Cardinal Arithmetic

Defining the Basic Operations

Since we do not need to keep track of order, cardinal arithmetic is rather easier
to define than ordinal arithmetic. We will define addition, multiplication, and
exponentiation simultaneously.

Definition card-arithmetic.1. When \(a\) and \(b\) are cardinals:
\[
\begin{align*}
  a \oplus b &= |a \uplus b| \\
  a \otimes b &= |a \times b| \\
  a^b &= |^b a|
\end{align*}
\]

where \(X^Y = \{f : f \text{ is a function } X \to Y\}\). (It is easy to show that \(X^Y\) exists
for any sets \(X\) and \(Y\); we leave this as an exercise.)

Problem card-arithmetic.1. Prove in \(Z\) that \(X^Y\) exists for any sets \(X\)
and \(Y\). Working in \(ZF\), compute \(\operatorname{rank}(X^Y)\) from \(\operatorname{rank}(X)\) and \(\operatorname{rank}(Y)\), in the
manner of ??.

It might help to explain this definition. Concerning addition: this uses
the notion of disjoint sum, \(\sqcup\), as defined in ??; and it is easy to see that this
definition gives the right verdict for finite cases. Concerning multiplication:
?? tells us that if \(A\) has \(n\) members and \(B\) has \(m\) members then \(A \times B\) has
\(n \cdot m\) members, so our definition simply generalises the idea to transfinite mul-
tiplication. Exponentiation is similar: we are simply generalising the thought
from the finite to the transfinite. Indeed, in certain ways, transfinite cardinal
arithmetic looks much more like “ordinary” arithmetic than does transfinite
ordinal arithmetic:

Proposition card-arithmetic.2. \(\oplus\) and \(\otimes\) are commutative and associative.

Proof. For commutativity, by ?? it suffices to observe that \((a \sqcup b) \approx (b \sqcup a)\)
and \((a \times b) \approx (b \times a)\). We leave associativity as an exercise. \(\square\)
Problem card-arithmetic.2. Prove that $\oplus$ and $\otimes$ are associative.

Proposition card-arithmetic.3. A is infinite iff $|A| \oplus 1 = 1 \oplus |A| = |A|$.

Proof. As in ??, from ?? and ??.

This explains why we need to use different symbols for ordinal versus cardinal addition/multiplication: these are genuinely different operations. This next pair of results shows that ordinal versus cardinal exponentiation are also different operations. (Recall that ?? entails that $2 = \{0, 1\}$):

Lemma card-arithmetic.4. \(|\wp(A)| = 2^{|A|}\), for any \(A\).

Proof. For each subset \(B \subseteq A\), let \(\chi_B \in \wp(2)\) be given by:

\[
\chi_B(x) = \begin{cases} 
1 & \text{if } x \in B \\
0 & \text{otherwise.}
\end{cases}
\]

Now let \(f(B) = \chi_B\); this defines a bijection \(f: \wp(A) \to A^2\). So \(\wp(A) \approx A^2\). Hence \(\wp(A) \approx |A|^2\), so that \(|\wp(A)| = |A|^2 = 2^{|A|}\).

This snappy proof essentially subsumes the discussion of ?? There, we showed how to “reduce” the uncountability of \(\wp(\omega)\) to the uncountability of the set of infinite binary strings, \(\mathbb{B}^\omega\). In effect, \(\mathbb{B}^\omega\) is just \(\omega^2\); and the preceding proof showed that the reasoning we went through in ?? will go through using any set \(A\) in place of \(\omega\). The result also yields a quick fact about cardinal exponentiation:

Corollary card-arithmetic.5. \(a < 2^a\) for any cardinal \(a\).

Proof. From Cantor’s Theorem (??) and Lemma card-arithmetic.4.

So \(\omega < 2^\omega\). But note: this is a result about cardinal exponentiation. It should be contrasted with ordinal exponentiation, since in the latter case \(\omega = 2^{(\omega)}\) (see ??).

Whilst we are on the topic of cardinal exponentiation, we can also be a bit more precise about the “way” in which \(\mathbb{R}\) is non-enumerable.

