an equinumerous one without changing the size of the result. An answer computed from representatives must not depend on which representatives we used. Compare “send p/q to p ” in Section 1.5 (Example (Relations that are not functions)), which fails exactly this test.

The comparison $\leq$ of Definition 3.4.1 is respected as well, with one exception.

Proposition 3.6.2. Monotonicity

Let A, A', B, B' be sets with $|A| \leq |A'|$ and $|B| \leq |B'|$. Then

- (a) $|A \sqcup B| \leq |A' \sqcup B'|$;
- (b) $|A \times B| \leq |A' \times B'|$;
- (c) if $A' \neq \emptyset$, then $|A^B| \leq |A'^{B'}|$.

Idea. Carry the injections across, as in the previous proof. For powers, a function on B must be extended to all of B' , and the extension needs a value to put on the points that B does not reach.

Proof. Let $u: A \rightarrow A'$ and $v: B \rightarrow B'$ be injections. (a), (b): the maps of the previous proof with u, v in place of α, β are injective, by Definition 1.4.1.

(c) Fix $a_0 \in A'$. For $f \in A^B$ define $F(f): B' \rightarrow A'$ by

$$F(f)(b') := \begin{cases} u(f(b)) & \text{if } b' = v(b) \text{ for some } b \in B, \\ a_0 & \text{if } b' \notin v(B). \end{cases}$$

In the first case b is unique, since v is injective, so $F(f)$ is a function. If $F(f) = F(g)$, then for every $b \in B$,

$$u(f(b)) = F(f)(v(b)) = F(g)(v(b)) = u(g(b)),$$

so $f(b) = g(b)$, since u is injective. Hence $f = g$ (Proposition 1.5.1), and F is an injection $A^B \rightarrow A'^{B'}$. ■

A non-example by minimal change. Drop “ $A' \neq \emptyset$ ” from (c), and take $A = A' = \emptyset$, $B = \emptyset$, $B' = \{0\}$. Then $|B| \leq |B'|$, but $\emptyset^\emptyset$ has one element, the empty function (Proposition 1.5.2), while $\emptyset^{\{0\}} = \emptyset$; there is no injection from a one-element set into $\emptyset$. The proof used a_0 exactly once, and here there is no a_0 . (If $A' = \emptyset$, then $A = \emptyset$ too, since a function into $\emptyset$ has empty domain.)

Quick check. Where does the proof of (c) use that v is injective? Where does it use that u is injective?

Solution. Injectivity of v makes $F(f)$ a function: the point b with $v(b) = b'$ must be unique. Injectivity of u makes F injective: $u(f(b)) = u(g(b))$ must give $f(b) = g(b)$.

3.6.4 Encoding: the diagonals of $\mathbb{N} \times \mathbb{N}$

Section 3.1 showed $\mathbb{N} \times \mathbb{N}$ countable by an injection. At the scratch work for Theorem 3.1.6 it set aside the list along the diagonals, because writing a formula for the position of (m, n) and checking that every position is used takes real work. The Quick check before 3.4’s Looking-ahead remark got $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$ from Theorem 3.4.3 without ever seeing a bijection. Here is the work, done.

For $s \in \mathbb{N}$, the **triangular number** $\tau_s := \sum_{i=1}^s i$ (Definition 2.3.1) has $\tau_0 = 0$ and $\tau_{s+1} = \tau_s + s + 1$. It counts the points on the diagonals $m + n = 0, 1, \dots, s - 1$, which hold $1, 2, \dots, s$ points.

Example. The diagonal pairing of $\mathbb{N} \times \mathbb{N}$ with $\mathbb{N}$

Show that $\pi(m, n) := \tau_{m+n} + n$ is a bijection $\mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$.

Idea (Scratch work). What must the code record? Which diagonal the point is on, $s = m + n$, and its place on that diagonal, $n \in \{0, \dots, s\}$; from s and n we read back $m = s - n$. The diagonals before diagonal s hold $1 + 2 + \dots + s = \tau_s$ points, so the code counts them and adds the place. Small values: diagonal 0 gives 0; diagonal 1 gives 1, 2; diagonal 2 gives 3, 4, 5.

The decoder must find, for each k , the diagonal it falls on.

Givens	Goal
$(m, n) \in \mathbb{N} \times \mathbb{N}$	$\pi(m, n) \in \mathbb{N}$
$k \in \mathbb{N}$	exactly one (m, n) with $\tau_{m+n} + n = k$
gap	every $k \in \mathbb{N}$ is $\tau_s + n$ with $s, n \in \mathbb{N}$, $n \leq s$, in exactly one way

Existence by induction on k : stepping from k to $k+1$ moves one place along the diagonal, or, at its end, to the start of the next one. Uniqueness: diagonal s fills the block $\tau_s, \dots, \tau_s + s$, just below τ_{s+1} , so different diagonals give different numbers.

Solution.

Claim. For every $k \in \mathbb{N}$ there are $s, n \in \mathbb{N}$ with $n \leq s$ and $k = \tau_s + n$, and the pair (s, n) is unique.

Proof. Existence, by Theorem 2.2.1 from 0. First, $0 = \tau_0 + 0$. Suppose $k = \tau_s + n$ with $n \leq s$. If $n < s$, then $k+1 = \tau_s + (n+1)$ with $n+1 \leq s$. If $n = s$, then $k+1 = \tau_s + s + 1 = \tau_{s+1} + 0$.

Uniqueness. First, $\tau_{j+1} = \tau_j + j + 1 > \tau_j$ for every j , so if $s < s'$, then $\tau_{s+1} \leq \tau_{s'}$, by Theorem 2.2.1 on s' from $s+1$. Now let $\tau_s + n = \tau_{s'} + n'$ with $n \leq s$ and $n' \leq s'$, and suppose $s \neq s'$; by symmetry $s < s'$. Then

$$\tau_s + n \leq \tau_s + s < \tau_{s+1} \leq \tau_{s'} \leq \tau_{s'} + n',$$

a contradiction. So $s = s'$, and then $n = n'$. ■

The bijection. $\pi(m, n) \in \mathbb{N}$, since $\tau_{m+n} \in \mathbb{N}$, by Theorem 2.2.1 on s from $\tau_0 = 0$ and $\tau_{s+1} = \tau_s + s + 1$ with Lemma 2.1.1 (b). For $k \in \mathbb{N}$, write $k = \tau_s + n$ by the claim and set $\delta(k) := (s - n, n)$, where $s - n \in \mathbb{N}$ because $n \leq s$ (Lemma 2.1.1 (d)); the uniqueness in the claim makes δ a function. Then $\pi(\delta(k)) = \tau_{(s-n)+n} + n = \tau_s + n = k$. And $\delta(\pi(m, n)) = (m, n)$, by the uniqueness applied to $k = \tau_{m+n} + n$, where $s = m + n \geq n$. By Theorem 1.6.4, π is a bijection.

A table of the first values: $\pi(0, 0) = 0$, $\pi(1, 0) = 1$, $\pi(0, 1) = 2$, $\pi(2, 0) = 3$, $\pi(1, 1) = 4$, $\pi(0, 2) = 5$. Decoding 11: $\tau_4 = 10 \leq 11 < 15 = \tau_5$, so $11 = \tau_4 + 1$ and $\delta(11) = (3, 1)$.

Example. Method: build a bijection by encoding and decoding

Template. (1) Say what an element of the source must record for nothing to be lost. (2) Choose a code: a rule sending each element to an element of the target, and check that it lands there. (3) Write the decoder: a rule reading an element of the source back from each element of the target, and check that it is a function, with exactly one answer for each input. (4) Check both round trips and cite Theorem 1.6.4.

When to use it. The two sets carry the same information arranged differently: two numbers

in one, a pair of sequences in one sequence, a function of two variables as a function with function values.

