Primer on Cardinalities

Jonathan L.F. King
University of Florida, Gainesville FL 32611-2082, USA
squash@ufl.edu
Webpage http://squash.1gainesville.com/teaching.html

4 October, 2021 (at *00:02*)

1a: *Defn: Exponentiation.* Given sets D and C, logicians define the symbol C^D as

$$C^D := \Big\{\text{The set of } \underline{all} \text{ fncs from } D{\to}C\Big\}.$$

These functions have **Domain** D and **Co-domain** C. Note well that C^D is a *set* of *functions*. For example, let $\Omega := \{\alpha,\beta,\gamma\}$ and $B := \{0,1\}$. Then B^Ω comprises the $2^3 = 8$ many fncs

$$\begin{array}{ll} \alpha,\beta,\gamma \mapsto 0,0,0; & \alpha,\beta,\gamma \mapsto 1,0,0; \\ \alpha,\beta,\gamma \mapsto 0,0,1; & \alpha,\beta,\gamma \mapsto 1,0,1; \\ \alpha,\beta,\gamma \mapsto 0,1,0; & \alpha,\beta,\gamma \mapsto 1,1,0; \\ \alpha,\beta,\gamma \mapsto 0,1,1; & \alpha,\beta,\gamma \mapsto 1,1,1. \end{array}$$

In contrast, Ω^B comprises these $3^2 = 9$ fncs:

$$\begin{array}{lll} 0,1 \mapsto \alpha,\alpha; & 0,1 \mapsto \beta,\alpha; & 0,1 \mapsto \gamma,\alpha; \\ 0,1 \mapsto \alpha,\beta; & 0,1 \mapsto \beta,\beta; & 0,1 \mapsto \gamma,\beta; \\ 0,1 \mapsto \alpha,\gamma; & 0,1 \mapsto \beta,\gamma; & 0,1 \mapsto \gamma,\gamma. \end{array}$$

Note, for finite sets P and Q, that $|P^Q| = |P|^{|Q|}$. It is for that reason that logicians use this Set^{Set} notation. [**N.B:** Consider sets $A \asymp B$ with $A \neq B$. Although sets A^B and B^A have the same *cardinality*, they are <u>*not*</u> the same set; this, since the fncs in A^B have B as their domain, whereas those in B^A have A as their domain, yet $B \neq A$.] □

1b: *Defn: Powerset.* The ***powerset*** of a set Ω, written $\mathcal{P}(\Omega)$, is the set of <u>*all*</u> subsets of Ω. *Why do logicians sometimes write* $\{0,1\}^\Omega$ *to mean* $\mathcal{P}(\Omega)$?

Well, there is a natural bijection between the two: A function $f{:}\Omega{\to}\{0,1\}$ yields a subset $S_f \subset \Omega$ by $S_f := \{x \in \Omega \mid f(x) = 1\}$. Easily, the map $f \mapsto S_f$ is a bijection from $\{0,1\}^\Omega$ onto $\mathcal{P}(\Omega)$.

Logicians often write the powerset as $\mathbf{2}^\Omega$, rather than $\{0,1\}^\Omega$, since all that was important about the base set $\{0,1\}$ was that it had 2 elements; it was not important what those elements were. □

ENTRANCE. Two sets A and B are ***equinumerous***, or "***bijective*** with each other", if *there exists* a bijection $A{\hookrightarrow\!\!\!\!\to}B$. [BTWay, we use a hook-arrow to indicate an injection, e.g, $A{\hookrightarrow}B$, and a doublehead-arrow, e.g $A{\twoheadrightarrow}B$ to indicate a surjection. Hence $\hookrightarrow\!\!\!\!\to$ indicates a bijection.] Write the equinumerous relation as

$$A \asymp B.$$

Write $A \preccurlyeq B$ if *there exists* an injection $A{\hookrightarrow}B$. Finally, let $A \prec B$ mean that $A \preccurlyeq B$ yet $A \not\asymp B$.

Easily, $\asymp$ is an equivalence relation. [On the class of cardinalities, relation $\preccurlyeq$ is a pre-order. Is $\preccurlyeq$ a *partial-order*? Is $\preccurlyeq$ a *total-order*?]

Call S ***countably-infinite*** or ***denumerable*** if $S \asymp \mathbb{N}$. A set S is ***countable*** if $S \preccurlyeq \mathbb{N}$, i.e, S is bijective with some subset of $\mathbb{N}$. [So a countable set is either *finite* or *countably-infinite*.] □

2a: Lemma. *Suppose sets* $P \asymp \widetilde{P}$ *and* $Q \asymp \widetilde{Q}$. *Then* $P^Q \asymp \widetilde{P}^{\widetilde{Q}}$. *Proof.* Exercise 1 *Who can post?*

2b: Card-Exponentiation Lemma (CE-Lemma). *Consider any three sets* Ω, B *and* C. *Then* $\Omega^{B\times C} \asymp [\Omega^B]^C$.
Proof. Exercise 2 *Posting Race!*

3: Countable-card Theorem. *Below,* S *represents an arbitrary* <u>*non-void*</u> *countable set.*

a: *An arbitrary subset of a countable set is countable. In particular, an arbitrary infinite subset of a countable set is countably-infinite.*

b: *Each of these is countably-infinite:*
$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{N}{\times}\mathbb{N}$, $S{\times}\mathbb{N}$.

c: *A union of countably many countable sets is countable.* ◊

4a: *Defn.* In referring to intervals, let ***LCRO*** mean "Left-Closed Right-Open" and let ***LORC*** mean "Left-Open Right-Closed".

Use $\overline{\mathbb{R}} := [-\infty, +\infty] := \{-\infty\} \cup \mathbb{R} \cup \{\infty\}$ to denote the ***extended reals***. In $\overline{\mathbb{R}}$, as an example, the set $[-\infty, 5)$ is a LCRO-interval, and $(7, \infty]$ is a LORC-interval. Both $[-4, \infty]$ and $\overline{\mathbb{R}}$ itself are closed intervals. All of these examples are *unbounded* intervals, whereas $(-4, 7]$ is a bounded interval.