Theorem card-arithmetic.6. \(|\mathbb{R}| = 2^\omega\)

Proof skeleton. There are plenty of ways to prove this. The most straightforward is to argue that \(\wp(\omega) \leq \mathbb{R}\) and \(\mathbb{R} \leq \wp(\omega)\), and then use Schröder-Bernstein to infer that \(\mathbb{R} \approx \wp(\omega)\), and Lemma card-arithmetic.4 to infer that \(|\mathbb{R}| = 2^\omega\). We leave it as an (illuminating) exercise to define injections \(f: \wp(\omega) \to \mathbb{R}\) and \(g: \mathbb{R} \to \wp(\omega)\).

Problem card-arithmetic.3. Complete the proof of Theorem card-arithmetic.6, by showing that \(\wp(\omega) \leq \mathbb{R}\) and \(\mathbb{R} \leq \wp(\omega)\).
It turns out that transfinite cardinal addition and multiplication is extremely easy. This follows from the fact that cardinals are (certain) ordinals, and so well-ordered, and so can be manipulated in a certain way. Showing this, though, is not so easy. To start, we need a tricksy definition:

**Definition card-arithmetic.7.** We define a canonical ordering, $\prec$, on pairs of ordinals, by stipulating that $\langle \alpha_1, \alpha_2 \rangle \prec \langle \beta_1, \beta_2 \rangle$ iff either:

1. $\max(\alpha_1, \alpha_2) < \max(\beta_1, \beta_2)$; or
2. $\max(\alpha_1, \alpha_2) = \max(\beta_1, \beta_2)$ and $\alpha_1 < \beta_1$; or
3. $\max(\alpha_1, \alpha_2) = \max(\beta_1, \beta_2)$ and $\alpha_1 = \beta_1$ and $\alpha_2 < \beta_2$

**Lemma card-arithmetic.8.** $\langle \alpha \times \alpha, \prec \rangle$ is a well-order, for any ordinal $\alpha$.

*Proof.* Evidently $\prec$ is connected on $\alpha \times \alpha$. For suppose that neither $\langle \alpha_1, \alpha_2 \rangle$ nor $\langle \beta_1, \beta_2 \rangle$ is $\prec$-less than the other. Then $\max(\alpha_1, \alpha_2) = \max(\beta_1, \beta_2)$ and $\alpha_1 = \beta_1$ and $\alpha_2 = \beta_2$, so that $\langle \alpha_1, \alpha_2 \rangle = \langle \beta_1, \beta_2 \rangle$.

To show well-ordering, let $X \subseteq \alpha \times \alpha$ be non-empty. Since $\alpha$ is an ordinal, some $\delta$ is the least member of $\{ \max(\gamma_1, \gamma_2) : \langle \gamma_1, \gamma_2 \rangle \in X \}$. Now discard all pairs from $\{ \langle \gamma_1, \gamma_2 \rangle \in X : \max(\gamma_1, \gamma_2) = \delta \}$ except those with least first coordinate; from among these, the pair with least second coordinate is the $\prec$-least element of $X$.

Now for a teensy, simple observation:

**Proposition card-arithmetic.9.** If $\alpha \approx \beta$, then $\alpha \times \alpha \approx \beta \times \beta$.

*Proof.* Just let $f : \alpha \to \beta$ induce $\langle \gamma_1, \gamma_2 \rangle \mapsto \langle f(\gamma_1), f(\gamma_2) \rangle$.

And now we will put all this to work, in proving a crucial lemma:

**Lemma card-arithmetic.10.** $\alpha \approx \alpha \times \alpha$, for any infinite ordinal $\alpha$

*Proof.* For reductio, let $\alpha$ be the least infinite ordinal for which this is false. ?? shows that $\omega \approx \omega \times \omega$, so $\omega \in \alpha$. Moreover, $\alpha$ is a cardinal: suppose otherwise, for reductio; then $|\alpha| \in \alpha$, so that $|\alpha| \approx |\alpha| \times |\alpha|$, by hypothesis; and $|\alpha| \approx \alpha$ by definition; so that $\alpha \approx \alpha \times \alpha$ by Proposition card-arithmetic.9.