The usual failure. Checking one round trip only: $\delta \circ \pi = \text{id}$ alone shows only that π is injective (Theorem 1.6.1). A decoder that is not a function, with two readings of one code or none (the interleaving of decimals, later in this section). If the decoder works on part of the target only, keep the injection and use Example (Method: injections both ways).

Warning. An injective code is not yet a bijection. The code $2^m 3^n$ of Theorem 3.1.6 is injective, but 5 is not a value, and no decoder is defined at 5. Step (3) of the method, a decoder defined on the **whole** target, is what makes π a bijection.

Quick check. Compute $\pi(3, 2)$ and $\delta(47)$.

Solution. $\pi(3, 2) = \tau_5 + 2 = 15 + 2 = 17$. For 47: $\tau_9 = 45 \leq 47 < 55 = \tau_{10}$, so $47 = \tau_9 + 2$, and $\delta(47) = (9 - 2, 2) = (7, 2)$. Check: $\pi(7, 2) = \tau_9 + 2 = 47$.

3.6.5 The laws of exponents, for all sets

For numbers, $m^{n+k} = m^n m^k$ and $(m^n)^k = m^{nk}$. Read through the sets these numbers count, each law says that two sets of functions are the same size, and for sets we must find the bijection.

Theorem 3.6.3. Laws of Cardinal Arithmetic

For all sets A, B, C, X, Y, Z :

- (a) $|A \sqcup B| = |B \sqcup A|$, $|(A \sqcup B) \sqcup C| = |A \sqcup (B \sqcup C)|$, $|A \times B| = |B \times A|$ and $|(A \times B) \times C| = |A \times (B \times C)|$;
- (b) $|A \times (B \sqcup C)| = |(A \times B) \sqcup (A \times C)|$;
- (c) $X^\emptyset$ has exactly one element, and $|X^{\{0\}}| = |X|$;
- (d) $|X^{Y \sqcup Z}| = |X^Y \times X^Z|$;
- (e) $|(X \times Y)^Z| = |X^Z \times Y^Z|$;
- (f) $|(X^Y)^Z| = |X^{Y \times Z}|$.

Idea (Scratch work). For (d): what is an element of each side? On the left, a function h defined on the tagged copies of Y and Z . On the right, a pair (f, g) with $f: Y \rightarrow X$ and $g: Z \rightarrow X$. A function on two disjoint pieces is the same thing as a function on each piece. So cut h into its two pieces by composing with the inclusions, and glue a pair back together piece by piece.

Givens	Goal
$h \in X^{Y \sqcup Z}$	an element of $X^Y \times X^Z$: $(h \circ \iota_Y, h \circ \iota_Z)$
$(f, g) \in X^Y \times X^Z$	one h with $h \circ \iota_Y = f$ and $h \circ \iota_Z = g$
gap	$h(y, 0) := f(y)$, $h(z, 1) := g(z)$ is a function: the parts do not overlap (after Definition 3.6.1)

Proof.

- (d) Let $\Phi(h) := (h \circ \iota_Y, h \circ \iota_Z)$ for $h \in X^{Y \sqcup Z}$. For $(f, g) \in X^Y \times X^Z$, let $\Psi(f, g)$ be the function $h: Y \sqcup Z \rightarrow X$ with

$$h(y, 0) := f(y), \quad h(z, 1) := g(z) \quad (y \in Y, z \in Z).$$

This is a function, because every element of $Y \sqcup Z$ has exactly one of the two forms. Then $\Phi(\Psi(f, g)) = (f, g)$: for $y \in Y$, $h(\iota_Y(y)) = h(y, 0) = f(y)$, so $h \circ \iota_Y = f$ by Proposition 1.5.1, and likewise $h \circ \iota_Z = g$; the pairs are equal by Definition 1.4.1. And $\Psi(\Phi(h)) = h$: the two functions agree at every $(y, 0)$ and every $(z, 1)$, which are all the points of $Y \sqcup Z$, so they are equal by Proposition 1.5.1. By Theorem 1.6.4, Φ is a bijection.

- (e) For $g \in (X^Y)^Z$, each $g(z)$ is a function $Y \rightarrow X$. Let $\Phi(g): Y \times Z \rightarrow X$, $\Phi(g)(y, z) := g(z)(y)$. For $h \in X^{Y \times Z}$ and $z \in Z$, the rule $y \mapsto h(y, z)$ is an element of X^Y ; let $\Psi(h): Z \rightarrow X^Y$ send z to it. Then

$$\Phi(\Psi(h))(y, z) = \Psi(h)(z)(y) = h(y, z)$$

for all (y, z) , so $\Phi(\Psi(h)) = h$. And $\Psi(\Phi(g))(z)$ is the function $y \mapsto g(z)(y)$, which is $g(z)$; so $\Psi(\Phi(g)) = g$. Here Proposition 1.5.1 is used twice: first for functions on Y , then for functions on Z . By Theorem 1.6.4, Φ is a bijection.

The remaining parts are proved by the same kind of regrouping; the maps are in the fold below.

■

○ Second reading · The other laws

Each map below has the stated inverse, and each round trip is one line of Proposition 1.5.1 and Definition 1.4.1. As a sample, the associativity of $\sqcup$ has three cases, one for each form of element; on $((b, 1), 0)$ the map gives $((b, 0), 1)$, and the inverse, reading the tag 1 outside and the tag 0 inside, returns $((b, 1), 0)$.

- (a) $A \sqcup B \rightarrow B \sqcup A$: $(a, 0) \mapsto (a, 1)$, $(b, 1) \mapsto (b, 0)$; it is its own inverse, with the roles of A and B exchanged. $(A \sqcup B) \sqcup C \rightarrow A \sqcup (B \sqcup C)$: $((a, 0), 0) \mapsto (a, 0)$, $((b, 1), 0) \mapsto ((b, 0), 1)$, $(c, 1) \mapsto ((c, 1), 1)$; the three forms of the source do not overlap, and the inverse reads the three forms of the target back. $A \times B \rightarrow B \times A$: $(a, b) \mapsto (b, a)$. $(A \times B) \times C \rightarrow A \times (B \times C)$: $((a, b), c) \mapsto (a, (b, c))$, with inverse $(a, (b, c)) \mapsto ((a, b), c)$.
- (b) $A \times (B \sqcup C) \rightarrow (A \times B) \sqcup (A \times C)$: $(a, (b, 0)) \mapsto ((a, b), 0)$ and $(a, (c, 1)) \mapsto ((a, c), 1)$; the

inverse moves the tag back inside.

- (c) $X^\emptyset = \{(\emptyset, X)\}$, the empty function, by Proposition 1.5.2 (a). The map $f \mapsto f(0)$ is a bijection $X^{\{0\}} \rightarrow X$, with inverse sending x to the function $0 \mapsto x$.
- (d) Let $p_1(x, y) := x$ and $p_2(x, y) := y$ on $X \times Y$. The map $h \mapsto (p_1 \circ h, p_2 \circ h)$ from $(X \times Y)^Z$ to $X^Z \times Y^Z$ has the inverse $(f, g) \mapsto (z \mapsto (f(z), g(z)))$.

Law (f) is called **currying**: a function of two variables becomes a function whose values are functions. For finite sets with m , n and k elements, the theorem gives back $m^{n+k} = m^n m^k$ and $(m^n)^k = m^{nk}$ with no induction in sight; the induction has moved into the counting of Section 2.5. Nothing in the proof used finiteness.

Example. Method: prove a law of sizes by a bijection of sets

Template. (1) Write out what an element of each side is: a tagged element, a pair, a function, a function with function values. (2) Find the map that only regroups: compose with the inclusions, pair the coordinates, or curry. (3) Write the reverse regrouping. (4) Check both round trips with Proposition 1.5.1 and Definition 1.4.1, and cite Theorem 1.6.4.