In the theorem below, the word "*interval*" means "*non-trivial interval*". That is, we exclude 1-point closed intervals, e.g $[7,7] \stackrel{\text{note}}{=} \{7\}$, as well as the empty interval, e.g $(7,7) \stackrel{\text{note}}{=} (7,7] \stackrel{\text{note}}{=} [7,7)$, each of which is the emptyset. [BTWay, the emptyset is open.] □

4b: Interval-card Theorem. *Each non-trivial subinterval of $\overline{\mathbb{R}}$ is equi-numerous with $\mathbb{R}$.* ◇

Proof. For $k = 1,2$, consider intervals $J_k := [a_k, b_k]$, with positive (finite) lengths $L_k := b_k - a_k$. Then the affine map

$$x \mapsto a_2 + \tfrac{L_2}{L_1} \cdot [x - a_1]$$

bijects J_1 onto J_2. The same map works for two open intervals, two LCRO-intervals, or two LORC-intervals.

Let $\mathcal{H} := \{\frac{1}{n}\}_{n=1}^{\infty}$ comprise the harmonic numbers. Define $f : [0,1] \to [0,1)$ as follows.[♡1]

4c:
$$\begin{aligned} &\textit{For } x \in \mathcal{H}\textit{: Let } n := \tfrac{1}{x}\textit{, then map } x \mapsto \tfrac{1}{n+1}. \\ &\textit{For } x \notin \mathcal{H}\textit{:} \qquad\qquad \textit{Map } x \mapsto x. \end{aligned}$$

This f is a bijection. And $g(x) := 1 - x$ bijects $[0,1)$ onto $(0,1]$. Defining $h : (0,1] \to (0,1)$ by rule (4c) also gives a bijection. Hence

$$[0,1] \xrightarrow{f} [0,1) \xrightarrow{g} (0,1] \xrightarrow{h} (0,1)\,. \quad \textit{Thus:}$$

All bounded intervals have the same cardinality.

Unbounded intervals. Extending tan() to $\overline{\mathbb{R}}$, note that tan bijects $J := [-\frac{\pi}{2}, \frac{\pi}{2}]$ onto the closed interval $\overline{\mathbb{R}}$. Consequently, every (bounded or unbounded) closed/open/LORO/LCRO sub-interval of $\overline{\mathbb{R}}$ is carried by arctan to a corresponding subinterval of J. Since these latter intervals are all bounded intervals, our earlier argument shows that they are all bijective with each other.[♡2] ♦

5: Cantor's diagonalization thm.

i: *Firstly, $\mathbb{N} \prec \mathbb{R}$. Moreover, for each function $f : \mathbb{N} \to \mathbb{R}$ there is an explicit construction of a point $\mathcal{NewPt}_f \in \mathbb{R}$ which is __not__ in* $\operatorname{Range}(f)$.

ii: *Every set S satisfies that $S \prec \mathcal{P}(S)$. Moreover, for each fnc $f : S \to \mathcal{P}(S)$, this set,*

$$\mathcal{NewSet}_f \quad := \quad \{z \in S \mid f(z) \not\ni z\}$$

is __not__ in $\operatorname{Range}(f)$. ◇

Proof of (i). Map $x \mapsto x$ injects $\mathbb{N}$ into $\mathbb{R}$, so $\mathbb{N} \preccurlyeq \mathbb{R}$.

Recall $\mathbb{N} \asymp \mathbb{Z}_+$ and $\mathbb{R} \asymp (0,1)$. Given $g : \mathbb{Z}_+ \to (0,1)$ we build $\mathcal{NewPt}_g \in (0,1)$ with $\mathcal{NewPt}_g \notin \operatorname{Range}(g)$, as follows. For $x \in (0,1)$, define digits $\mathbf{d}_n^x$ so that

$$\sum_{n=1}^{\infty} \frac{\mathbf{d}_n^x}{10^n} \quad = \quad x\,.$$

Moreover, when x is a 10-adic rational, use the expansion which is eventually '9'. [Any fixed rule will work.]

If we write the decimal expansions of $g(1), g(2), \ldots$ in a two-dimensional table, then digits $\delta_n := \mathbf{d}_n^{g(n)}$ lie along the diagonal, whence the name of the proof.

For a digit d, let

$$\overline{d} \;:=\; \left\{ \begin{matrix} 3 & \text{, if } d \neq 3; \\ 7 & \text{, otherwise.} \end{matrix} \right\}.$$

Finally, define digit $\alpha_n := \overline{\delta_n}$. Then point

$$\mathcal{NewPt}_g \;:=\; \sum_{n=1}^{\infty} \frac{\alpha_n}{10^n}$$

lies in $(0,1)$ and [Exercise 3] is **not** in $\operatorname{Range}(g)$. ♦

Proof of (ii). Injection $x \mapsto \{x\}$ shows that $S \preccurlyeq \mathcal{P}(S)$.

To see that $S \not\asymp \mathcal{P}(S)$, note: *For each $z \in S$, the symmetric-difference $\mathcal{NewSet}_f \triangle f(z)$ owns z; hence $\mathcal{NewSet}_f$ differs from $f(z)$.* ♦

[♡1] This (4c) uses one of our "*Cantor's–Hotel maps*" from class.

[♡2] BTWay, fnc $x \mapsto \mathrm{e}^x$ bijects $\mathbb{R} \hookrightarrow\!\!\!\!\rightarrow \mathbb{R}_+$, and $x \mapsto \mathrm{e}^x / [\mathrm{e}^x + 1]$ maps $\mathbb{R} \hookrightarrow\!\!\!\!\rightarrow (0,1)$. Indeed, each an order-preserving homeomorphism. The latter fnc is the sigmoid function.