Now, for each $\langle \gamma_1, \gamma_2 \rangle \in \alpha \times \alpha$, consider the segment:

$$\text{Seg}(\gamma_1, \gamma_2) = \{ \langle \delta_1, \delta_2 \rangle \in \alpha \times \alpha : \langle \delta_1, \delta_2 \rangle \prec \langle \gamma_1, \gamma_2 \rangle \}$$
Letting $\gamma = \max(\gamma_1, \gamma_2)$, note that $\langle \gamma_1, \gamma_2 \rangle \vartriangleleft \langle \gamma + 1, \gamma + 1 \rangle$. So, when $\gamma$ is infinite, observe:

$$\text{Seg}(\gamma_1, \gamma_2) \vartriangleleft \left((\gamma + 1) \cdot (\gamma + 1)\right)$$
$$\cong (\gamma \cdot \gamma), \text{ by } ?? \text{ and Proposition card-arithmetic.9}$$
$$\cong \gamma, \text{ by the induction hypothesis}$$
$$\vartriangleleft \alpha, \text{ since } \alpha \text{ is a cardinal}$$

So $\text{ord}(\alpha \times \alpha, \triangleleft) \leq \alpha$, and hence $\alpha \times \alpha \preceq \alpha$. Since of course $\alpha \preceq \alpha \times \alpha$, the result follows by Schröder-Bernstein. \hfill \Box

Finally, we get to our simplifying result:

**Theorem card-arithmetic.11.** If $a, b$ are infinite cardinals, then:

$$a \otimes b = a \oplus b = \text{max}(a, b).$$

**Proof.** Without loss of generality, suppose $a = \text{max}(a, b)$. Then invoking Lemma card-arithmetic.10, $a \otimes a = a \leq a \oplus b \leq a \oplus a \leq a \otimes a$. \hfill \Box

Similarly, if $a$ is infinite, an $a$-sized union of $\leq a$-sized sets has size $\leq a$:

**Proposition card-arithmetic.12.** Let $a$ be an infinite cardinal. For each ordinal $\beta \in a$, let $X_\beta$ be a set with $|X_\beta| \leq a$. Then $\bigcup_{\beta \in a} X_\beta \leq a$.

**Proof.** For each $\beta \in a$, fix an injection $f_\beta : X_\beta \to a$.\footnote{How are these “fixed”? See ??;} Define an injection $g : \bigcup_{\beta \in a} X_\beta \to a$ by $g(v) = \langle \beta, f_\beta(v) \rangle$, where $v \in X_\beta$ and $v \notin X_\gamma$ for any $\gamma \in \beta$. Now $\bigcup_{\beta \in a} X_\beta \preceq a \times a \approx a$ by Theorem card-arithmetic.11. \hfill \Box

### card-arithmetic.3 Some Simplification with Cardinal Exponentiation

Whilst defining $\vartriangleleft$ was a little involved, the upshot is a useful result concerning cardinal addition and multiplication, Theorem card-arithmetic.11. Transfinite exponentiation, however, cannot be simplified so straightforwardly. To explain why, we start with a result which extends a familiar pattern from the finitary case (though its proof is at a high level of abstraction):

**Proposition card-arithmetic.13.** $a^{b \otimes c} = a^b \otimes a^c$ and $(a^b)^c = a^{b \otimes c}$, for any cardinals $a, b, c$.

**Proof.** For the first claim, consider a function $f : (b \sqcup c) \to a$. Now “split this”,

by defining $f_b(\beta) = f(\beta, 0)$ for each $\beta \in b$, and $f_c(\gamma) = f(\gamma, 1)$ for each $\gamma \in c$.

The map $f \mapsto (f_b \times f_c)$ is a bijection $b^{\sqcup}c : a \to (b^a \times c^a)$.

For the second claim, consider a function $f : c \to (b^a)$; so for each $\gamma \in c$ we have some function $f(\gamma) : b \to a$. Now define $f^*(\beta, \gamma) = (f(\gamma))^{\langle \beta, \gamma \rangle}$ for each $\langle \beta, \gamma \rangle \in b \times c$. The map $f \mapsto f^*$ is a bijection $c^b : a \to b^{c \otimes a}$. \hfill \Box
Now, what we would like is an easy way to compute $a^b$ when we are dealing with infinite cardinals. Here is a nice step in this direction:

**Proposition card-arithmetic.14.** If $2 \leq a \leq b$ and $b$ is infinite, then $a^b = 2^b$

*Proof.*

\[
2^b \leq a^b \leq (2^a)^b = 2^{a \otimes b} = 2^b,
\]

by Lemma card-arithmetic.4, Proposition card-arithmetic.13, and Theorem card-arithmetic.11. □

We should not really expect to be able to simplify this any further, since $b < 2^b$ by Lemma card-arithmetic.4. However, this does not tell us what to say about $a^b$ when $b < a$. Of course, if $b$ is finite, we know what to do.