When to use it. A law familiar from numbers, such as $m^{n+k} = m^n m^k$, is claimed for sets of any size; or a size is to be computed by rewriting a set step by step.

The usual failure. Computing with symbols, as in “ $|X|^{|Y|+|Z|} = |X|^{|Y|} |X|^{|Z|}$ ”, when no number $|X|$ exists and the step is the law itself: (N9) of Logic and Proof, Example (What is not allowed). Dropping the tags: with $\cup$ in place of $\sqcup$ the law fails: for $X = \{0, 1\}$ and $Y = Z = \{0\}$, $X^{Y \cup Z}$ has 2 elements and $X^Y \times X^Z$ has 4 (Exercise B4 (b)).

Quick check. Let $X = \{0, 1\}$, $Y = \{a\}$ and $Z = \{b, c\}$. How many elements has each side of (d)? Let $h(a, 0) = 1$, $h(b, 1) = 0$, $h(c, 1) = 1$. What is $\Phi(h)$?

Solution. $Y \sqcup Z = \{(a, 0), (b, 1), (c, 1)\}$ has three elements, and a function from it to $\{0, 1\}$ is fixed by three values, each 0 or 1: $2 \cdot 2 \cdot 2 = 8$ functions. On the right, X^Y has 2 elements and X^Z has 4, so the product has $2 \cdot 4 = 8$. And $\Phi(h) = (f, g)$ with $f(a) = 1$, $g(b) = 0$, $g(c) = 1$.

3.6.6 Subsets are 0–1 functions

Section 1.5 stated, for every set, that subsets and 0–1 functions match, and gave both maps: send f to $\{x : f(x) = 1\}$ and A to $\mathbf{1}_A$. Here are the two round trips, which make 2 a base like any other.

Theorem 3.6.4. Subsets and 0–1 Functions

For every set X , the map $A \mapsto \mathbf{1}_A$ is a bijection $\mathcal{P}(X) \rightarrow \{0, 1\}^X$, with inverse $f \mapsto \{x \in X : f(x) = 1\}$. In particular $|\mathcal{P}(X)| = |\{0, 1\}^X|$.

Proof. For $A \subseteq X$, $\mathbf{1}_A \in \{0, 1\}^X$ (Example (First functions) (d)), and $\{x \in X : \mathbf{1}_A(x) = 1\} = A$ by the definition of $\mathbf{1}_A$. For $f \in \{0, 1\}^X$, let $S := \{x \in X : f(x) = 1\}$. For $x \in S$, $\mathbf{1}_S(x) = 1 = f(x)$. For $x \in X \setminus S$, $f(x) \neq 1$, so $f(x) = 0 = \mathbf{1}_S(x)$. So $\mathbf{1}_S = f$ (Proposition 1.5.1). By Theorem 1.6.4, $A \mapsto \mathbf{1}_A$ is a bijection. ■

Section 2.5 (the fold after Proposition 2.5.8), Section 3.3 (after Corollary 3.3.3) and Section 3.4 (the Quick check after Proposition 3.4.2) quoted this correspondence; it is now a theorem to cite.

Corollary 3.6.5. No Set Is the Size of Its 0–1 Functions

For every set X , $|X| < |\{0, 1\}^X|$.

Idea. One injection is easy; for strictness, move a bijection over to $\mathcal{P}(X)$ with the theorem just proved, where Cantor’s theorem forbids it.

Proof. The map $x \mapsto \mathbf{1}_{\{x\}}$ is injective, since $\mathbf{1}_{\{x\}}$ takes the value 1 at x only; so $|X| \leq |\{0, 1\}^X|$. A bijection $X \rightarrow \{0, 1\}^X$, followed by the inverse of the bijection of Theorem 3.6.4, would be a bijection $X \rightarrow \mathcal{P}(X)$ (Theorem 1.5.4 (c)), in particular a surjection, against Theorem 3.3.2. ■

So $\mathbb{N}$, $\{0, 1\}^{\mathbb{N}}$, $\{0, 1\}^{\{0, 1\}^{\mathbb{N}}}$, ... grow strictly at each step, and there is no largest size.

3.6.7 No set of all sets, once more

Section 3.3 (consequence (i) after Theorem 3.3.2) saw that Russell’s argument is Cantor’s, with the rule $f(x) = x$ and R_A in the role of D . What is new here is a proof **by sizes** of the last clause of Theorem 1.2.4: there is no set of which every set is an element.

Suppose U were such a set. Every subset of U is a set, hence an element of U , so $\mathcal{P}(U) \subseteq U$. Define $f: U \rightarrow \mathcal{P}(U)$ by $f(u) := u$ if $u \in \mathcal{P}(U)$, and $f(u) := \emptyset$ otherwise. It is onto: each $S \in \mathcal{P}(U)$ lies in U , and $f(S) = S$. This contradicts Theorem 3.3.2.

Cantor’s set for this f , $D = \{u \in U : u \notin f(u)\}$, agrees with $R_U = \{u \in U : u \notin u\}$ on $\mathcal{P}(U)$, and contains every $u \in U \setminus \mathcal{P}(U)$, since $u \notin \emptyset$. The unrestricted collection $\{x : x \notin x\}$ is never formed.

3.6.8 The size of the line

The hook asked about $\mathbb{R} \times \mathbb{R}$; first $\mathbb{R}$ itself. A real number in $[0, 1)$ is a digit sequence, a function $\mathbb{Z}_{>0} \rightarrow \{0, \dots, 9\}$. So $\mathbb{R}$ should be a power, and that power should be a power of 2.

Theorem 3.6.6. The Line Is a Power of Two

$$|\mathbb{R}| = |\{0, 1\}^{\mathbb{N}}| = |\mathcal{P}(\mathbb{N})|.$$

Idea. Injections both ways (Example (Method: injections both ways)). Into the 0–1 sequences, the digits are encoded and the laws do the bookkeeping. Out of them, a 0–1 sequence is read as decimal digits 0 and 1, which contain no 9.

Proof. Let $T := \{0, 1, \dots, 9\}$ and $W := T^{\mathbb{Z}_{>0}}$, the set of digit sequences (Definition 3.3.1).

$|[0, 1]| \leq |W|$. This is the step of the proof of Theorem 3.3.4. Send x to its expansion not ending in all 9s: one exists by (D1), and only one by (D3), so the rule is a function and no choice is made. It is injective, since a digit sequence is an expansion of only one number, by (D2).

$|W| \leq |\{0, 1\}^{\mathbb{N}}|$. The map $n \mapsto n + 1$ is a bijection $\mathbb{N} \rightarrow \mathbb{Z}_{>0}$ (inverse $m \mapsto m - 1$, Lemma 2.1.1 (c)), so $|W| = |T^{\mathbb{N}}|$ (Proposition 3.6.1 (c)). The map $j \mapsto \mathbf{1}_{\{j\}}$ injects T into $\{0, 1\}^T$, so $|T^{\mathbb{N}}| \leq |(\{0, 1\}^T)^{\mathbb{N}}|$ (Proposition 3.6.2 (c), as $\{0, 1\}^T \neq \emptyset$), and this is $|\{0, 1\}^{T \times \mathbb{N}}|$ by Theorem 3.6.3 (f). A pair (j, n) is recorded by one number, by the method of Example (Method: build a bijection by encoding and decoding): the code $(j, n) \mapsto 10n + j$ is a bijection $T \times \mathbb{N} \rightarrow \mathbb{N}$, whose decoder takes quotient and remainder on division by 10 (Theorem 2.2.3, with the quotient in $\mathbb{N}$ as in the claim in the proof of Proposition 3.1.5). So $|\{0, 1\}^{T \times \mathbb{N}}| = |\{0, 1\}^{\mathbb{N}}|$ (Proposition 3.6.1 (c)). Composing the maps gives an injection $W \rightarrow \{0, 1\}^{\mathbb{N}}$ (Theorem 1.5.4 (a)).