Schröder-Bernstein

Here, we examine cardinality relations between two sets, $\mathbf{X}$ and $\mathbf{\Omega}$. The below arguments do not require these sets be disjoint, but the idea is easier understand when they are. At no cost, we can arrange that $\mathbf{X}$ be disjoint from $\mathbf{\Omega}$ by replacing $\mathbf{X}$ by $\mathbf{X}\times\{1\}$, and replacing $\mathbf{\Omega}$ by $\mathbf{\Omega}\times\{2\}$.

6.1: *Consider a map $g\colon\mathbf{X}\to\mathbf{\Omega}$, an injection $h\colon\mathbf{\Omega}\hookrightarrow\mathbf{X}$, and a subset $B \subset h(\mathbf{\Omega}) \overset{note}{\subset} \mathbf{X}$. These determine a function $\theta\colon\mathbf{X}\to\mathbf{\Omega}$ by setting $F := \mathbf{X} \smallsetminus B$, and defining*

$$\theta\lfloor_B := h^{-1}\lfloor_B, \quad \text{and} \quad \theta\lfloor_F := g\lfloor_F\,.$$

Let $[\![g, h\colon B]\!]$ denote this function θ.

[So we map Forward on F, and Backward on B.]

Given g, h and B as above, with g an *injection*, say that "*the set B is **(g,h)-backward-good***" if the resulting function $\theta\colon\mathbf{X}\to\mathbf{\Omega}$ of (6.1) is a *bijection*, and call θ an "**(g,h)-good bijection**". The corresponding forward set $F := \mathbf{X} \smallsetminus B$ is **(g,h)*-forward-good***.

6.2: Weak Schröder-Bernstein thm. *For sets $\mathbf{X}$ and $\mathbf{\Omega}$: If $\mathbf{X} \preccurlyeq \mathbf{\Omega}$ and $\mathbf{X} \succcurlyeq \mathbf{\Omega}$, then $\mathbf{X} \asymp \mathbf{\Omega}$.* ♢

6.3: Schröder-Bernstein Thm [S-B thm]. *Fix injections*

$$\mathbf{X} \overset{g}{\hookrightarrow} \mathbf{\Omega} \quad \text{and} \quad \mathbf{X} \overset{h}{\hookleftarrow} \mathbf{\Omega}\,.$$

Then there exists an (g,h)-good bijection.

Indeed, defining the collection of points in each set with no pre-image in the other set,

$$\widehat{X} \;:=\; \mathbf{X} \smallsetminus h(\mathbf{\Omega}) \quad \text{and} \quad \widehat{\Omega} \;:=\; \mathbf{\Omega} \smallsetminus g(\mathbf{X})\,,$$

we have this: The Smallest and Largest, in the sense of inclusion, (g,h)-backward-good sets are

6.4: $$\mathcal{S}_{\langle g,h\rangle} \;:=\; \bigcup_{n=0}^{\infty} [h\circ g]^{\circ n}(h(\widehat{\Omega})) \quad \text{and}$$

6.5: $$\mathcal{L}_{\langle g,h\rangle} \;:=\; \mathbf{X} \smallsetminus \Big[\bigcup_{n=0}^{\infty} [h\circ g]^{\circ n}(\widehat{X})\Big]\,,$$

resp.. In particular, $\mathcal{S}_{\langle g,h\rangle} \subset \mathcal{L}_{\langle g,h\rangle} \subset \mathrm{Range}(h)$. ♢

Proof. Use the 4-orbit picture from class. ♦

Bits

Define half-open and open intervals in the reals,

$$L := [0,1) \quad\text{and}\quad R := (0,1] \quad\text{and}\quad J := (0,1)\,.$$

Recall that each dyadic rational has two binary numerals; the remaining reals each have one binary numeral. Define the all-zero and all-one names

$$\bar{\mathbf{0}} := 000\cdots\,, \quad\text{and}\quad \bar{\mathbf{1}} := 111\cdots\,,$$

Let Ec be the set of eventually constant-1 or eventually constant-0 names.

Below, I'll use ***"word"*** for a *finite* string bits, e.g "10010". I'll use ***"name"*** for a (one-sided) *infinite* string, e.g 10111100100100100100... (e.g, start with "10111" then repeat the pattern "100" forever.)

Let $\textsc{Bits} := 2^{\mathbb{Z}_+}$ be the set of bit-sequences

$$\vec{\mathbf{b}} = b_1 b_2 b_3 \ldots, \quad \textit{with each } b_j \in \{0,1\}.$$

So $\textsc{Bits} \asymp \mathcal{P}(\text{denumerable})$.

7a: *Defn.* Define a fnc $\text{BinOne}\colon (0,1) \to \textsc{Bits}$ that produces the binary numeral of a point. Specifically, $\text{BinOne}(x)$ is the unique bit-sequence $\vec{\mathbf{b}}$ such that

$$\sum_{n=1}^{\infty} \frac{b_n}{2^n} = x\,,$$

and: *If x is a dyadic rational, then $\vec{\mathbf{b}}$ is eventually constant 1.* [E.g $\text{BinOne}(3/4) = 10111\cdots = 10\bar{\mathbf{1}}$.]

Define $\text{BinDTer}\colon \textsc{Bits} \to [0,1]$ [*Binary to Doubled-Ternary*] by

$$\text{BinDTer}(\vec{\mathbf{b}}) := \sum_{n=1}^{\infty} \frac{2b_n}{3^n}\,.$$

So $\text{BinDTer}(10\bar{\mathbf{1}})$ is the number whose base-3 numeral is $.2022\cdots$, is $\frac{2}{3} + \frac{1}{9} = \frac{7}{9}$. The range of BinDTer is the famous "middle thirds" ***Cantor set***.

