PMATH 453/753

Primer on cardinal arithmetic

Definition/Notation. Let A, B be sets. We write

- $|A| \leq |B|$ if there is an injective map $f : A \to B$, and
- $|A| = |B|$ if there is a bijective map $f : A \to B$.

The equivalences classes of sets modulo the relation $|A| = |B|$ are called *cardinal numbers*.

Write $\aleph_0 = |\mathbb{N}|$ and $\boldsymbol{c} = |\mathbb{R}|$. We know $\aleph_0 < \boldsymbol{c}$ by Cantor's diagonal argument, i.e. $\aleph_0 \leq \boldsymbol{c}$ but $\boldsymbol{c} \not\leq \aleph_0$. Also, see (vi) and (vii) below.

Cantor-Bernstein-Schröder Theorem. $|A| \leq |B|$ and $|B| \leq |A|$ implies $|A| = |B|$.

Proof. See almost any book on real analysis. □

Continuum Hypothesis. There is no cardinal number $\aleph$ such that $\aleph_0 < \aleph < \boldsymbol{c}$.

Paul Cohen won the Fields medal for proving this is independent of ZFC axiom structure (the usual world analysits prefer to live in).

Cardinal arithmetic

Define

$$|A| + |B| = |A \sqcup B| \text{ (disjoint union)}, \quad |A||B| = |A \times B|.$$

It is easy to verify these operations are associative, commutative and there is even a distributive law: $|A|(|B|+|C|) = |A \times (B \sqcup C)| = |(A \times B) \sqcup (A \times C)| = |A||B| + |A||C|$. Note that with n copies of A we have $|A| + \cdots + |A| = |A \sqcup \cdots \sqcup A| = |\{1, \ldots, n\} \times A|$; we denote this cardinal $n|A|$. We let $A^B = \{f : B \to A \,|\, f \text{ is a function}\}$. We define

$$|A|^{|B|} = \left|A^B\right|.$$

Note that usual power rules apply: $(|A|^{|B|})^{|C|} = |(A^B)^C| = |A^{B \times C}| = |A|^{|B||C|}$ and $|A|^n = |A^{\{1,\ldots,n\}}| = |A \times \cdots \times A|$ (n times).

Exercises. (Try these yourself [with hints for the hard bits].)

(i) $|A| \geq \aleph_0 \iff$ there is $B \subsetneq A$ such that $|B| = |A|$. (We call these *infinite* cardinals. Finite cardinals – i.e. not infinite – will be identified with natural numbers; $|\varnothing| = 0$.)

(ii) A is infinite $\iff \aleph_0|A| = |A| \iff |A| = n|A|$ for each n in $\mathbb{N}$.
[Use a Zorn argument to show A can be partitioned into infinte countable sets. Manually show that $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$ to further partition each element of the partition into infinite countable sets.]

(iii) Given any two sets A, B either $|A| \leq |B|$ or $|B| \leq |A|$.
[Find a maximal pair (E, f) such that $E \subseteq A$ and $f : E \to B$ is injective, i.e. maximal w.r.t. $(E, f) \leq (E', f')$ iff $E \subseteq E'$ and $f'|_E = f$. Verify that either $|E| = |A|$ or $|E| = |B|$.] (We remark that if any two cardinals are comparable, then through an ordinal-arithmetic idea called "Hartog's number", it can be proved that any set A is well-orderable. Thus it is impossible to prove (iii) without A of C.)

(iv) A is infinite $\iff |A|^n = |A|$ for each n in $\mathbb{N}$.
[It suffices to show for $n = 2$ (why?). Find a maximal pair (B, f), $B \subseteq A$ and $f : B \to B \times B$ bijection, same partial ordering as in (iii) above. If $|B| < |A|$ then $|A \setminus B| = |A|$ (why?). There would be $B' \subset A \setminus B$ with $|B'| = |B|$ and one could construct $\tilde{f}$ for which $(B, f) \leq (B \cup B', \tilde{f})$, which violates assumptions on (B, f).]

(v) A is infinite $\iff |\mathcal{F}(A)| = |A|$, where $\mathcal{F}(A) = \{F \in \mathcal{P}(A) : |F| < \aleph_0\}$.
(This might be useful for proving $\dim \mathcal{X}$, $\mathcal{X}$ a vector space, is well-defined.)

(vi) $2^{\aleph_0} = |\mathcal{P}(\mathbb{N})| = \boldsymbol{c}$, $\boldsymbol{c}^{\aleph_0} = \boldsymbol{c}$, $\aleph_0^{\aleph_0} = \boldsymbol{c}$.
[For the first, identify indicator functions with sets where $2 = |\{0, 1\}|$, then write all elements in the open unit interval in binary form. The latter statements just use arithmetic rules and CBS.]

(vii) $2^{|A|} = |\mathcal{P}(A)| > |A|$ for any set A.
[Use a Cantor diagonalisation argument. Given any map $f : A \to \mathcal{P}(A)$, let $E_f = \{x \in A : x \in f(x)\}$. Only one of E_f of $A \setminus E_f$ is in the range of f, so no surjection is possible.]