$|\{0, 1\}^{\mathbb{N}}| \leq |[0, 1]|$. For $b \in \{0, 1\}^{\mathbb{N}}$, let $c_{k+1} := b(k)$ for $k \in \mathbb{N}$: a digit sequence with digits 0 and 1 only. By (D2) it is an expansion of exactly one $y_b \in [0, 1]$, and $y_b \leq t_1 + \frac{1}{10} \leq \frac{2}{10}$ by Definition 3.3.1 at $n = 1$, so $y_b \in [0, 1)$. If $b \neq b'$, the two digit sequences differ. If also $y_b = y_{b'}$, they would be two different expansions of one number, and by (D3) one of them would end in all 9s; but neither contains a 9. So $y_b \neq y_{b'}$, and $b \mapsto y_b$ is injective.

Conclusion. By Proposition 3.4.1 (b) and Theorem 3.4.3, $|[0, 1]| = |\{0, 1\}^{\mathbb{N}}|$. By Example (The real line and its intervals), $|[0, 1]| = |\mathbb{R}|$, and by Theorem 3.6.4, $|\{0, 1\}^{\mathbb{N}}| = |\mathcal{P}(\mathbb{N})|$. Chaining with Proposition 2.5.1 proves the theorem. ■

The first step is the one of Exercise C1 of Section 3.4. What is new is the middle step, where the laws reduce the bookkeeping to the one-line code $(j, n) \mapsto 10n + j$ in place of the set $E(x)$ of that exercise, and the last, where the digits 0 and 1 suffice because (D3) needs only that no 9 appears. Neither step needed binary expansions of real numbers.

Remark (Notation in other books). Many books treat sizes as objects, called **cardinal numbers**, and write $\aleph_0$ for the size of $\mathbb{N}$ and $2^{\aleph_0}$, or $\mathfrak{c}$, for the size of $\mathbb{R}$. Making a size into an object needs more set theory than this book uses (Section 2.5, the fold after Propo-

sition 2.5.1). Here “ $|A| = 2^{\aleph_0}$ ” can be read only as shorthand for $|A| = |\{0, 1\}^{\mathbb{N}}|$. Whether some subset of $\mathbb{R}$ is strictly bigger than $\mathbb{N}$ and strictly smaller than $\mathbb{R}$ is the **continuum hypothesis**; it is known to be neither provable nor refutable from the usual axioms of set theory, if those axioms are consistent.

Quick check. Which step of the proof of [Theorem 3.6.6](#) uses the axiom of choice?

Solution. None. The expansion of x is picked by a rule (“the one not ending in all 9s”), every other map is a formula, and Theorem 3.4.3 was proved without choice (Section 3.4).

3.6.9 Back to the plane

Example. Interleaving digits

The natural map $[0, 1) \times [0, 1) \rightarrow [0, 1)$ interleaves digits. If $x = 0.a_1a_2\dots$ and $y = 0.b_1b_2\dots$, with the expansions not ending in all 9s, let

$$F(x, y) := 0.a_1b_1a_2b_2\dots;$$

the inverse splits the digits of z into the odd and the even places. Is F a bijection?

Solution. F is a function into $[0, 1)$. The expansions of x and y are fixed by the rule, as in the last proof. Let c be the interleaved sequence: $c_{2k-1} := a_k$, $c_{2k} := b_k$. It has infinitely many places that are not 9 (those of a), so it does not end in all 9s, and by (D2) it is an expansion of exactly one $z \in [0, 1]$. To see $z < 1$, let n be the first place with $c_n \leq 8$ (Theorem 2.1.3). Every earlier digit is 9, so by Proposition 2.3.6

$$t_n \leq (1 - 10^{-(n-1)}) + 8 \cdot 10^{-n} = 1 - 2 \cdot 10^{-n},$$

and $z \leq t_n + 10^{-n} \leq 1 - 10^{-n} < 1$.

F is injective. If $F(x, y) = F(x', y') = z$, both interleaved sequences are expansions of z and neither ends in all 9s, so by (D3) they are equal. Then $a = a'$ and $b = b'$, and $x = x'$, $y = y'$ by (D2).

F is not onto. Take $z = \frac{1}{11} = 0.090909\dots$. The truncations at even places are $t_{2j} = \frac{9}{99}(1 - 100^{-j}) = \frac{1}{11} - \frac{1}{11}100^{-j}$ (Proposition 2.3.6 with $r = \frac{1}{100}$), and the inequalities of Definition 3.3.1 hold at every place. This expansion has no tail of 0s and no tail of 9s, so by (D3) it is the only expansion of $\frac{1}{11}$. A preimage (x, y) would need $b = 9, 9, 9, \dots$; but b was the expansion of y not ending in all 9s.

The splitting “inverse” named “the $y \in [0, 1)$ whose expansion is 999...” without checking that such a y exists: that is (N14) of Logic and Proof, Example (What is not allowed). So the direct route gives an injection and no bijection. The injection is enough (Example (Method: injections both ways)), and the laws give a bijection with no digit-fiddling.

Theorem 3.6.7. The Plane Is the Size of the Line

$$|\mathbb{R} \times \mathbb{R}| = |\mathbb{R}|.$$

Idea. By the method of [Example \(Method: prove a law of sizes by a bijection of sets\)](#): replace $\mathbb{R}$ by $\{0, 1\}^{\mathbb{N}}$ and rewrite the plane step by step.

Proof. By [Theorem 3.6.6](#) and [Proposition 3.6.1](#) (b), $|\mathbb{R} \times \mathbb{R}| = |\{0, 1\}^{\mathbb{N}} \times \{0, 1\}^{\mathbb{N}}|$. By [Theorem 3.6.3](#) (d), this is $|\{0, 1\}^{\mathbb{N} \sqcup \mathbb{N}}|$. By [Example \(Two copies of \$\mathbb{N}\$ \)](#) and [Proposition 3.6.1](#) (c), this is $|\{0, 1\}^{\mathbb{N}}|$, which is $|\mathbb{R}|$ by [Theorem 3.6.6](#). Chaining with [Proposition 2.5.1](#) proves the theorem. ■

Read through the maps, the composite on 0–1 sequences sends (a, b) to the sequence with $a(n)$ at place $2n$ and $b(n)$ at place $2n + 1$: the interleaving of Exercise B3 of Section 3.4. The trouble with decimals has gone because 0–1 sequences, unlike numbers, have no double expansions. That price is paid once, in the proof of [Theorem 3.6.6](#).

Theorem 3.6.8. Sequences of Natural Numbers

$$|\mathbb{N}^{\mathbb{N}}| = |\mathbb{R}|.$$

Idea. By the method of [Example \(Method: prove a law of sizes by a bijection of sets\)](#), with injections both ways: a 0–1 sequence is already a sequence of natural numbers, and a natural number is recorded by a 0–1 sequence.

Proof. Send $b \in \{0, 1\}^{\mathbb{N}}$ to the same rule with codomain $\mathbb{N}$. This map is injective: two sequences with the same image have the same value at every point, so they are equal ([Proposition 1.5.1](#)). In the other direction, $n \mapsto \mathbf{1}_{\{n\}}$ is an injection $\mathbb{N} \rightarrow \{0, 1\}^{\mathbb{N}}$, so $|\mathbb{N}^{\mathbb{N}}| \leq |(\{0, 1\}^{\mathbb{N}})^{\mathbb{N}}|$ ([Proposition 3.6.2](#) (c), as $\{0, 1\}^{\mathbb{N}} \neq \emptyset$). This is $|\{0, 1\}^{\mathbb{N} \times \mathbb{N}}|$ ([Theorem 3.6.3](#) (f)), and that is $|\{0, 1\}^{\mathbb{N}}|$ by [Example \(The diagonal pairing of \$\mathbb{N} \times \mathbb{N}\$ with \$\mathbb{N}\$ \)](#) and [Proposition 3.6.1](#) (c). By [Proposition 3.4.1](#) (b) and [Theorem 3.4.3](#), $|\mathbb{N}^{\mathbb{N}}| = |\{0, 1\}^{\mathbb{N}}|$, which is $|\mathbb{R}|$ by [Theorem 3.6.6](#). ■

Exercise B4 (d) of Section 3.4 reached the equality $|\mathbb{N}^{\mathbb{N}}| = |\{0, 1\}^{\mathbb{N}}|$ through graphs and $\mathcal{P}(\mathbb{N} \times \mathbb{N})$.

