Chapter udf

Cardinal Arithmetic

card-arithmetic.1 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:

\[ a \oplus b := |a \sqcup b| \]
\[ a \otimes b := |a \times b| \]
\[ a^b := |^b a| \]

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

Problem card-arithmetic.1. Prove in ZF that $^XY$ exists for any sets $X$ and $Y$. Working in ZF, compute rank($^XY$) from rank($X$) and 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 multiplication. 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. \qed
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 $\omega = \{0, 1\}$):

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

Proof. For each subset $B \subseteq A$, let $\chi_B \in A^2$ 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, $B^\omega$; In effect, $B^\omega$ is just $\omega^\omega$; 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 $\wp(\omega) \preceq \mathbb{R}$ and $\mathbb{R} \preceq \wp(\omega)$, 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 for the reader 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 $\wp(\omega) \preceq \mathbb{R}$ and $\mathbb{R} \preceq \wp(\omega)$.
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.** 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.** $\langle \alpha \times \alpha, \prec \rangle$ 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 $X$. \hfill \Box

Now for a teensy, simple observation:

**Proposition.** 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.** $\alpha \approx \alpha \times \alpha$, 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.**

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

$\text{Seg}(\gamma_1, \gamma_2) = \{\langle \delta_1, \delta_2 \rangle \in \alpha \times \alpha : \langle \delta_1, \delta_2 \rangle \prec \langle \gamma_1, \gamma_2 \rangle\}$

---

1 Cf. the naughtiness described in the footnote to ??.
Let $\gamma = \max(\gamma_1, \gamma_2)$. When $\gamma$ is infinite, observe:

$$\text{Seg}(\gamma_1, \gamma_2) \trianglelefteq ((\gamma + 1) \cdot (\gamma + 1)), \text{ by the first clause defining } \triangleleft$$

$$\approx (\gamma \cdot \gamma), \text{ by Proposition card-arithmetic.9}$$

$$\approx \gamma, \text{ by the induction hypothesis}$$

$$\prec \alpha, \text{ since } \alpha \text{ is a cardinal}$$

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.

Finally, we get to our simplifying result:

**Theorem card-arithmetic.11.** If \(a, b\) are infinite cardinals, \(a \otimes b = a \oplus b = \max(a, b)\).

**Proof.** Without loss of generality, suppose \(a = \max(a, b)\). Then invoking Proposition card-arithmetic.10, \(a \otimes a = a \leq a \oplus b \leq a \oplus a \leq a \otimes a\).

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 \(\bigcup_{\beta \in a} X_\beta \preceq a \times a \approx a\) by Theorem card-arithmetic.11.

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

Whilst defining \(\triangleleft\) 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 at quite 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 \(f: (b \sqcup c) \rightarrow a\). Now “split this”, by defining \(f_\beta(\gamma) = f(\beta, 0)\) for each \(\beta \in b\), and \(f_\gamma(\beta) = f(\gamma, 1)\) for each \(\gamma \in c\).

The map \(f \mapsto (f_\beta \times f_\gamma)\) is a bijection \(b \sqcup c \rightarrow (b \times c)\).

For the second claim, consider a function \(f: c \rightarrow (b^a)\); so for each \(\gamma \in c\) we have some function \(f(\gamma): b \rightarrow a\). Now define \(f^*(\beta, \gamma) = f(\gamma)(\beta)\) for each \(\langle \beta, \gamma \rangle \in b \times c\). The map \(f \mapsto f^*\) is a bijection \(c \rightarrow (b^a)\) to \(b^a \otimes c\).
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.**

\[ 2^b \leq a^b, \text{ as } 2 \leq a \]
\[ \leq (2^a)^b, \text{ by Lemma card-arithmetic.4} \]
\[ = 2^{a \otimes b}, \text{ by Proposition card-arithmetic.13} \]
\[ = 2^b, \text{ by Theorem card-arithmetic.11} \]

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 $n - 1$ applications of Theorem card-arithmetic.11.

Additionally, in certain 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.

### 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 nicely with powersets. This section is dedicated to explaining all of this. (Although, to be honest, it’s more of a gesture in the direction of something fascinating.)

We will start by introducing some nice notation.

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

\[ \aleph_0 := \omega \]
\[ \beth_0 := \omega \]
\[ \aleph_{\alpha+1} := (\aleph_{\alpha})^\oplus \]
\[ \beth_{\alpha+1} := 2^{\aleph_{\alpha}} \]
\[ \aleph_\alpha := \bigcup_{\beta < \alpha} \aleph_\beta \]
\[ \beth_\alpha := \bigcup_{\beta < \alpha} \beth_\beta \] 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. Now, these notations provide us with infinite cardinals.

