ORDER AND ARITHMETIC OF CARDINALITIES

PETE L. CLARK

Here we pursue Cantor's theory of cardinalities of infinite sets a bit more deeply. We also begin to take a more sophisticated approach in that we identify which results depend upon the Axiom of Choice and strive to give proofs which avoid it when possible. However, we defer a formal discussion of the Axiom of Choice and its equivalents to a later installment, so the reader who has not encountered it before can ignore these comments and/or skip ahead to the next installment.

We warn the reader that the main theorem in this installment – Theorem 1 (which we take the liberty of christening "The Second Fundamental Theorem of Set Theory") – will not be proved until the next installment, in which we give a systematic discussion of well-ordered sets.

1. The fundamental relation $\leq$

Let's look back at what we did in the last section. We introduced a notion of equivalence on sets – essentially we proposed the project of classifying sets up to bijection. Looking at finite sets, we found that each equivalence class contained a representative of the form $[n]$ for a unique natural number n. Thus the set of equivalence classes of finite sets is $\mathbb{N}$. Then we considered whether all infinite sets were equivalent to each other, and found that they are not.

If we look back at finite sets (it is remarkable, and perhaps comforting, how much of the inspiration for some rather recondite-looking set-theoretic constructions comes from the case of finite sets) we can't help but notice that $\mathbb{N}$ has so much more structure than just a set. First, it is a semiring: this means that we have operations of $+$ and $\cdot$, but in general we do not have $-$ or $/$. Second it has a natural ordering $\leq$ which is indeed a *well-ordering*: that is, $\leq$ is a linear ordering on x in which every non-empty subset has a least element. (The well-ordering property is easily seen to be equivalent to the principle of mathematical induction.)

Remarkably, *all* of these structures generalize fruitfully to equivalence classes of sets! What does this mean? For a set S, let $|S|$ stand for its equivalence class. (This construction is commonplace in mathematics but has problematic aspects in set theory since the collection of sets equivalent with any nonempty set S does not form a set. Let us run with this notion for the moment, playing an important mathematician's trick: rather than worrying about what $|S|$ *is*, let us see how it *behaves*, and then later we can attempt to define it in terms of its behavior.)

Definition: We will say $S_1 \leq S_2$ if there exists an injection $\iota : S_1 \hookrightarrow S_2$.

Let $\mathcal{F}$ be any family (i.e., set!) of sets S_α. Then our $\leq$ gives a relation on $\mathcal{F}$;

what properties does it have? It is of course reflexive and transitive, which means it is (by definition) a *quasi-ordering*. On the other hand, it is generally not a partial ordering, because $S_{\alpha_1} \leq S_{\alpha_2}$ and $S_{\alpha_2} \leq S_{\alpha_1}$ does not in general imply that $S_{\alpha_1} = S_{\alpha_2}$: indeed, suppose have two distinct, but equivalent sets (say, two sets with three elements apiece). However, given a quasi-ordering we can formally associate a partial ordering, just by taking the quotient by the equivalence relation $x \leq y, y \leq x$. However, exactly how the associated partial ordering relates to the given quasi-ordering is in general unclear.

Therefore we can try to do something less drastic. Namely, let us write $|S_1| \leq |S_2|$ if $S_1 \leq S_2$. We must check that this is well-defined, but no problem: indeed, if $S_i \equiv T_i$ then choosing bijections $\beta_i : S_i \to T_i$, we get an injection

$$\beta_2 \circ \iota \circ \beta_1^{-1} : T_1 \to T_2.$$

Thus we can pass from the quasi-ordered set $(\mathcal{F}, \leq)$ to the quasi-ordered set of equivalence classes $(|\mathcal{F}|, \leq)$. Since we removed an obvious obstruction to the quasi-ordering being a partial ordering, it is natural to wonder whether or not this partial ordering on equivalence classes is better behaved. If $\mathcal{F}$ is a family of finite sets, then $|\mathcal{F}|$ is a subset of $\mathbb{N}$ so we have a well-ordering. The following stunning result asserts that this remains true for infinite sets:

Theorem 1. *(Second fundamental theorem of set theory) For any family $\mathcal{F}$ of sets, the relation $\leq$ descends to $|\mathcal{F}|$ and induces a well-ordering.*

Remark: This result requires the Axiom of Choice (AC), to be discussed later.