Exercise-4: *Both* BinOne *and* BinDTer *are injections.* □

7b: S-B corollary. *It is the case that* $\mathbb{R} \asymp \mathcal{P}(\mathbb{N})$. ◊

Proof. Inject $\mathbb{R} \hookrightarrow \textsc{Bits}$ by

$$\mathbb{R} \asymp (0,1) \overset{\text{BinOne}}{\hookrightarrow} \textsc{Bits}\,.$$

In the other direction,

$$\textsc{Bits} \overset{\text{BinDTer}}{\hookrightarrow} [0,1] \hookrightarrow \mathbb{R}\,,$$

injecting $\textsc{Bits} \hookrightarrow \mathbb{R}$. Now apply Schröder-Bernstein. ♦

Explicit bijection $\psi\colon \textsc{Bits} \hookrightarrow\!\!\!\!\rightarrow (0,1]$

In half-open $(0,1]$, let Dy be this sequence of dyadics:

$$\textsc{Dy} = \left(\tfrac{1}{1}, \tfrac{1}{2}, \tfrac{1}{4}, \tfrac{3}{4}, \tfrac{1}{8}, \tfrac{3}{8}, \tfrac{5}{8}, \tfrac{7}{8}, \tfrac{1}{16}, \tfrac{3}{16}, \tfrac{5}{16}, \tfrac{7}{16}, \ldots \tfrac{15}{16}, \tfrac{1}{32}, \tfrac{3}{32}, \ldots \tfrac{31}{32}, \ldots\right).$$

Define

$$\psi(\vec{\mathbf{a}}) := \begin{cases} \mu(\vec{\mathbf{a}}) & , \text{ if } \vec{\mathbf{a}} \in \textsc{Ec}\,; \\ \sum_{n=1}^{\infty} \frac{a_n}{2^n} & , \text{ Otherwise} \end{cases}$$

where map $\mu\colon \textsc{Ec} \hookrightarrow\!\!\!\!\rightarrow \textsc{Dy}$ is:

Eventually constant $\vec{\mathbf{a}}$	$\longmapsto$	*Dyadic number* $\mu(\vec{\mathbf{a}})$
$\bar{\mathbf{1}}$		1/1
$\bar{\mathbf{0}}$		1/2
$0\bar{\mathbf{1}}$		1/4
$1\bar{\mathbf{0}}$		3/4
$00\bar{\mathbf{1}}$		1/8
$01\bar{\mathbf{0}}$		3/8
$10\bar{\mathbf{1}}$		5/8
$11\bar{\mathbf{0}}$		7/8
$000\bar{\mathbf{1}}$		1/16
$001\bar{\mathbf{0}}$		3/16
$010\bar{\mathbf{1}}$		5/16
$011\bar{\mathbf{0}}$		7/16
$100\bar{\mathbf{1}}$		9/16
$101\bar{\mathbf{0}}$		11/16
$110\bar{\mathbf{1}}$		13/16
$111\bar{\mathbf{0}}$		15/16
$0000\bar{\mathbf{1}}$		1/32
$0001\bar{\mathbf{0}}$		3/32
$0010\bar{\mathbf{1}}$		5/32
$0011\bar{\mathbf{0}}$		7/32
⋮		⋮
$1111\bar{\mathbf{0}}$		31/32
$00000\bar{\mathbf{1}}$		1/64
$00001\bar{\mathbf{1}}$		3/64
$00010\bar{\mathbf{1}}$		5/64
⋮		⋮
$11110\bar{\mathbf{0}}$		61/64
$11111\bar{\mathbf{0}}$		63/64
$000000\bar{\mathbf{1}}$		1/128
$000001\bar{\mathbf{1}}$		3/128
⋮		⋮

8: Power-of-reals Thm.

a: *The plane is equi-numerous with the line.*

b: *For each posint k, we have that $\mathbb{R}^k \asymp \mathbb{R}$.*

c: *Cartesian-power $\mathbb{R}^{\mathbb{N}}$ is equi-numerous with $\mathbb{R}$.* ◊

Pf of (a). Map $\text{BITS}\times\text{BITS} \overset{\mathcal{W}}{\hookrightarrow\!\!\!\!\rightarrow} \text{BITS}$ by interweaving the bits, as follows.

$$\mathcal{W}(\vec{\mathbf{a}}, \vec{\mathbf{c}}) \;:=\; a_1\, c_1\, a_2\, c_2\, a_3\, c_3\, a_4\, c_4\, \ldots$$

Pick your favorite bijection $\mathcal{B}{:}\,\mathbb{R} \hookrightarrow\!\!\!\!\rightarrow \text{BITS}$. Then

$$f(x,y) \;:=\; \mathcal{B}^{-1}\Big(\mathcal{W}(\mathcal{B}(x),\, \mathcal{B}(y))\Big)$$

bijects the plane $\mathbb{R}\times\mathbb{R}$ to the line $\mathbb{R}$. ♦

Pf of (b,c). [Note (a) is the $k{=}2$ case of (b).] To prove that $\text{BITS}^k \asymp \text{BITS}$, we can interleave k bit-seqs.

Alternatively, producing an injection

$$\varphi{:}\,\text{BITS}^{\mathbb{N}} \hookrightarrow \text{BITS}$$

establishes (a,b,c) in one swell foop. [Trivially $\text{BITS} \hookrightarrow \text{BITS}^{\mathbb{N}}$, so S-B thm says $\text{BITS}^k \asymp \text{BITS}^{\mathbb{N}} \asymp \text{BITS}$.] We make our φ an actual bijection, as follows: Notice that $\text{BITS}^{\mathbb{N}}$ can be viewed as a sequence of bit-seqs; i.e, it is a bit-quadrant, ie, a bit at each point of $\mathbb{N}\times\mathbb{N}$. Pick your favorite bijection showing $\mathbb{N}\times\mathbb{N} \asymp \mathbb{N}$, e.g, diagonal raster-scan. Then

$$\text{BITS}^{\mathbb{N}} \;=\; 2^{\mathbb{N}\times\mathbb{N}} \;\overset{\text{by (2a)}}{\asymp}\; 2^{\mathbb{N}} \;=\; \text{BITS}\,. \qquad ♦$$

9: Continuous-fncs Thm.

i: *Firstly,* $\mathbb{R}^{\mathbb{R}} \asymp 2^{\mathbb{R}} \overset{note}{\asymp} \left\{\begin{matrix}\textit{Functions only taking}\\ \textit{on values 5 and 7.}\end{matrix}\right\}$.

ii: *Also,* $\mathbf{C}(\mathbb{R}{\to}\mathbb{R}) \asymp \mathbb{R} \overset{note}{\asymp} \{\textit{Constant fncs}\}$. ◊

Challenging: *Exercise 5.* (?)