**Proposition card-arithmetic.18.** Both $\aleph_\alpha$ 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 ??.

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

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

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

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:

**General Continuum Hypothesis (GCH).** $\aleph_\alpha = \beth_\alpha$, for all $\alpha$.

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 $a^b = a^\oplus$).

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 $\neg$GCH to $ZFC$. Indeed, consider the simplest non-trivial instance of GCH, namely:

---

2Peirce 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 $\alpha \geq \omega$.

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

Cohen (1963) proved that if \( \text{ZFC} \) is consistent then so is \( \text{ZFC} + \neg \text{CH} \).

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 \( \text{ZFC} \), 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 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 \( \text{ZFC} \) is certainly striking, but it is certainly not incredible (in the literal sense). The point is simply that, for all \( \text{ZFC} \) 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. (Though you may want to start with the very nice discussion in Potter 2004, §15.6.)

\section*{card-arithmetic.5 \( \aleph \)-Fixed Points}

In \ref{card-arithmetic:sec}, 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 \textit{bigger} with every step. So it is tempting to conjecture that \( \kappa < \aleph_\kappa \) for every ordinal \( \kappa \).

But this conjecture is \textit{false}, given \( \text{ZFC} \). In fact, we can easily prove that there are \( \aleph \)-fixed-points, i.e., cardinals \( \kappa \) such that \( \kappa = \aleph_\kappa \).

\begin{proposition}[card-arithmetic.20] There is an \( \aleph \)-fixed-point.
\end{proposition}

\begin{proof} Using recursion, define:

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

\end{proof}
Now $\kappa$ is a cardinal by ???. 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:

[\kappa 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 ??).

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 . . .

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 $\kappa = \aleph_{\kappa}$?

Setting that aside, and assuming we accept $\text{ZFC}$, 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 $\beth$-fixed-point, i.e., a $\kappa$ such that $\kappa = \beth_{\kappa}$

**Proof.** As in **Proposition card-arithmetic.20**, using “$\beth$” in place of “$\aleph$”.  

---

*Forgetting about leap years.*
Proposition card-arithmetic.22. \( |V_{\omega + \alpha}| = \beth_\alpha \). If \( \omega \cdot \omega \leq \alpha \), then \( |V_\alpha| = \beth_\alpha \).

Proof. The first claim holds by a simple transfinite induction. The second claim follows, since if \( \omega \cdot \omega \leq \alpha \) then \( \omega + \alpha = \alpha \). To establish this, we use facts about ordinal arithmetic from ???. First note that \( \omega \cdot \omega = \omega \cdot (1 + \omega) = (\omega \cdot 1) + (\omega \cdot \omega) = \omega + (\omega \cdot \omega) \). Now if \( \omega \cdot \omega \leq \alpha \), i.e., \( \alpha = (\omega \cdot \omega) + \beta \) for some \( \beta \), then \( \omega + \alpha = \omega + ((\omega \cdot \omega) + \beta) = (\omega + (\omega \cdot \omega)) + \beta = (\omega \cdot \omega) + \beta = \alpha \). \( \square \)

Corollary card-arithmetic.23. There is a \( \kappa \) such that \( |V_\kappa| = \kappa \).

Proof. Let \( \kappa \) be a \( \beth \)-fixed point, as given by Proposition card-arithmetic.21. Clearly \( \omega \cdot \omega < \kappa \). So \( |V_\kappa| = \beth_\kappa = \kappa \) by Proposition card-arithmetic.22. \( \square \)

There are as many stages beneath \( V_\kappa \) as there are elements of \( V_\kappa \). Intuitively, then, \( V_\kappa \) 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 \( \kappa \), 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 \( \tau \) as follows. For any \( A \), let \( \tau_0(A) = |A| \), let \( \tau_{\alpha+1}(A) = \beth_{\kappa_\alpha} \), and let \( \tau(\alpha) = \bigcup_{\beta < \alpha} \tau(\beta) \) if \( \beta \) is a limit.

The construction is defined for all ordinals. Intuitively, then, \( \tau \) is an injection from the ordinals to \( \beth \)-fixed points. And, exactly as before, for any ordinal \( \alpha \), the stage \( V_{\tau_\alpha} \) is as wide as it is tall.

Photo Credits

---

\(^5\)We’re using the Hebrew letter “\( \beth \)”; it has no standard definition in set theory.
Bibliography