In its full generality, Theorem 1 is best derived in the course of a systematic development of the theory of well-ordered sets, and we shall present this theory later on. However, the following special case can be proved now:

Theorem 2. *(Schröder-Bernstein) If $M \leq N$ and $N \leq M$, then $M \equiv N$.*

Proof: Certainly we may assume that M and N are disjoint. Let $f : M \hookrightarrow N$ and $g : N \hookrightarrow M$. Consider the following function B on $M \cup N$: if $x \in M$, $B(x) = f(x) \in N$; if $x \in N$, $B(x) = g(x) \in M$. Now we consider the B orbits on $M \cup N$. Put $B^m = B \circ \ldots \circ B$ (m times). There are four cases:
Case 1: The forward B-orbit of x is finite. Equivalently, for some m, $B^m(x) = x$. Then the backwards B-orbit is equal to the B-orbit, so the full B-orbit is finite. Otherwise the B-orbit is infinite, and we consider the backwards B-orbit.
Case 2: The backwards B-orbit also continues indefinitely, so for all $m \in \mathbb{Z}$ we have pairwise disjoint elements $B^m(x) \in M \cup N$.
Case 3: For some $m \in \mathbb{Z}^+$, $B^{-m}(x)$ is not in the image of f or g.

As these possibilities are exhaustive, we get a partition of $M \cup N$ into three types of orbits: (i) finite orbits, (ii) $\{B^m \mid m \geq m_0\}$, and (iii) $\{B^m \mid m \in \mathbb{Z}\}$. We can use this information to define a bijection from M to N. Namely, f itself is necessarily a bijection from the Case 1 elements of M to the Case 1 elements of N, and the same holds for Case 3. f need not surject onto every Case 2 element of N, but the Case 2 element of $M \cup N$ have been partitioned into sets isomorphic to $\mathbb{Z}^+$, and pairing up the first element occurring in M with the first element occurring in N, and so forth, we have defined a bijection from M to N!

Remark: In this proof we *did not* use the Axiom of Choice.

Theorem 1 asserts that $|S|$ is measuring, in a very reasonable sense, the *size* of the set S: if two sets are inequivalent, it is because one of them is larger than the other. This motivates a small change of perspective: we will say that $|S|$ is the *cardinality* of the set S. Note well that we have not made any mathematical change: we have not defined cardinalities in an absolute sense – i.e., we have not said what sort of object $|\mathbb{N}|$ is – but only in a relational sense: i.e., as an invariant of a set that measures whether a set is bigger or smaller than another set.

1.1. **Addition of cardinalities.** For two sets S_1 and S_2, define the disjoint union $S_1 \coprod S_2$ to be $S_1' \cup S_2'$, where $S_i' = \{(s,1) \mid s \in S_i\}$. Note that there is an obvious bijection $S_i \to S_i'$; the point of this little artifice is that even if S_1 and S_2 are not disjoint, S_1' and S_2' will be.[1] Now consider the set $S_1 \coprod S_2$.

Fact 3. *The equivalence class $|S_1 \coprod S_2|$ depends only on the equivalence classes $|S_1|$ and $|S_2|$.*

Proof: All this means is that if we have bijections $\beta_i : S_i \to T_i$, then there is a bijection from $S_1 \coprod S_2$ to $T_1 \coprod T_2$, which is clear: there is indeed a canonical bijection, namely $\beta_1 \coprod \beta_2$: by definition, this maps an element $(s,1)$ to $(\beta_1(s),1)$ and an element $(s,2)$ to $(\beta_2(s),2)$.