Corollary 3.6.9. Sequences of Real Numbers

$$|\mathbb{R}^{\mathbb{N}}| = |\mathbb{R}|.$$

Proof. In one chain,

$$\begin{aligned} |\mathbb{R}^{\mathbb{N}}| &= |(\{0, 1\}^{\mathbb{N}})^{\mathbb{N}}| = |\{0, 1\}^{\mathbb{N} \times \mathbb{N}}| \\ &= |\{0, 1\}^{\mathbb{N}}| = |\mathbb{R}|, \end{aligned}$$

by [Proposition 3.6.1](#) (c) with [Theorem 3.6.6](#), then [Theorem 3.6.3](#) (f), then [Example \(The diagonal pairing of \$\mathbb{N} \times \mathbb{N}\$ with \$\mathbb{N}\$ \)](#) with [Proposition 3.6.1](#) (c), and [Theorem 3.6.6](#) again, chained by [Proposition 2.5.1](#). No further appeal to [Theorem 3.4.3](#) is needed beyond the one inside [Theorem 3.6.6](#). ■

So both guesses of the hook were wrong. The plane is no bigger than the line, and $\mathbb{N}^{\mathbb{N}}$ is no bigger either. For every infinite set X it is in fact true that $|X \times X| = |X|$ and $|X \sqcup X| = |X|$; in general these cannot be proved without the axiom of choice (the first is equivalent to it), and this book does not prove them.

Quick check. Show that $|\mathbb{R}^{\mathbb{N}} \times \mathbb{R}| = |\mathbb{R}|$.

Solution. By [Corollary 3.6.9](#) and [Proposition 3.6.1](#) (b), $|\mathbb{R}^{\mathbb{N}} \times \mathbb{R}| = |\mathbb{R} \times \mathbb{R}|$, which is $|\mathbb{R}|$ by [Theorem 3.6.7](#); chain with [Proposition 2.5.1](#).

Remark (Looking ahead). Respecting size, [Proposition 3.6.1](#), is an instance of a requirement that [Section 4.2](#) names: a rule stated through representatives must give the same answer for all of them. There it is called well-definedness, and it is what makes functions on quotient sets possible.

3.6.10 Exercises

3.6.10.1 A. Check your understanding

Exercise. A1

- True or false, for every set A : $|\emptyset \sqcup A| = |A|$; $\emptyset \times A = \emptyset$; $A^{\emptyset}$ has exactly one element; $\emptyset^A = \emptyset$.
- Under the bijection of [Theorem 3.6.3](#) (f) with $X = Y = \{0, 1\}$ and $Z = \{0\}$, which element of $(X^Y)^Z$ corresponds to $h(y, z) := y$?
- Give an injection $\mathbb{R} \sqcup \mathbb{N} \rightarrow \mathbb{R}$.
- The proof of [Theorem 3.6.6](#) reads a 0–1 sequence as decimal digits 0 and 1. Which

other pairs of digits give an injection into $[0, 1)$ in the same way? Why does the pair 0 and 9 not follow from (D3) alone?

Solution.

- (a) True: $\emptyset \sqcup A = A \times \{1\}$, and $(a, 1) \mapsto a$ is a bijection onto A . True: no pair has a first coordinate in $\emptyset$. True, by Proposition 1.5.2 (a). False: for $A = \emptyset$, $\emptyset^\emptyset$ has one element, the empty function; the claim holds for every non-empty A , by Proposition 1.5.2 (b).
- (b) The g with $g(0) = \text{id}_{\{0,1\}}$, since $g(0)(y) = h(y, 0) = y$ for both $y \in \{0, 1\}$.
- (c) Send $(x, 0) \mapsto x/(1 + |x|)$, which lies in $(-1, 1)$ (Example (The real line and its intervals)), and $(n, 1) \mapsto n + 1 \geq 1$. Each part is injective (the first is a bijection onto $(-1, 1)$, the second cancels the 1), and the values of the two parts are disjoint, so the map is injective.
- (d) Any pair that misses 9 works unchanged: a sequence with no 9s cannot end in all 9s, so (D3) rules out two different expansions of one number, and the first digit is at most 8, so $y_b \leq \frac{8}{10} + \frac{1}{10} < 1$. Any pair that misses 0 gives an injection too, since a sequence with no 0s cannot end in all 0s; but if the pair contains 9, the sequence of all 9s goes to 1, so the target must be widened to $[0, 1]$, which Example (The real line and its intervals) also covers. (The digits 1 and 2, used in Exercise C1 of Section 3.4, miss both.) With the digits 0 and 9, one sequence could end in all 9s and another in all 0s, which is exactly the situation (D3) allows; so (D3) alone does not decide whether $b \mapsto y_b$ is injective, and a further computation at the first differing place would be needed.

3.6.10.2 B. Practice

Exercise. B1: Encodings

Prove each equality by an explicit bijection and its inverse.

- (a) $|\mathbb{N} \times \{0, 1, 2\}| = |\mathbb{N}|$.
- (b) $|\{0, 1\}^{\mathbb{N}}| = |\{0, 1, 2, 3\}^{\mathbb{N}}|$.
- (c) $|\mathbb{N} \times \mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$, using the pairing π of [Example \(The diagonal pairing of \$\mathbb{N} \times \mathbb{N}\$ with \$\mathbb{N}\$ \)](#) twice, with an explicit decoder.

Solution.

- (a) Send $(n, r) \mapsto 3n + r$. The inverse sends m to (q, r) , the quotient and remainder of m on division by 3 (Theorem 2.2.3, with $q \in \mathbb{N}$ as in the claim in the proof of Proposition 3.1.5). Both round trips follow from the uniqueness in the division algorithm.
- (b) For $c \in \{0, 1\}^{\mathbb{N}}$ let $\Phi(c)(n) := 2c(2n) + c(2n + 1) \in \{0, 1, 2, 3\}$. For the inverse, given $d \in \{0, 1, 2, 3\}^{\mathbb{N}}$, write $d(n) = 2q_n + r_n$ with $q_n, r_n \in \{0, 1\}$ (division by 2, unique), and set $c(2n) := q_n$, $c(2n + 1) := r_n$. This defines c on all of $\mathbb{N}$, since each $m \in \mathbb{N}$ is $2n$ or $2n + 1$ for exactly one n . The round trips follow from the two uniqueness statements and Proposition 1.5.1.
- (c) Let $E(m, n, k) := \pi(\pi(m, n), k)$. The decoder sends k' to (m, n, k) , where $\delta(k') = (j, k)$ and $\delta(j) = (m, n)$. The round trips follow from $\delta \circ \pi = \text{id}$ and $\pi \circ \delta = \text{id}$, each used twice, together with the characteristic property of triples (the paragraph after the proof

of Corollary 3.1.7). For example, $E(1, 0, 1) = \pi(\pi(1, 0), 1) = \pi(1, 1) = 4$.

Exercise. B2: More laws

By the method of [Example \(Method: prove a law of sizes by a bijection of sets\)](#), prove for all sets A, B, X :

- (a) $|\mathcal{P}(A \sqcup B)| = |\mathcal{P}(A) \times \mathcal{P}(B)|$;
- (b) $|X^{\{0,1\}}| = |X \times X|$.