Algebraic numbers

A complex number γ is ***algebraic*** if it is a root of some non-zip intpoly [equiv., ratpoly] f. Thus

$$\boldsymbol{\alpha} := \sqrt[5]{19} \quad \text{and} \quad \boldsymbol{\beta} := [1-\sqrt{13}]/6$$

are algebraic numbers, since $\boldsymbol{\alpha}$ is a root of $x^5 - 19$, and $\boldsymbol{\beta}$ is a root of $3x^2 - x - 1$. Evidently each rational number P/Q is algebraic, since it is a root of intpoly $Qx - P$.

Each algebraic number γ has an associated posint called its ***degree***, written $\text{Deg}(\gamma)$. Writing $\mathbf{d} := \text{Deg}(\gamma)$, then γ is a root of some degree-$\mathbf{d}$ intpoly, but is the root of *no lower-degree* [non-zip] intpoly.

The rationals are precisely those numbers of degree 1. The above $\boldsymbol{\alpha}$ has $\text{Deg}(\boldsymbol{\alpha}) \le 5$. The above $\boldsymbol{\beta}$ has $\text{Deg}(\boldsymbol{\beta}) = 2$, since $\sqrt{13}$ is irrational.

Use $\mathbb{A}$ for the <u>*set*</u> of algebraic numbers in $\mathbb{C}$. We see that $\mathbb{A}$ is stratified into a *hierarchy* by degree. The numbers in the complement, $\mathbb{C} \smallsetminus \mathbb{A}$, *transcend* this hierarchy so –not surprisingly– each such number is said to be ***transcendental***. Although this is not obvious, each of these three numbers

$$\boldsymbol{\pi}, \qquad \mathsf{e}, \qquad \tau := \sum_{n=1}^{\infty} \frac{1}{b_n}, \text{ where } b_n := 2^{n!},$$

is transcendental.[♡3]

We define the ***degree*** of a transcendental number to be ∞. That is to say, the degree of a number $\gamma \in \mathbb{C}$ is the *infimum* of numbers $d \in [1..\infty)$ such that γ is a zero of some degree-d intpoly.

[♡3] Such a τ is called a *Liouville number*. There is an explanation of Liouville numbers on my Teaching Page.

Defn. Algebraists use notation $\mathbb{Z}[x]$ for the set of $\mathbb{Z}$-coefficient polynomials written using variable "x". They use $\mathbb{Q}[x]$ for the set of rational-coeff polynomials. □

11: Lemma. *Sets $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$ are equi-numerous, and each is countably-infinite.* ♢

Pf. Certainly $\mathbb{Q}[x] \asymp \mathbb{Z}[x] \asymp \mathbb{N}[x]$, since $\mathbb{Q} \asymp \mathbb{Z} \asymp \mathbb{N}$.

Let p_k be the k^{th}-prime; so $p_0{=}2$, $p_1{=}3$, $p_2{=}5$, ... A $\mathbb{N}$-coefficient polynomial can be written uniquely as

$$\dagger\text{:} \qquad c_0 + c_1 x + c_2 x^2 + c_3 x^3 + \ldots,$$

where ∞-sequence $\vec{\mathbf{c}}$ is eventually-constant-zero. Mapping (†) to

$$\ddagger\text{:} \qquad \prod_{k=0}^{\infty} [p_k]^{c_k},$$

is well-defined [since $\vec{\mathbf{c}}$ is eventually-const-zero] and is an bijection $\mathbb{N}[x] \hookrightarrow\!\!\!\!\rightarrow \mathbb{Z}_+$. [E.g, Zip maps to $2^0 \cdot 3^0 \cdot 5^0 \cdots = 1$. And $3x^2 + x^4$ maps to $p_2^3 \cdot p_4^1 = 5^3 \cdot 11 = 1375$.] ♦

12: Algebraic-numbers Thm. *The set $\mathbb{A}$ of algebraic numbers is denumerable.* ♢

Pf. Each [non-zip] intpoly has only finitely-many roots. And Lemma (11) asserts only countably many intpolys. Thus $\mathbb{A}$ is a countable union of countable sets, hence is countable, courtesy (3), the Countable-card theorem. ♦

(*And now, the Appendices!* See next page.)

§A Schröder-Bernstein computation

S-B Challenge. Let's use Schröder-Bernstein to construct a bijection $\theta{:}\mathbb{Z}_+\to\mathbb{Q}_+$. [Since $\mathbb{Z}_+$ and $\mathbb{Q}_+$ are not disjoint, I'll use blue for $\mathbb{Z}_+$ and its elements, and use reddish colors for $\mathbb{Q}_+$ and *its* elements.] Define the Divides map $D{:}\mathbb{Z}_+\to\mathbb{Q}_+$ by

$$D(n) \;:=\; n/3\,.$$

Easily, D is well-defined, and is an injection.

Each positive rational can be uniquely written p/q, where $p\perp q$ are posints. Define $R{:}\mathbb{Q}_+\to\mathbb{Z}_+$ [it applies to Ratios] by

$$R(p/q) \;:=\; 2^{p-1}{\cdot}3^{q-1}\,.$$

[For example, $R(1/1) = 2^{1-1}{\cdot}3^{1-1} = 2^0 3^0 = 1$. And $R(7/3) = 2^{7-1}{\cdot}3^{3-1} = 576$.] This R is well-defined, and is injective because prime-factorization is *unique*.

