Today:
  o Comparing the size of infinite sets, cont
  o Asymptotic notation

Announcements:
  o Dog day next Tuesday! BYOD.

Comparing infinite sets, continued

Review:

\(|A| \leq |B|\) if there exists an injection \(f : A \to B\).
\(|A| = |B|\) or \(A \sim B\), if there exists a bijection \(\pi : A \to B\). The sets are **equipotent**, **equicardinal**
\(|A| \neq |B|\) if \(\neg(\exists f : A \to B)\)
\(|A| < |B|\) if \(|A| \leq |B|\) but \(|A| \neq |B|\): there is an injection but no bijection from A to B.

A set is **finite** if it is empty or equipotent with \(\{1, \ldots, n\}\) for some natural number \(n\)
A set is **infinite** if it is not finite.
A set is **countably infinite** if it is equipotent with \(\mathbb{N}\).
Write \(|A| = \aleph_0\)
That symbol is called a **cardinal number**.
So the numbers you know about are 0, 1, 2, ..., \(\aleph_0\), \(\aleph\)

We showed last time that

Examples:
- \(\mathbb{N} \sim \mathbb{Z}\)
- \(\{0,1,\ldots\} \sim \{1,2,\ldots\}\) (hotel with countably many occupied rooms; a new customer arrives)
- \(\mathbb{N} \sim \{1,2\} \times \mathbb{N}\) (hotel with infinitely many occupied rooms; countably many new customer arrives)

Can also show
- \(\mathbb{N} \sim \mathbb{Q}\) : the rationals are countably infinite
- \(\mathbb{N} \sim \{0,1\}^*\) : the strings (over a fixed alphabet, say binary) are countably infinite

But we showed
- \(|\mathbb{N}| < |\mathbb{R}|\) : the reals are uncountable

Let's modify the proof a little to show that
- The number of languages (sets of strings over \(\{0,1\}\)) is uncountable

Give the standard diagonalization proof for this.
Important corollary:
**Cor**: there are languages that no computer program can recognize.
Theorem [Cantor] $|A| < |\mathcal{P}(A)|$

- Prove Cantor's theorem

**Proof of Cantor's theorem**, from Wikipedia [Cantor’s Theorem]: To establish Cantor’s theorem it is enough to show that, for any given set $A$, no function $f$ from $A$ into the power set of $A$, can be surjective, i.e. to show the existence of at least one subset of $A$ that is not an element of the image of $A$ under $f$. Such a subset is given by the following construction:

$$B = \{ x \in A : x \notin f(x) \}.$$

This means, by definition, that for all $x$ in $A$, $x \in B$ if and only if $x \notin f(x)$. For all $x$ the sets $B$ and $f(x)$ cannot be the same because $B$ was constructed from elements of $A$ whose images (under $f$) did not include themselves. More specifically, consider any $x \in A$, then either $x \in f(x)$ or $x \notin f(x)$. In the former case, $f(x)$ cannot equal $B$ because $x \in f(x)$ by assumption and $x \notin B$ by the construction of $B$. In the latter case, $f(x)$ cannot equal $B$ because $x \notin f(x)$ by assumption and $x \in B$ by the construction of $B$.

Thus there is no $x$ such that $f(x) = B$; in other words, $B$ is not in the image of $f$. Because $B$ is in the power set of $A$, the power set of $A$ has a greater cardinality than $A$ itself.

**Theorem** [Cantor-Bernstein-Schroeder] If $|A| \leq |B|$ and $|B| \leq |A|$ then $|A| = |B|$.

Many proofs, but not simple. I read the one on the Wikipedia page and thought it incoherent. I will leave this for when you take a set theory class … except we (UCD) don’t seem to have one.

**Wikipedia**: The continuum hypothesis (CH) states that there are no cardinals strictly between $\aleph_0$ and $2^{\aleph_0}$. The generalized continuum hypothesis (GCH) states that for every infinite set $X$, there are no cardinals strictly between $|X|$ and $2^{|X|}$. The continuum hypothesis is independent of the usual axioms of set theory, the Zermelo-Fraenkel axioms, together with the axiom of choice (ZFC).

**Leftover**

n! – factorial – didn’t mention

Review of properties of logs – $\lg$, $\log$, $\ln$.
Inverse of $2^x$, $10^x$, $e^x$ (exp)
$y \mapsto \ln(y)$ (the right notation for how to descript the action of a function. Note the kind of arrow.)

Also $\lambda$-notation: $f = \lambda x. \ln(x)$

$$f = \lambda x. x^2 + 1$$

$\log(ab) = \log(a) + \log(b)$
$\log_c(b) = \log_c(b) / \log_c(a)$
$s^a = (s^a)^b$
$a^x a^y = a^{x+y}$

Function composition

$f \circ g$
$f: A \to B, \ g: B \to C$

then $(g \circ f): A \to C$ is defined by
$(g \circ f)(x) = g(f(x))$

Kind of "backwards", but fairly tradition. Some mathematicians (eg, in algebra) will reverse it,
$(x) (f \circ g) \ "function operates on the left"

Comparing growth-rates of functions –Asymptotic notation and view

Motivate the notation. Will do big-$O$ and Theta.
http://en.wikipedia.org/wiki/Big_O_notation

$O(g) = \{ f: \mathbb{N} \to \mathbb{R}: \exists C, N \text{ s.t. } f(n) \leq C g(n) \text{ for all } n \geq N\}$

People often use “is” or “=” for “is a member of” or “is an anonymous element of”. I myself don't like this.

Reasons for asymptotic notation:
1. simplicity – makes arithmetic simple, makes analyses easier
2. When applied to running times: Works well, in practice, to get a feel for efficiency
3. When applied to running times: Facilitates greater model-independence

Reasons against:
1. Hidden constants can matter
2. Mail fail to care about things that one should care about
3. Not everything has an “n” value to grow

If $f \in O(n^2)$, $g \in O(n^2)$ the $f+g \in O(n^2)$
If $f \in O(n^2)$ and $g \in O(n^3)$ then $f+g \in O(n^3)$
If $f \in O(n \log n)$ and $g \in O(n)$ then $fg \in O(n^2 \log n)$
etc.
May write $O(f) + O(g)$, and other arithmetic operators

True/False:

If $f \in \Theta(n^2)$ then $f \in O(n^2)$ TRUE
(Truth: $n! = \Theta((n/e)^n \sqrt{n})$)
Discuss the runtime evaluation of a simple code fragment, eg,

```plaintext
for i = 1 to n do
    for j = 1 to 10*floor(i/3) do
        Constant time statement
```

Will do many more examples next week.