**Proposition card-arithmetic.15.** If $a$ is infinite and $n \in \omega$ then $a^n = a$

*Proof.* $a^n = a \otimes a \otimes \ldots \otimes a = a$, by Theorem card-arithmetic.11. □

Additionally, in some other cases, we can control the size of $a^b$:

**Proposition card-arithmetic.16.** If $2 \leq b < a \leq 2^b$ and $b$ is infinite, then $a^b = 2^b$

*Proof.* $2^b \leq a^b \leq (2^b)^b = 2^{b \otimes b} = 2^b$, reasoning as in Proposition card-arithmetic.14. □

But, beyond this point, things become rather more subtle.

### card-arithmetic.4 The Continuum Hypothesis

The previous result hints (correctly) that cardinal exponentiation would be quite easy, if infinite cardinals are guaranteed to “play straightforwardly” with powers of $2$, i.e., (by Lemma card-arithmetic.4) with taking powersets. But we cannot assume that infinite cardinals do play straightforwardly powersets.

To start unpacking this, we introduce some nice notation.

**Definition card-arithmetic.17.** Where $a^\oplus$ is the least cardinal strictly greater than $a$, we define two infinite sequences:

\[
\begin{align*}
\aleph_0 &= \omega & \beth_0 &= \omega \\
n_{\alpha+1} &= (n_{\alpha})^\oplus & \beth_{\alpha+1} &= 2^{\beth_{\alpha}} \\
n_{\alpha} &= \bigcup_{\beta<\alpha} n_{\beta} & \beth_{\alpha} &= \bigcup_{\beta<\alpha} \beth_{\beta}
\end{align*}
\]

when $\alpha$ is a limit ordinal.
The definition of $a^\oplus$ is in order, since ?? tells us that, for each cardinal $a$, there is some cardinal greater than $a$, and Transfinite Induction guarantees that there is a least cardinal greater than $a$. The rest of the definition of $a$ is provided by transfinite recursion.

Cantor introduced this “$\aleph$” notation; this is aleph, the first letter in the Hebrew alphabet and the first letter in the Hebrew word for “infinite”. Peirce introduced the “$\beth$” notation; this is beth, which is the second letter in the Hebrew alphabet.\(^2\) Now, these notations provide us with infinite cardinals.

**Proposition card-arithmetic.18.** $\aleph_\alpha$ and $\beth_\alpha$ are cardinals, for every ordinal $\alpha$.

**Proof.** Both results hold by a simple transfinite induction. $\aleph_0 = \beth_0 = \omega$ is a cardinal by ???. Assuming $\aleph_\alpha$ and $\beth_\alpha$ are both cardinals, $\aleph_{\alpha+1}$ and $\beth_{\alpha+1}$ are explicitly defined as cardinals. And the union of a set of cardinals is a cardinal, by ???. \qed

Moreover, every infinite cardinal is an $\aleph$:

**Proposition card-arithmetic.19.** If $a$ is an infinite cardinal, then $a = \aleph_\gamma$ for some unique $\gamma$.

**Proof.** By transfinite induction on cardinals. For induction, suppose that if $b < a$ then $b = \aleph_\beta$. If $a = b^\oplus$ for some $b$, then $a = (\aleph_\beta)^\oplus = \aleph_{\beta+1}$. If $a$ is not the successor of any cardinal, then since cardinals are ordinals $a = \bigcup_{b < a} b = \bigcup_{\beta < a} \aleph_\beta$, so $a = \aleph_\gamma$ where $\gamma = \bigcup_{b < a} \gamma_b$. \qed

Since every infinite cardinal is an $\aleph$, this prompts us to ask: is every infinite cardinal a $\beth$? Certainly if that were the case, then the infinite cardinals would “play straightforwardly” with the operation of taking powersets. Indeed, we would have the following:

\begin{center}
**Generalized Continuum Hypothesis (GCH).** $\aleph_\alpha = \beth_\alpha$, for all $\alpha$.
\end{center}