Let $\theta{:}\mathbb{Z}_+\to\mathbb{Q}_+$ be the (D,R)-good bijection with the *smallest* backward set. [So θ uses R^{-1} *only* on those (D,R)-orbits that start in $\mathbb{Q}_+$.]

Compute $\theta(18)$. *Compute* $\theta(4)$. □

Want to think about it first? Good idea!
WARNING: *A soln is on the next page.*

Looking into the Past. When does an $n \in \mathbb{Z}_+$ have an R-preimage? Exactly when n factors as $2^{p-1}\cdot 3^{q-1}$ with posints p and q coprime to each other.

Backtracing 18. This gives

$$\begin{array}{cccl}
\mathbb{Z}_+ & & \mathbb{Q}_+ & \\ \hline
18 & \nwarrow & & \\
 & \nearrow & 2/3 & \big[\text{since } 18 = 2^{2-1}\cdot 3^{3-1}\big] \\
2 & \nwarrow & & \\
 & \nearrow & 2/1 & \big[\text{since } 2 = 2^{2-1}\cdot 3^{1-1}\big] \\
\boxed{6} & & &
\end{array}$$

This 6 has no R-preimage. For although 6 *is* a product of powers of 2 and 3, the exponents are *not* coprime: $6 = 2^{2-1}\cdot 3^{2-1}$, and 2 is not coprime to 2. Hence:

$$\dagger\text{:} \qquad \theta(18) \overset{\text{Fwd}}{\equiv} D(18) = 18/3 = 6/1.$$

Backtracing 4. We compute:

$$\begin{array}{cccl}
\mathbb{Z}_+ & & \mathbb{Q}_+ & \\ \hline
4 & \nwarrow & & \\
 & \nearrow & 3/1 & \big[\text{since } 4 = 2^{3-1}\cdot 3^{1-1}\big] \\
9 & \nwarrow & & \\
 & \nearrow & 1/3 & \big[\text{since } 9 = 2^{1-1}\cdot 3^{3-1}\big] \\
1 & \nwarrow & & \\
 & \nearrow & 1/1 & \big[\text{since } 1 = 2^{1-1}\cdot 3^{1-1}\big] \\
3 & \nwarrow & & \\
 & & \boxed{1/2} & \big[\text{since } 3 = 2^{1-1}\cdot 3^{2-1}\big].
\end{array}$$

Backtracing terminates with $\frac{1}{2}$, since $3\cdot\frac{1}{2}$ is not in $\mathbb{Z}_+$ i.e, $\frac{1}{2} \notin \text{Range}(D)$. Thus

$$\ddagger\text{:} \qquad \theta(4) \overset{\text{Bwd}}{\equiv} R^{-1}(4) = 3/1 = 3.$$ ♦

Forward tracing 6. As an example, let's follow the (D, R)-orbit of 6 a bit further:

$$\begin{array}{cccl}
\mathbb{Z}_+ & & \mathbb{Q}_+ & \\ \hline
\boxed{6} & \searrow & & \\
 & \swarrow & 2/1 & \\
2 & \searrow & & \\
 & \swarrow & 2/3 & \\
18 & \searrow & & \\
 & \swarrow & 6/1 & \\
32 & \searrow & & \big[\text{since } 32 = 2^{6-1}\cdot 3^{1-1}\big] \\
 & \swarrow & 32/3 & \\
19327352832 & \vdots & & \big[\text{since } 19327352832 = 2^{32-1}\cdot 3^{3-1}\big]
\end{array}$$

Discussion. *Whether the* S-B algorithm *is constructive depends one's definition of* "constructive". *How to constructively tell if an orbit has no beginning?*

§B Appendix: AC $\Longrightarrow$ WO

Orders

Below, ***order*** means *strict total-order*. For an order-symbol $<$, $\prec$, $\sqsubset$, use $\leq$, $\preccurlyeq$, $\sqsubseteq$, for the non-strict versions.

Fixing an order $<$ on set $\boldsymbol{X}$ and a $p \in \boldsymbol{X}$, let

$$\boldsymbol{X}^{<p} := \{x \in \boldsymbol{X} \mid x < p\},$$

and analogously for $\boldsymbol{X}^{\leq p}$. Subset $\mathrm{I} \subset \boldsymbol{X}$ is an "***initial segment*** of $\boldsymbol{X}$" if $[\forall s \in \mathrm{I}, \forall x \in \boldsymbol{X}\colon\ x < s \ \Rightarrow\ x \in \mathrm{I}]$. Every non-void init-seg is of form $\boldsymbol{X}^{<p}$ or $\boldsymbol{X}^{\leq p}$.

For orders $\langle \boldsymbol{X}, < \rangle$ and $\langle \boldsymbol{\Omega}, \prec \rangle$, an "***order-embedding***, f, *of* $\boldsymbol{X}$ *into* $\boldsymbol{\Omega}$", written $f\colon \boldsymbol{X} \overset{\text{emb}}{\hookrightarrow} \boldsymbol{\Omega}$, means

$$\forall a,b \in \boldsymbol{X}\colon\quad a < b \ \text{ IFF } \ \varphi(a) \prec \varphi(b).$$

[Another name is an "*<u>into</u>-isomorphism*".]

Write $f\colon \boldsymbol{X} \overset{\text{init}}{\hookrightarrow} \boldsymbol{\Omega}$ if $f\colon \boldsymbol{X} \overset{\text{emb}}{\hookrightarrow} \boldsymbol{\Omega}$ <u>*and*</u> $\mathrm{Range}(f)$ is an *initial-segment* of $\boldsymbol{\Omega}$.