The upshot is that it makes formal sense to define $|S_1| + |S_2|$ as $|S_1 \coprod S_2|$: our addition operation on sets descends to equivalence classes. Note that on finite sets this amounts to

$$m + n = |[m]| + |[n]| = |[m] \coprod [n]| = |[m+n]| = m + n.$$

Theorem 4. *Let S and T be sets, not both finite. Suppose that $S \leq T$. Then $|S| + |T| = |T|$.*

Remark: By Theorem 1, for any two sets we have either $S \leq T$ or $T \leq S$, so the result implies that for all infinite sets, $|S| + |T| = \max(|S|, |T|)$. However, the proof of Theorem 4 itself does *not* require the Axiom of Choice, which is why we have stated it this way.

There is a fairly elementary proof of Theorem 4, which however uses Zorn's Lemma. At this stage in the development of the theory the reader might like to see such a proof, so we will present it now (certainly Zorn's Lemma is known and used in "mainstream mathematics"). We begin with the following preliminary result which is of interest in its own right.

Proposition 5. *An infinite set S can be expressed as a disjoint union of countable subsets.*

Proof: Consider the partially ordered set each of whose elements is a pairwise disjoint family of countable subsets of S, and with $\leq$ being set-theoretic inclusion. Any chain $\mathcal{F}_i$ in this poset has an upper bound: just take the union of all the elements in the chain: this is certainly a family of countable subsets of S, and if any element of $\mathcal{F}_i$ intersects any element of $\mathcal{F}_j$, then $\mathcal{F}_{\max(i,j)}$ contains both of these

---

[1]This in turn raises canonicity issues, which we will return to later.

elements so is not a pairwise disjoint family, contradiction. By Zorn's Lemma we are entitled to a maximal such family $\mathcal{F}$. Then $S \setminus \bigcup_{i \in \mathcal{F}} S_i$ must be finite, so the remaining elements can be added to any one of the elements of the family.

Proposition 6. *Any infinite set A can be written as $B \coprod C$, where $|A| = |B| = |C|$.*

Proof: Express $A = \bigcup_{i \in \mathcal{F}} A_i$, where each $A_i \cong \mathbb{Z}^+$. So partition S_i into $B_i \cup C_i$ where B_i and C_i are each countable, and take $B = \bigcup_{i \in \mathcal{F}} B_i$, $C = \bigcup_{i \in \mathcal{F}} C_i$.

Proof of Theorem 4: Let S and T be sets; by Theorem 1 we may assume $|S| \leq |T|$. Then clearly $|S| + |T| \leq |T| + |T|$, but the preceding result avers $|T| + |T| = |T|$. So $|S| + |T| \leq |T|$. Clearly $|T| \leq |S| + |T|$, so by the Schröder-Bernstein Theorem we conclude $|S| + |T| = |T|$.

Exercise 1: Suppose that S is infinite and $T \subset S$. Show that S can be expressed as a disjoint union of subsets of cardinality $|T|$.

1.2. **Subtraction of cardinalities.** It turns out that we cannot formally define a subtraction operation on infinite cardinalities, as one does for finite cardinalities using set-theoretic subtraction: given sets S_1 and S_2, to define $|S_1| - |S_2|$ we would like to find sets $T_i \cong S_i$ such that $T_2 \subset T_1$, and then define $|S_1| - |S_2|$ to be $|T_1 \setminus T_2|$. Of course even for finite sets this only makes literal sense if $|S_2| \leq |S_1|$; in general, we are led to introduce negative numbers through an entirely formal (or algebraic) process, which we can recognize as the group completion of a monoid (or the ring completion of a commutative semiring).

However, here the analogy between infinite and finite breaks down: given $S_2 \subset S_1$, $T_2 \subset T_1$ and bijections $\beta_i : S_i \to T_i$, we absolutely do not in general have a bijection $S_1 \setminus S_2 \to T_1 \setminus T_2$. For instance, take $S_1 = T_1 = \mathbb{Z}^+$ and $S_2 = 2\mathbb{Z}^+$, the even numbers. Then $|S_1 \setminus S_2| = |\mathbb{N}|$. However, we could take $T_2 = \mathbb{Z}^+$ and then $T_2 \setminus T_1 = \emptyset$. For that matter, given any $n \in \mathbb{Z}^+$, taking T_2 to be $\mathbb{Z}^+ \setminus [n]$, we get $T_1 \setminus T_2 = [n]$. Thus when attempting to define $|\mathbb{N}| - |\mathbb{N}|$ we find that we get all conceivable answers, namely all equivalence classes of at most countable sets. This phenomenon does generalize:

Proposition 7. *(Subtraction theorem) For any $|S_1| \leq |S_2| \leq |S_3|$, there exist bijections $\beta_1 : S_1 \to T_1$, $\beta_3 : S_3 \to T_3$ such that $T_1 \subset T_3$ and $|T_3 \setminus T_1| = |S_2|$.*

Proof: As long as S_1 and S_2 are disjoint, we may take $T_1 = S_1$, $T_2 = S_2$ and $T_3 = S_1 \cup S_2$.

1.3. **Multiplication of cardinalities.** Let S_1 and S_2 be sets. Using the Cartesian product, we can also define a multiplication of cardinalities:

$$|S_1| \times |S_2| = |S_1 \times S_2|.$$

We ask the reader to pause for 10 seconds and check that this is well-defined, i.e., invariant on equivalence classes.

At this point, we have what appears to be a very rich structure on our cardinalities: suppose that $\mathcal{F}$ is a family of sets which is, up to bijection, closed under $\coprod$ and $\times$. Then the family $|\mathcal{F}|$ of cardinalities of these sets has the structure of a well-ordered semiring.

Example: Take $\mathcal{F}$ to be any collection of finite sets containing, for all $n \in \mathbb{N}$, at least one set with n elements. Then $|\mathcal{F}| = \mathbb{N}$ and the semiring and (well)-ordering are the usual ones.

Example: Take $\mathcal{F}$ to be a family containing finite sets of all cardinalities together with $\mathbb{N}$. Then, since $\mathbb{N} \coprod \mathbb{N} \cong \mathbb{N}$ and $\mathbb{N} \times \mathbb{N} \cong \mathbb{N}$, the corresponding family of cardinals $|\mathcal{F}|$ is a well-ordered semiring. It contains $\mathbb{N}$ as a subring and one other element, $|\mathbb{N}|$; in other words, as a set of cardinalities it is $\mathbb{N} \cup \{\mathbb{N}\}$, a slightly confusing-looking construction which we will see much more of later on. As a well-ordered set we have just taken $\mathbb{N}$ and added a single element (the element $\mathbb{N}$!) which is is larger than every other element. It is clear that this gives a well-ordered set; indeed, given any well-ordered set $(S, \leq)$ there is another well-ordered set, say $s(S)$, obtained by adding an additional element which is strictly larger than every other element (check and see that this gives a well-ordering). The semiring structure is, however, not very interesting: every $x \in \mathbb{N} \cup \{\mathbb{N}\}$, $x + \mathbb{N} = x \cdot \mathbb{N} = \mathbb{N}$. In particular, the ring completion of this semiring is the 0 ring. (It suffices to see this on the underlying commutative monoid. Recall that the group completion of a commutative monoid M can be represented by pairs (p, m) of elements of M with $(p, m) \sim (p', m')$ iff there exists some $x \in M$ such that $x + p + m' = x + p' + m$. In our case, taking $x = \mathbb{N}$ we see that all elements are equivalent.)

However, like addition, multiplication of infinite cardinalities turns out not to be very interesting.

Theorem 8. *Let T be infinite and S a nonempty subset of T. Then $|S| \times |T| = |T|$.*

The same remarks are in order here as for the addition theorem (Theorem 4): combining with cardinal trichotomy, we conclude that $|S| \times |T| = \max(|S|, |T|)$ for any infinite sets. This deduction uses the Axiom of Choice, whereas the theorem as stated does not. However, it is easier to give a proof using Zorn's Lemma, which is what we will do. Moreover, as for the additive case, it is convenient to first establish the case of $S = T$. Indeed, assuming that $T \times T \cong T$, we have

$$|S| \times |T| \leq |T| \times |T| = |T| \leq |S| \times |T|.$$

So let us prove that for any infinite set T, $T \times T \cong T$.