Solution.

- (a) Directly: send $S \mapsto (\{a \in A : (a, 0) \in S\}, \{b \in B : (b, 1) \in S\})$, with inverse $(S_1, S_2) \mapsto (S_1 \times \{0\}) \cup (S_2 \times \{1\})$. The round trips hold because every element of $A \sqcup B$ is $(a, 0)$ or $(b, 1)$, and not both (after [Definition 3.6.1](#)). Or by laws: $|\mathcal{P}(A \sqcup B)| = |\{0, 1\}^{A \sqcup B}|$ by [Theorem 3.6.4](#), which is $|\{0, 1\}^A \times \{0, 1\}^B|$ by [Theorem 3.6.3](#) (d), which is $|\mathcal{P}(A) \times \mathcal{P}(B)|$ by [Theorem 3.6.4](#) twice with [Proposition 3.6.1](#) (b).
- (b) Send $f \mapsto (f(0), f(1))$, with inverse sending (x, x') to the function $0 \mapsto x, 1 \mapsto x'$. Or from (c) and (d) of [Theorem 3.6.3](#), since $\{0, 1\}$ is the same size as $\{0\} \sqcup \{0\}$, by $0 \mapsto (0, 0), 1 \mapsto (0, 1)$.

Exercise. B3: Sets the size of the line, used later

Prove:

- (a) $|\mathbb{N} \times \mathbb{R}| = |\mathbb{R}|$;
- (b) $|\mathbb{R} \sqcup \mathbb{R}| = |\mathbb{R}|$;
- (c) $|\mathbb{R}^k| = |\mathbb{R}|$ for every integer $k \geq 2$.

Solution.

- (a) $x \mapsto (0, x)$ injects $\mathbb{R}$ into $\mathbb{N} \times \mathbb{R}$. In the other direction, $\mathbb{N} \times \mathbb{R} \subseteq \mathbb{R} \times \mathbb{R}$, so the inclusion followed by a bijection $\mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$ ([Theorem 3.6.7](#)) is an injection $\mathbb{N} \times \mathbb{R} \rightarrow \mathbb{R}$. Apply [Theorem 3.4.3](#).
- (b) Unwinding [Definition 3.6.1](#), $\mathbb{R} \sqcup \mathbb{R} = (\mathbb{R} \times \{0\}) \cup (\mathbb{R} \times \{1\}) = \mathbb{R} \times \{0, 1\}$, a subset of $\mathbb{R} \times \mathbb{R}$; so it injects into $\mathbb{R}$ as in (a). And $x \mapsto (x, 0)$ injects $\mathbb{R}$ into $\mathbb{R} \sqcup \mathbb{R}$. Apply [Theorem 3.4.3](#).
- (c) By [Theorem 2.2.1](#) with $n_0 = 2$. The base case $k = 2$ is [Theorem 3.6.7](#). Step: the map $((x_1, \dots, x_k), x_{k+1}) \mapsto (x_1, \dots, x_{k+1})$ is a bijection $\mathbb{R}^k \times \mathbb{R} \rightarrow \mathbb{R}^{k+1}$, by the characteristic property of tuples (the paragraph after the proof of [Corollary 3.1.7](#)). So

$$|\mathbb{R}^{k+1}| = |\mathbb{R}^k \times \mathbb{R}| = |\mathbb{R} \times \mathbb{R}| = |\mathbb{R}|,$$

by the hypothesis with [Proposition 3.6.1](#) (b), then [Theorem 3.6.7](#), chained by [Proposition 2.5.1](#). (The book has no 1-tuples and defines X^k for $k \geq 2$ only, so the induction

starts at 2.)

Exercise. B4: Prove or disprove

Prove each true statement and refute each false one with a counterexample. Here A, B, C, X, Y, Y', Z are sets.

- (a) If $|A \sqcup C| = |B \sqcup C|$, then $|A| = |B|$.
- (b) $|X^{Y \cup Z}| = |X^Y \times X^Z|$.
- (c) If $|Y| \leq |Y'|$, then $|X^Y| \leq |X^{Y'}|$.
- (d) $|\mathbb{N}^{\{0,1\}}| = |\{0,1\}^{\mathbb{N}}|$.
- (e) If $|A| < |B|$ and $C \neq \emptyset$, then $|A \times C| < |B \times C|$.
- (f) There is a set X with $|\{0,1\}^X| \leq |X|$.

Solution.

- (a) False. Take $A = \{0\}$, $B = \emptyset$, $C = \mathbb{N}$. The map $(0, 0) \mapsto 0$, $(n, 1) \mapsto n + 1$ is a bijection $\{0\} \sqcup \mathbb{N} \rightarrow \mathbb{N}$, with inverse $0 \mapsto (0, 0)$ and $m \mapsto (m - 1, 1)$ for $m \geq 1$ (Lemma 2.1.1 (c)). And $(n, 1) \mapsto n$ is a bijection $\emptyset \sqcup \mathbb{N} = \mathbb{N} \times \{1\} \rightarrow \mathbb{N}$. So both sides are the size of $\mathbb{N}$, while $|\{0\}| \neq |\emptyset|$.
- (b) False. Take $X = \{0, 1\}$ and $Y = Z = \{0\}$. Then $Y \cup Z = \{0\}$, and $X^{Y \cup Z}$ has 2 elements, while $X^Y \times X^Z$ has $2 \cdot 2 = 4$. Finite sets with different numbers of elements are not equinumerous (Corollary 2.5.4). The statement is true when $Y \cap Z = \emptyset$, by Quick check 1 (c) with Proposition 3.6.1 (c), and Theorem 3.6.3 (d).
- (c) False. Take $X = \emptyset$, $Y = \emptyset$, $Y' = \{0\}$: this is the non-example after Proposition 3.6.2. It is true when $X \neq \emptyset$, by Proposition 3.6.2 (c).
- (d) False. The map $f \mapsto (f(0), f(1))$ is a bijection $\mathbb{N}^{\{0,1\}} \rightarrow \mathbb{N} \times \mathbb{N}$, with inverse sending (m, n) to the function $0 \mapsto m$, $1 \mapsto n$. Since $\mathbb{N} \times \mathbb{N}$ is countable (Theorem 3.1.6), there is an injection $\mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ (Theorem 3.1.2), and so an injection $\mathbb{N}^{\{0,1\}} \rightarrow \mathbb{N}$ (Theorem 1.5.4 (a)). If $\mathbb{N}^{\{0,1\}}$ were the same size as $\{0, 1\}^{\mathbb{N}}$, composing would inject $\{0, 1\}^{\mathbb{N}}$ into $\mathbb{N}$, making it countable (Theorem 3.1.2), against Theorem 3.3.1. Base and exponent do not commute.
- (e) False. Take $A = \{0\}$, $B = \{0, 1\}$, $C = \mathbb{N}$; then $|A| < |B|$ (Corollary 2.5.4 for “no bijection”). But $|\{0\} \times \mathbb{N}| = |\mathbb{N}|$, by $(0, n) \mapsto n$, and $|\{0, 1\} \times \mathbb{N}| = |\mathbb{N}|$: the map $(r, n) \mapsto (n, r)$ is a bijection $\{0, 1\} \times \mathbb{N} \rightarrow \mathbb{N} \sqcup \mathbb{N}$, and Example (Two copies of $\mathbb{N}$) finishes.
- (f) False. For every X , $x \mapsto \mathbf{1}_{\{x\}}$ gives $|X| \leq |\{0, 1\}^X|$, so $|\{0, 1\}^X| \leq |X|$ would give $|X| = |\{0, 1\}^X|$ by Theorem 3.4.3, against Corollary 3.6.5.