14a: Prop'n. *For well-orders $\langle \boldsymbol{X}, < \rangle$ and $\langle \boldsymbol{\Omega}, \prec \rangle$, suppose $\varphi\colon \boldsymbol{X} \overset{\text{init}}{\hookrightarrow} \boldsymbol{\Omega}$ and $\lambda\colon \boldsymbol{X} \overset{\text{init}}{\hookrightarrow} \boldsymbol{\Omega}$. Then $\varphi = \lambda$.* $\diamondsuit$

Pf. Assuming $\varphi \neq \lambda$, let $\mathbf{t} \in \boldsymbol{X}$ be the *smallest* $\boldsymbol{X}$-value s.t, WLOG, $\lambda(\mathbf{t}) \succ \varphi(\mathbf{t}) =: \boldsymbol{\tau}$. For each $x < \mathbf{t}$, then, $\lambda(x) = \varphi(x) \prec \boldsymbol{\tau} \prec \lambda(\mathbf{t})$. Thus $\lambda()$ skips over $\boldsymbol{\tau}$, hence is not an init-seg map. ※

14b: Lemma. *Fix well-orders $\langle \boldsymbol{X}, < \rangle$ and $\langle \boldsymbol{\Omega}, \prec \rangle$. If they are order-isomorphic, then the isomorphism is unique.*

If not, then exactly one of them is ord-iso to a subset the other. Moreover, it admits an ord-iso to an initial-segment, and this $\overset{\text{init}}{\hookrightarrow}$ map is unique. $\diamondsuit$

Pf. Let $\mathcal{C}$ be the set of $p \in \boldsymbol{X}$ for which init-seg $\boldsymbol{X}^{\leq p}$ admits a map $f_p\colon \boldsymbol{X}^{\leq p} \overset{\text{init}}{\hookrightarrow} \boldsymbol{\Omega}$. For $s > p$, both in $\mathcal{C}$, our Prop'n (14a) implies that the restriction of f_s to $\boldsymbol{X}^{\leq p}$ equals f_p. Consequently, the union

$$\varphi := \bigcup_{p \in \mathcal{C}} f_p$$

is a well-defined map into $\boldsymbol{\Omega}$. Its domain is initial-segment

$$\mathrm{I} := \bigcup_{p \in \mathcal{C}} \boldsymbol{X}^{\leq p}.$$

This φ is an ord-iso, since each f_p is, and maps onto $\boldsymbol{\Omega}$-init-seg

$$\Lambda := \bigcup_{p \in \mathcal{C}} \mathrm{Range}(f_p).$$

Which direction? If I equals $\boldsymbol{X}$, then $\varphi\colon \boldsymbol{X} \overset{\text{init}}{\hookrightarrow} \boldsymbol{\Omega}$.

Otherwise, let $\mathbf{s} := \mathrm{Min}(\boldsymbol{X} \smallsetminus \mathrm{I})$. Could Λ fail to be all of $\boldsymbol{\Omega}$? *No!*, since otherwise we could extend φ by mapping $\mathbf{s}$ to $\mathrm{Min}(\boldsymbol{\Omega} \smallsetminus \Lambda)$. Hence $\varphi^{-1}\colon \boldsymbol{\Omega} \overset{\text{init}}{\hookrightarrow} \boldsymbol{X}$. ♦

14c: Corollary. *On the proper-class of Well-Order-types, relation $\overset{\text{init}}{\hookrightarrow}$ is a [lax, i.e, non-strict] well-order.* $\diamondsuit$

Well-ordering Axiom. The WOAxiom states that each set admits a well-order. □

15: WOA$\Rightarrow$AC thm. *Assuming WOAxiom, each collection $\mathcal{C}$ of non-void sets, admits a choice fnc.* $\diamondsuit$

Proof. Let $<$ be a well-order on $\mathbf{U} := \bigcup(\mathcal{C})$. This engenders choice-fnc $A \mapsto \mathrm{Min}^{<}(A)$, for each $A \in \mathcal{C}$. ♦

Zermelo's pf AC ⇒ Well-ordering Principle

In 1904, Ernst Zermelo proved the then-surprising result that AC implies WOAxiom.

16a: *Shy-function.* On a set $\boldsymbol{X}$, let $\mathfrak{M} := 2^{\boldsymbol{X}} \setminus \{\boldsymbol{X}\}$ be the collection of *proper* subsets. The Axiom-of-Choice gives the existance of a ***shy-fnc*** $\mathcal{Y}:\mathfrak{M}\to\boldsymbol{X}$ satisfying

$$\dagger: \qquad \forall S \in \mathfrak{M}: \quad \mathcal{Y}(S) \in \boldsymbol{X} \setminus S\,,$$

[The shY-fnc picks an $\boldsymbol{X}$-element $\mathcal{Y}(S)$ that *avoids* S.] A shy-fnc comes from AC applied to collection $\{\boldsymbol{X} \setminus S\}_{S\in\mathfrak{M}}$ of non-void sets.

$\boxed{\textit{Henceforth, there is a fixed a shy-fnc } \mathcal{Y} \textit{ on } \boldsymbol{X}.}$.

On a subset $S\subset\boldsymbol{X}$, a well-order $\prec$ is "*good on S*" [*or "pair $\langle S,\prec\rangle$ is good"*] if

$$\ddagger: \qquad \forall t \in S: \quad \mathcal{Y}(S^{\prec t}) = t\,. \qquad \square$$

16b: *Obs.* Fix a good $\langle S,\prec\rangle$. For each proper $\prec$-init-seg $\mathrm{I} \subsetneqq S$, let $\mathbf{t} := \mathrm{Min}^{\prec}(S \setminus \mathrm{I})$. Thus $\mathrm{I} = S^{\prec\mathbf{t}}$. Hence

$$£: \qquad \mathrm{Min}^{\prec}(S \setminus \mathrm{I}) = \mathcal{Y}(\mathrm{I})\,. \qquad \square$$

16c: Shy lemma. *For subsets $S,T \subset \boldsymbol{X}$, suppose pairs $\langle S,<\rangle$ and $\langle T,\prec\rangle$ are each good. Then either $S\subset T$ or $T\subset S$.*

When $S\subset T$, then S is a $\prec$-initial-segment. Further, $<$ equals $\prec\!\lfloor_S$; the $\prec$-order restricted to S.