Consider the poset consisting of pairs (S_i, f_i), where $S_i \subset T$ and f_i is a bijection from S_i to $S_i \times S_i$. Again the order relation is the natural one: $(S_i, f_i) \leq (S_j, f_j)$ if $S_i \subset S_j$ and $f_j|_{S_i} = f_i$. Now we apply Zorn's Lemma, and, as is often the case, the verification that every chain has an upper bound is immediate because we can just take the union over all elements of the chain. Therefore we get a maximal element (S, f).

Now, as for the case of the addition theorem, we need not have $S = T$; put $S' = T \setminus S$. What we *can* say is that $|S'| < |S|$. Indeed, otherwise we have $|S'| \geq |S|$, so that inside S' there is a subset S'' with $|S''| = |S|$. But we can enlarge $S \times S$ to $(S \cup S'') \times (S \cup S'')$. The bijection $f : S \to S \times S$ gives us that

$$|S''| = |S| = |S| \times |S| = |S''| \times |S''|.$$

Thus using the addition theorem, there is a bijection $g : S \cup S'' \to (S \cup S'') \times (S \cup S'')$ which can be chosen to extend $f : S \to S \times S$; this contradicts the maximality of

(S, f).

Thus we have that $|S'| < |S|$ as claimed. But then we have $|T| = |S \cup S'| = \max(|S|, |S'|) = |S|$, so

$$|T| \times |T| = |S| \times |S| = |S| = |T|,$$

completing the proof.

Exercise 2: Prove the analogue of Proposition 7 for cardinal division.

Exercise 3: Verify that $+$ and $\cdot$ are commutative and associative operations on cardinalities, and that multiplication distributes over addition. (There are two ways to do this. One is to use the fact that $|S| + |T| = |S| \cdot |T| = \max(|S|, |T|)$ unless S and T are both finite. On the other hand one can verify these identities directly in terms of identities on sets.)

1.4. **Cardinal exponentiation.** For two sets S and T, we define S^T to be the set of all functions $f : T \to S$. Why do we write S^T instead of T^S? Because the cardinality of the set of all functions from $[m]$ to $[n]$ is n^m: for each of the m elements of the domain, we must select one of the n elements of the codomain. As above, this extends immediately to infinite cardinalities:

Definition: $|S|^{|T|} := |S^T|$ (and again, it is no problem to see that this is well-defined).

Recall that in the first installment of the notes we proved that

$$(|X|^{|Y|})^{|Z|} = |X|^{|Y| \cdot |Z|}$$

by means of a canonical bijection between sets.

Exercise 4: Show that for any sets X, Y, Z we have

$$|X|^{|Y| + |Z|} = |X|^{|Y|} \cdot |X|^{|Z|}.$$
$$(|X| \times |Y|)^{|Z|} = |X|^{|Z|} \cdot |Y|^{|Z|}.$$

Thus all is well formally with this new operation: it has the same formal algebraic properties as the usual exponentiation. However, in stark contrast to addition and multiplication, the first fundamental theorem of set theory (Cantor's Theorem) ensures the nontriviality of cardinal exponentiation: for all sets S, $2^{|S|} > |S|$.

Cantor's Theorem guarantees that exponentiation of cardinalities is going to be more interesting than addition or multiplication: it asserts that for all S, $2^{|S|} > |S|$. As we observed in the first set of notes, $|\mathbb{R}| = 2^{|\mathbb{N}|}$. It is traditional to write c for $|\mathbb{R}|$ (c is for *continuum*).

What might one expect $2^{|S|}$ to be? The only canonical guess seems to be the minimalist one: since any collection of cardinalities is well-ordered, for any cardinality κ, there exists a smallest cardinality which is greater than κ, traditionally called κ^+. Thus perhaps we might expect that $2^{|S|} = |S|^+$ for all infinite S.

If we look at the case of finite sets, this makes us a little nervous, since 2^n is very

much larger than $n^+ = n + 1$. On the other hand, our simple formulas for addition and multiplication of infinite cardinalities do not hold for finite cardinalities either – in short, we have no real evidence so are simply guessing.