Moreover, if GCH held, then we could make some considerable simplifications with cardinal exponentiation. In particular, we could show that when $b < a$, the value of $a^b$ is trapped by $a \leq a^b \leq a^\oplus$. We could then go on to give precise conditions which determine which of the two possibilities obtains (i.e., whether $a = a^b$ or $a^b = a^\oplus$).\(^3\)

But GCH is a hypothesis, not a theorem. In fact, Gödel (1938) proved that if ZFC is consistent, then so is ZFC + GCH. But it later turned out that we can equally add ¬GCH to ZFC. Indeed, consider the simplest non-trivial instance of GCH, namely:

\(^2\)Peirce used this notation in a letter to Cantor of December 1900. Unfortunately, Peirce also gave a bad argument there that $\beth_\alpha$ does not exist for $\alpha \geq \omega$.

\(^3\)The condition is dictated by cofinality.
Continuum Hypothesis (CH). $\aleph_1 = \beth_1$.

Cohen (1963) proved that if ZFC is consistent then so is ZFC + ¬CH. So the Continuum Hypothesis is independent from ZFC.

The Continuum Hypothesis is so-called, since “the continuum” is another name for the real line, $\mathbb{R}$. Theorem card-arithmetic.6 tells us that $|\mathbb{R}| = \beth_1$. So the Continuum Hypothesis states that there is no cardinal between the cardinality of the natural numbers, $\aleph_0 = \beth_0$, and the cardinality of the continuum, $\beth_1$.

Given the independence of (G)CH from ZFC, what should say about their truth? Well, there is much to say. Indeed, and much fertile recent work in set theory has been directed at investigating these issues. But two very quick points are certainly worth emphasising.

First: it does not immediately follow from these formal independence results that either GCH or CH is indeterminate in truth value. After all, maybe we just need to add more axioms, which strike us as natural, and which will settle the question one way or another. Gödel himself suggested that this was the right response.

Second: the independence of CH from ZFC is certainly striking, but it is certainly not incredible (in the literal sense). The point is simply that, for all ZFC tells us, moving from cardinals to their successors may involve a less blunt tool than simply taking powersets.

With those two observations made, if you want to know more, you will now have to turn to the various philosophers and mathematicians with horses in the race.⁴

### card-arithmetic.5 $\aleph$-Fixed Points

In ??, we suggested that Replacement stands in need of justification, because it forces the hierarchy to be rather tall. Having done some cardinal arithmetic, we can give a little illustration of the height of the hierarchy.

Evidently $0 < \aleph_0$, and $1 < \aleph_1$, and $2 < \aleph_2$... and, indeed, the difference in size only gets bigger with every step. So it is tempting to conjecture that $\kappa < \aleph_\kappa$ for every ordinal $\kappa$.

But this conjecture is false, given ZFC. In fact, we can prove that there are $\aleph$-fixed-points, i.e., cardinals $\kappa$ such that $\kappa = \aleph_\kappa$.

**Proposition card-arithmetic.20.** There is an $\aleph$-fixed-point.

---

⁴Though you might want to start by reading Potter (2004, §15.6).
Proof. Using recursion, define:

\[
\kappa_0 = 0 \\
\kappa_{n+1} = \aleph_{\kappa_n} \\
\kappa = \bigcup_{n<\omega} \kappa_n
\]

Now \(\kappa\) is a cardinal by \(\Xi\). But now:

\[
\kappa = \bigcup_{n<\omega} \kappa_{n+1} = \bigcup_{n<\omega} \aleph_{\kappa_n} = \bigcup_{\alpha<\kappa} \aleph_\alpha = \aleph_\kappa
\]

Boolos once wrote an article about exactly the \(\aleph\)-fixed-point we just constructed. After noting the existence of \(\kappa\), at the start of his article, he said:

\[
[k is a pretty big number, by the lights of those with no previous exposure to set theory, so big, it seems to me, that it calls into question the truth of any theory, one of whose assertions is the claim that there are at least \(\kappa\) objects. (Boolos, 2000, p. 257)
\]

And he ultimately concluded his paper by asking:

\[
[do we suspect that, however it may have been at the beginning of the story, by the time we have come thus far the wheels are spinning and we are no longer listening to a description of anything that is the case? (Boolos, 2000, p. 268)
\]

If we have, indeed, outrun “anything that is the case”, then we must point the finger of blame directly at Replacement. For it is this axiom which allows our proof to work. In which case, one assumes, Boolos would need to revisit the claim he made, a few decades earlier, that Replacement has “no undesirable” consequences (see \(\Xi\)).