3.6.10.3 C. Going deeper

Exercise. C1: Functions from the line to the line

Prove that $|\mathbb{R}^{\mathbb{R}}| = |\mathcal{P}(\mathbb{R})|$. Deduce that there is no surjection $\mathbb{R} \rightarrow \mathbb{R}^{\mathbb{R}}$.

Solution (Hint 1). Replace the base $\mathbb{R}$ by $\{0, 1\}^{\mathbb{N}}$, then curry.

Solution (Hint 2). You will need $|\mathbb{N} \times \mathbb{R}| = |\mathbb{R}|$.

Solution. Let $\beta: \mathbb{R} \rightarrow \{0, 1\}^{\mathbb{N}}$ be a bijection (Theorem 3.6.6). Then

$$\begin{aligned} |\mathbb{R}^{\mathbb{R}}| &= |(\{0, 1\}^{\mathbb{N}})^{\mathbb{R}}| = |\{0, 1\}^{\mathbb{N} \times \mathbb{R}}| \\ &= |\{0, 1\}^{\mathbb{R}}| = |\mathcal{P}(\mathbb{R})|, \end{aligned}$$

by Proposition 3.6.1 (c) with β and $\text{id}_{\mathbb{R}}$; then Theorem 3.6.3 (f) with $Y = \mathbb{N}$, $Z = \mathbb{R}$; then Exercise (B3: Sets the size of the line, used later) (a) with Proposition 3.6.1 (c), now in the exponent; then Theorem 3.6.4; chained by Proposition 2.5.1.

For the second part, let $\Theta: \mathbb{R}^{\mathbb{R}} \rightarrow \mathcal{P}(\mathbb{R})$ be a bijection. If $s: \mathbb{R} \rightarrow \mathbb{R}^{\mathbb{R}}$ were onto, then $\Theta \circ s: \mathbb{R} \rightarrow \mathcal{P}(\mathbb{R})$ would be onto (Theorem 1.5.4 (b)), against Theorem 3.3.2. Since $x \mapsto c_x$, where $c_x(t) := x$ for all t , is an injection $\mathbb{R} \rightarrow \mathbb{R}^{\mathbb{R}}$ (evaluate at 0), and a bijection would be a surjection, $|\mathbb{R}| < |\mathbb{R}^{\mathbb{R}}|$ (Definition 3.4.1): there are more functions $\mathbb{R} \rightarrow \mathbb{R}$ than real numbers.

Marking scheme. (10 points) - 2: replaces the base $\mathbb{R}$ by $\{0, 1\}^{\mathbb{N}}$, citing the bijection and Proposition 3.6.1 (c). - 3: applies currying in the right direction: $(X^Y)^Z$ with $Y = \mathbb{N}$, $Z = \mathbb{R}$, to reach $\{0, 1\}^{\mathbb{N} \times \mathbb{R}}$. - 2: uses $|\mathbb{N} \times \mathbb{R}| = |\mathbb{R}|$ together with respecting size in the exponent. - 1: passes from $\{0, 1\}^{\mathbb{R}}$ to $\mathcal{P}(\mathbb{R})$. - 2: rules out a surjection by composing with the bijection and citing Theorem 3.3.2. Any other complete route (for example graphs into $\mathcal{P}(\mathbb{R} \times \mathbb{R})$, an injection $\mathcal{P}(\mathbb{R}) \rightarrow \mathbb{R}^{\mathbb{R}}$ and Theorem 3.4.3) earns the 8 points of the first part, split between the two injections. Fatal errors (0 for the step): computing with symbols as if sizes were numbers (“ $\mathfrak{c}^{\mathfrak{c}} = 2^{\aleph_0 \mathfrak{c}}$ ”) with no bijection behind each step.

Exercise. C2: Find the error

Claim: $\{0, 1\}^{\mathbb{N}}$ is countable.

Proof. Send b to the natural number $N(b) := \sum_k b(k)2^k$. Different sequences have different binary digits, so N is injective, and an injection into $\mathbb{N}$ makes a set countable (Theorem 3.1.2).

Is the conclusion true? Where does the argument fail? What does it prove?

Solution. The conclusion is false: $\{0, 1\}^{\mathbb{N}}$ is uncountable (Theorem 3.3.1).

The error is in the first line. $N(b)$ is named before it is shown to exist: (N14) of Logic and Proof, Example (What is not allowed). The sum is infinite whenever b has infinitely many 1s, and Section 2.3 defines only finite sums (Definition 2.3.1); no natural number is “ $1 + 2 + 4 + \dots$ ”. The all-1 sequence is a witness: it has no value under N .

What survives. On the sequences that are eventually 0, the sum is finite ($\sum_{k < K} b(k)2^k$ for any K past the last 1), and N is defined there. It is injective once the uniqueness of binary digits is proved, which Exercise R1 below does not do (R1 gives existence only). The countability of that set follows anyway, with no binary digits: changing the codomain from $\{0, 1\}$ to $\mathbb{N}$ injects it into the set of eventually zero functions $\mathbb{N} \rightarrow \mathbb{N}$ of Exercise (R4), at the end of this section, which is countable; compose with an injection of that set into $\mathbb{N}$ (Theorem 3.1.2, Theorem 1.5.4 (a)).

Marking scheme. (10 points) - 2: says the conclusion is false, citing Theorem 3.3.1. - 3: names the failing step, an infinite sum named as a natural number, with (N14). - 2: gives a witness, such as the all-1 sequence. - 2: says what the argument does prove: the eventually zero sequences form a countable set. - 1: flags that the injectivity of N on them needs the uniqueness of binary digits, which is not proved. Fatal errors (0 for the step): calling the conclusion true; locating the error in “an injection into $\mathbb{N}$ makes a set countable”, which is correct.

Exercise. C3: Rearrangements of $\mathbb{N}$

Let B be the set of bijections $\mathbb{N} \rightarrow \mathbb{N}$. Exercise C2 of Section 3.3 showed that B is uncountable. Prove that it has exactly the size of $\mathbb{R}$: $|B| = |\mathbb{R}|$.

Solution. Up. Every bijection $\mathbb{N} \rightarrow \mathbb{N}$ is a function $\mathbb{N} \rightarrow \mathbb{N}$, so $B \subseteq \mathbb{N}^{\mathbb{N}}$, and the inclusion followed by a bijection $\mathbb{N}^{\mathbb{N}} \rightarrow \mathbb{R}$ (Theorem 3.6.8) is an injection $B \rightarrow \mathbb{R}$.

Down. For $b \in \{0, 1\}^{\mathbb{N}}$, let $\sigma_b: \mathbb{N} \rightarrow \mathbb{N}$ swap $2n$ and $2n + 1$ when $b(n) = 1$, and fix them when $b(n) = 0$; this is a function, since each $m \in \mathbb{N}$ is $2n$ or $2n + 1$ for exactly one n . It is its own inverse, so $\sigma_b \in B$ (Theorem 1.6.4). The map $b \mapsto \sigma_b$ is injective, since $b(n) = 1$ exactly when $\sigma_b(2n) = 2n + 1$. This is the construction of Exercise (C2: Permutations of the naturals).

Composing the *Up* injection with a bijection $\mathbb{R} \rightarrow \{0, 1\}^{\mathbb{N}}$ (Theorem 3.6.6) gives $|B| \leq |\{0, 1\}^{\mathbb{N}}|$ (Proposition 3.4.1 (b)); by Theorem 3.4.3, $|B| = |\{0, 1\}^{\mathbb{N}}|$, and this is $|\mathbb{R}|$ by Theorem 3.6.6.