The problem seemingly becomes more concrete when we remember that $2^{|\mathbb{Z}^+|} = |\mathbb{R}| =: c$. So the above minimalist guess says that any infinite subset of $\mathbb{R}$ is either in bijection with $\mathbb{Z}^+$ or with $\mathbb{R}$ itself. This guess was made by Cantor, who was famously unable to prove it, despite much effort: it is now called Cantor's *Continuum Hypothesis* (CH). Moreover, the guess that $2^S = |S|^+$ for all infinite sets is called the *Generalized Continuum Hypothesis* (GCH).

Will anyone argue if I describe the continuum hypothesis (and its generalization) as the most vexing problem in all of mathematics? Starting with Cantor himself, some of the greatest mathematical minds have been brought to bear on this problem. For instance, in his old age David Hilbert claimed to have proved CH and he even published his paper in *Crelle*, but the proof was flawed. Kurt Gödel proved in 1944 that CH is relatively consistent with the ZFC axioms for set theory – in other words, assuming that the ZFC axioms are consistent (if not, all statements in the language can be formally derived from them!), it is not possible to deduce CH as a formal consequence of these axioms. In 1963, Paul Cohen showed that the negation of CH is also relatively consistent with ZFC, and for this he received the Fields Medal. Cohen's work undoubtedly revolutionized set theory, and his methods ("forcing") have since become an essential tool. But where does this leave the status of the Continuum Hypothesis?

The situation is most typically summarized by saying that Gödel and Cohen showed the undecidability of CH – i.e., that it is neither true nor false in the same way that Euclid's parallel postulate is neither true nor false. However, to accept this as the end of the story is to accept that what we know about sets and set theory is exactly what the ZFC axiom scheme tells us, but of course this is a position that would require (philosophical as well as mathematical) justification – as well as a position that seems to be severely undermined by the very issue at hand! Thus, a more honest admission of the status of CH would be: we are not even sure whether or not the problem is open. From a suitably Platonistic mathematical perspective – i.e., a belief that what is true in mathematics is different from what we are able (in practice, or even in principle) to prove – one feels that either there exists some infinite subset of $\mathbb{R}$ which is equivalent to neither $\mathbb{Z}^+$ nor $\mathbb{R}$, or there doesn't, and the fact that none of the ZFC axioms allow us to decide this simply means that the ZFC axioms are not really adequate. It is worth noting that this position was advocated by both Gödel and Cohen.

In recent years this position has begun to shift from a philosophical to a mathematical one: the additional axioms that will decide CH one way or another are no longer hypothetical. The only trouble is that they are themselves very complicated, and "intuitive" mostly to the set theorists that invent them. Remarkably – considering that the Axiom of Choice and GCH are to some extent cognate (and indeed GCH implies AC) – the consensus among experts seems to be settling towards *rejecting* CH in mathematics. Among notable proponents, we mention the

leading set theorist Hugh Woodin. His and other arguments are vastly beyond the scope of these notes.

To a certain extent, cardinal exponentiation reduces to the problem of computing the cardinality of 2^S. Indeed, one can show the following

Theorem 9. *If X has at least 2 elements and Y has at least one element then*

$$\max(|X|, 2^{|Y|}) \leq |X|^{|Y|} \leq \max(2^{|X|}, 2^{|Y|}).$$

We omit the proof for now.

1.5. **Note on sources.** Most of the material of this installment is due to Cantor, with the exception of the Schröder-Bernstein theorem (although Cantor was able to deduce the Second Fundamental Theorem from the fact that every set can be well-ordered, which we now know to be equivalent to the Axiom of Choice). Our proofs of Theorems 4 and 8 follow Kaplansky's *Set Theory and Metric Spaces*. Gödel's views on the Continuum Problem are laid out with his typical (enviable) clarity in *What Is Cantor's Continuum Problem?* It is interesting to remark that this paper was first written before Cohen's work – although a 1983 reprint in Benacerraf and Putnam's *Philosophy of Mathematics* contains a short appendix acknowledging Cohen – but the viewpoint that it expresses (anti-formalist, and favoring the negation of CH) is perhaps *more* accepted today than it was at the time of its writing.