[*IOWords, $\langle S,<\rangle \xrightarrow{init} \langle T,\prec\rangle$ via the identity-map.*] ♢

16d: *Prelim.* A subset $J \subset \boldsymbol{X}$ is ***mutual*** if $J \subset S \cap T$, together with

J is init-seg w.r.t $<$ and w.r.t $\prec$, and orders $<$ and $\prec$ agree on J. □

Pf. Let $\mathcal{C}$ comprise those $p\in S$ s.t $S^{\leq p}$ is *mutual*. Automatically, the union $\boxed{\mathrm{I} := \bigcup_{p\in\mathcal{C}} S^{\leq p}}$ is mutual. [We don't need this, but note $\mathcal{C} = \mathrm{I}$.]

Inclusion. If $\mathrm{I} \subsetneqq S \cap T$, then (£) gives

$$\mathrm{Min}^{<}(S \setminus \mathrm{I}) = \mathcal{Y}(\mathrm{I}) = \mathrm{Min}^{\prec}(T \setminus \mathrm{I}) \overset{\text{note}}{\in} S \cap T\,.$$

With $\mathbf{y} := \mathcal{Y}(\mathrm{I})$, then $S^{\leq\mathbf{y}} = \mathrm{I} \sqcup \{\mathbf{y}\} = T^{\preceq\mathbf{y}}$. Orders $<$ and $\prec$ agree on $\mathrm{I}\sqcup\{\mathbf{y}\}$, yielding ※ that $\mathbf{y}$ is in $\mathrm{I} \overset{\text{recall}}{=\!=} \bigcup_{p\in\mathcal{C}} S^{\leq p}$.

If $S = \mathrm{I}$, then $S \subset T$ is a $\prec$-init-segment on which orders $<$ and $\prec$ agree. And if $T = \mathrm{I}$, then $T \subset S$ is a $<$-init-segment on which orders $<$ and $\prec$ agree. ♦

Prelim and Caveat. Consider $\mathcal{C}$, a collection of $\langle S,\prec_S\rangle$ pairs with $\prec_S$ a partial-order on $S\subset\boldsymbol{X}$. This $\mathcal{C}$ is ***consistent*** if for each $\langle S,\prec_S\rangle$ and $\langle T,\prec_T\rangle$, partial-orders $\prec_S$ and $\prec_T$ agree on $S \cap T$. When, further, always either $S \subset T$ or $T \subset S$, then $\mathcal{C}$ is ***nested***.

Define relation

$$*: \qquad < := \bigcup_{\langle S,\prec_S\rangle\,\in\,\mathcal{C}} \prec_S \quad \textit{on set} \quad \mathbf{U} := \bigcup_{\langle S,\prec_S\rangle\,\in\,\mathcal{C}} S\,.$$

When $\mathcal{C}$ *consistent*, then $<$ is a partial-order [exercise]. If each $\prec_S$ is a *total*-order, and $\mathcal{C}$ is *nested*, then $<$ is a *total*-order [exercise].

If, in addition, each $\prec_S$ is a well-order, must $<$ be a WOrder? *No!* Let $S_n := [-n\,..\,\infty) \subset \mathbb{Z}$, for $n = 1, 2, \ldots$, with order $\prec_n$ being $<\!\lfloor_{S_n}$. The $(*)$-union gives relation $<$ on $\mathbf{U} = \mathbb{Z}$; not a well-order. □

17: Zermelo's W-O Thm. *If a set $\boldsymbol{X}$ admits a shy-fnc, then $\boldsymbol{X}$ admits a well-order.* ♢

Pf. Let $\mathcal{C}$ comprise all good pairs $\langle S,\prec_S\rangle$, where $S\subset\boldsymbol{X}$, and use $(*)$ to define relation $<$ on set $\mathbf{U}$. Our $\mathcal{C}$ is nested, courtesy the Shy lemma; hence $<$ is a total-order.

$<$ is a well-order. Fix a non-void subset $B\subset\mathbf{U}$.

For j=1,2, consider pairs $\langle S_j,\prec_j\rangle$ having intersection $B \cap S_j$ non-void. Let $\mathbf{s}_j$ be the $\prec_j$-min of $B \cap S_j$. By the Shy lemma, WLOG S_1 is a $\prec_2$-init-seg of S_2; thus $\mathbf{s}_2 = \mathbf{s}_1$. Hence $\mathbf{s}_1$ is $\mathrm{Min}^{<}(B \cap \mathbf{U})$.

Well-order $\langle\mathbf{U},<\rangle$ is good. Fix a $t \in \mathbf{U}$. There exists a good $\langle S,\prec\rangle$ with $t \in S$. The Shy lemma implies S is a $<$-init-seg. Thus $\mathbf{U}^{<t} = S^{\prec t} = t$.

U is everything. If $\mathbf{U} \subsetneq \boldsymbol{X}$, let $\mathbf{y} := \mathcal{Y}(\mathbf{U})$. Extend $\boldsymbol{<}$ to well-order $\lessdot$ on $\widehat{\mathbf{U}} := \mathbf{U} \sqcup \{\mathbf{y}\}$ by defining $u \lessdot \mathbf{y}$ for each $u \in \mathbf{U}$. Easily, $\langle \widehat{\mathbf{U}}, \lessdot \rangle$ is good, contradicting that $\mathcal{C}$ comprised *all* good pairs. ♦

Filename: `Problems/SetTheory/primer-cardinality.latex`
As of: *Monday 13Apr2020.* Typeset: *4Oct2021 at 00:02.*