Marking scheme. (10 points) - 3: shows $|B| \leq |\mathbb{R}|$, through $B \subseteq \mathbb{N}^{\mathbb{N}}$ and Theorem 3.6.8. - 3: defines σ_b and shows that it is a bijection of $\mathbb{N}$. - 2: shows that $b \mapsto \sigma_b$ is injective, by reading $b(n)$ off $\sigma_b(2n)$. - 2: concludes by Theorem 3.4.3 and Theorem 3.6.6. Fatal errors (0 for the step): concluding $|B| = |\mathbb{R}|$ from “ B is uncountable and $B \subseteq \mathbb{N}^{\mathbb{N}}$ ” alone, with no injection from a set the size of $\mathbb{R}$ into B .

3.6.10.4 R. Review

Exercise. R1

Prove that every integer $n \geq 1$ is a sum of distinct powers of 2: there are an integer $r \geq 1$ and natural numbers $k_1 > k_2 > \dots > k_r$ with $n = 2^{k_1} + 2^{k_2} + \dots + 2^{k_r}$.

Solution. We use Theorem 2.2.2 with $n_0 = 1$. Let $n \geq 1$, and suppose every integer m with $1 \leq m < n$ is such a sum.

The largest power of 2 not above n . The set $T := \{k \in \mathbb{N} : 2^k > n\}$ is non-empty, since $2^n \geq 1 + n > n$ by Theorem 2.3.7 with $x = 1$. By Theorem 2.1.3 it has a least element m (the method of Example (Method: the least element)). Since $2^0 = 1 \leq n$, $0 \notin T$, so $m \geq 1$, and $K := m - 1 \in \mathbb{N}$ (Lemma 2.1.1 (c)). As $K < m$, $K \notin T$; so

$$2^K \leq n < 2^{K+1}.$$

The step. Let $s := n - 2^K$, so $0 \leq s < 2^{K+1} - 2^K = 2^K$. If $s = 0$, then $n = 2^K$, a sum with $r = 1$. If $s \geq 1$, then $s < n$, because $2^K \geq 1$. By the hypothesis, $s = 2^{k_1} + \cdots + 2^{k_r}$ with $k_1 > \cdots > k_r$. Each $2^{k_i} \leq s < 2^K$, so $k_i < K$ (if $k_i \geq K$, then $2^{k_i} \geq 2^K$ by Proposition 2.3.4 (e)). Hence

$$n = 2^K + 2^{k_1} + \cdots + 2^{k_r}, \quad K > k_1 > \cdots > k_r,$$

a sum of distinct powers of 2. By Theorem 2.2.2, every $n \geq 1$ is such a sum. For example $13 = 2^3 + 2^2 + 2^0$.

The base 1 is the right one: 0 is not a sum of one or more powers of 2, since each power is positive.

Exercise. R2

Show that $\forall x \exists y R(x, y) \not\models \exists y \forall x R(x, y)$ by a counter-model whose domain is $\mathbb{N}$. Say in words what the two sentences say when $R(x, y)$ is read as “ $x < y$ ”.

Solution. Let $\mathfrak{M}$ have domain $\mathbb{N}$ and $R^{\mathfrak{M}} := \{(d, e) \in \mathbb{N} \times \mathbb{N} : d < e\}$. Both formulas are sentences, so no assignment matters.

The premise is true. $\forall x \exists y (x < y)$ says “every natural number has a larger one”. For each $d \in \mathbb{N}$, $e := d + 1 \in \mathbb{N}$ has $d < e$.

The conclusion is false. $\exists y \forall x (x < y)$ says “some natural number is larger than every natural number”. For any $e \in \mathbb{N}$, the choice $d := e$ gives $d < e$ false, so no e works.

So $\mathfrak{M}$ is a counter-model, and $\forall x \exists y R(x, y) \not\models \exists y \forall x R(x, y)$. By the soundness statement of *Logic and Proof*, Section 7.2 (the subsection “From counter-models to non-derivability”), a counter-model shows non-derivability: $\forall x \exists y R(x, y) \not\models \exists y \forall x R(x, y)$.

This is the converse of Logic and Proof, Proposition 5.6.2 with the variables renamed and the two places of R exchanged (read $R(x, y)$ as $R(y, x)$), and the counter-model is the one of Logic and Proof, Example (The swap of $\exists$ and $\forall$): there the domain was $\mathbb{Z}$ and R was read as $>$; with the roles of the variables exchanged, R read as $<$ and the domain cut down to $\mathbb{N}$, the same witnesses work, as checked above. In the premise the larger number y is chosen after x and depends on it; the conclusion asks for one y in advance.

Exercise. R3

For an integer $n \geq 1$, how many truth functions with n inputs are there? Prove your answer.

Solution. There are 2^{2^n} . A truth function with n inputs (Logic and Proof, Definition 4.4.4) assigns a truth value to each row $(a_1, \dots, a_n)$; read a row as the function $i \mapsto a_i$ on $\{1, \dots, n\}$, and let L be the set of rows.

There are 2^n rows. The map sending a row to $\{i \in \{1, \dots, n\} : a_i = \text{T}\}$ is a bijection $L \rightarrow \mathcal{P}(\{1, \dots, n\})$ (injective and surjective by Example (Method: proving injectivity) and Example (Method: proving surjectivity)): a row is determined by the places where it is T, and every set of places arises: given $A \subseteq \{1, \dots, n\}$, the row with $a_i = \text{T}$ for $i \in A$ and $a_i = \text{F}$ otherwise maps to A , and two rows with the same T-places agree at every i , since each a_i is T or F. Since $\{1, \dots, n\}$ has n elements, Proposition 2.5.8 gives 2^n subsets, so L has 2^n elements (compose the bijections).

There are 2^{2^n} truth functions. In the same way, a truth function f is determined by the set $\{\rho \in L : f(\rho) = \text{T}\} \subseteq L$, and every subset of L arises (the same two checks, with $f \mapsto \{\rho : f(\rho) = \text{T}\}$ in place of the row map); so the truth functions are in bijection with $\mathcal{P}(L)$, which has 2^{2^n} elements by Proposition 2.5.8 again. For $n = 1, 2, 3$ this gives 4, 16, 256.

Exercise. R4

A function $f: \mathbb{N} \rightarrow \mathbb{N}$ is **eventually zero** if there is $N \in \mathbb{N}$ with $f(n) = 0$ for every $n \geq N$. Is the set of eventually zero functions countable?

Solution. Yes. The tool is a **countable union of countable sets**. For $N \in \mathbb{N}$ let Z_N be the set of $f: \mathbb{N} \rightarrow \mathbb{N}$ with $f(n) = 0$ for every $n \geq N$; the set of eventually zero functions is $Z := \bigcup_{N \in \mathbb{N}} Z_N$. Each Z_N is countable:

- Z_0 has one element, the zero function, so it is countable.
- For $N = 1$, $f \mapsto f(0)$ is a bijection $Z_1 \rightarrow \mathbb{N}$: a function in Z_1 is determined by its value at 0, and every value occurs.
- For $N \geq 2$, $f \mapsto (f(0), \dots, f(N-1))$ is a bijection $Z_N \rightarrow \mathbb{N} \times \dots \times \mathbb{N}$ (N factors), by the same reasoning and the characteristic property of tuples; the product is countable by Corollary 3.1.7, and so is Z_N (compose a surjection $\mathbb{N} \rightarrow \mathbb{N} \times \dots \times \mathbb{N}$ with the inverse bijection, Proposition 3.1.4).

By Theorem 3.2.3, Z is countable. (That theorem uses Axiom 3.2.1; here it could be avoided, since each Z_N comes with an explicit listing, but the question did not ask for that.)

Why the look-alike fails. A diagonal argument, as in Theorem 3.3.1, builds from a list $f_0, f_1, \dots$ of eventually zero functions the function $g(n) := f_n(n) + 1$. It differs from every f_n , but $g(n) \geq 1$ for every n , so g is **not** eventually zero: it is not in Z , and nothing is contradicted. A diagonal argument proves uncountability only when the diagonal object stays inside the set; this is the usual failure named in Example (Method: the diagonal).