But is the existence of \(\kappa\) so bad? It might help, here, to consider Russell’s Tristram Shandy paradox. Tristram Shandy documents his life in his diary, but it takes him a year to record a single day. With every passing year, Tristram falls further and further behind: after one year, he has recorded only one day, and has lived 364 days unrecorded days; after two years, he has only recorded two days, and has lived 728 unrecorded days; after three years, he has only recorded three days, and lived 1092 unrecorded days . . . 5 Still, if Tristram is immortal, Tristram will manage to record every day, for he will record the \(n\)th day on the \(n\)th year of his life. And so, “at the end of time”, Tristram will have a complete diary.

Now: why is this so different from the thought that \(\alpha\) is smaller than \(\aleph_\alpha\)—and indeed, increasingly, desperately smaller—up until \(\kappa\), at which point, we catch up, and \(\kappa = \aleph_\kappa\)?

5Forgetting about leap years.
Setting that aside, and assuming we accept ZFC, let’s close with a little more fun concerning fixed-point constructions. The next three results establish, intuitively, that there is a (non-trivial) point at which the hierarchy is as wide as it is tall:

**Proposition card-arithmetic.21.** There is a ℶ-fixed-point, i.e., a κ such that κ = ℶκ.

*Proof.* As in Proposition card-arithmetic.20, using “ℵ” in place of “κ”.

**Proposition card-arithmetic.22.** |Vω+α| = ℶα. If ω · ω ≤ α, then |Vα| = ℶα.

*Proof.* The first claim holds by a simple transfinite induction. The second claim follows, since if ω · ω ≤ α then ω + α = α. To establish this, we use facts about ordinal arithmetic from Prop. card-arithmetic.21. First note that ω · ω = ω · (1 + ω) = (ω · 1) + (ω · ω) = ω + (ω · ω). Now if ω · ω ≤ α, i.e., α = (ω · ω) + β for some β, then ω + α = ω + ((ω · ω) + β) = (ω + (ω · ω)) + β = (ω · ω) + β = α.

**Corollary card-arithmetic.23.** There is a κ such that |Vκ| = κ.

*Proof.* Let κ be a ℶ-fixed point, as given by Proposition card-arithmetic.21. Clearly ω · ω < κ. So |Vκ| = ℶκ = κ by Proposition card-arithmetic.22.

There are as many stages beneath Vκ as there are elements of Vκ. Intuitively, then, Vκ is as wide as it is tall. This is very Tristram-Shandy-esque: we move from one stage to the next by taking powersets, thereby making our hierarchy much bigger with each step. But, “in the end”, i.e., at stage κ, the hierarchy’s width catches up with its height.

One might ask: How often does the hierarchy’s width match its height? The answer is: As often as there are ordinals. But this needs a little explanation.

We define a term τ as follows. For any A, let:

\[
\begin{align*}
\tau_0(A) &= |A| \\
\tau_{n+1}(A) &= \beth\tau_n(A) \\
\tau(A) &= \bigcup_{n<\omega} \tau_n(A)
\end{align*}
\]

As in Proposition card-arithmetic.21, τ(A) is a ℶ-fixed point for any A, and trivially |A| < τ(A). So now consider this recursive definition:

\[
\begin{align*}
W_0 &= 0 \\
W_{\alpha+1} &= \tau(W_\alpha) \\
W_\alpha &= \bigcup_{\beta<\alpha} W_\beta, \text{ when } \alpha \text{ is a limit}
\end{align*}
\]
The construction is defined for all ordinals. Intuitively, then, $W$ is “an injection” from the ordinals to $\aleph$-fixed points. And, exactly as before, $V_{W,\alpha}$ is as wide as it is tall, for any $\alpha$.

Photo Credits
Bibliography


