# MACM-300: Intro to Formal Languages and Automata

Anoop Sarkar – anoop@cs.sfu.ca

Cantor's Theorem. $|\mathcal{N}| < |P(\mathcal{N})|$.
Proof (by contradiction).
Note that *equivalent sets* have the same number of members. For *infinite* sets we show equivalence between two sets by providing a 1-1 mapping between elements from the two sets.
Note that it cannot be the case that $|\mathcal{N}| > |\mathcal{P}(\mathcal{N})|$ as $\mathcal{P}(\mathcal{N})$ includes the sets $\{1\}, \{2\}, \{3\}, \ldots$
So, if we show a contradiction for $|\mathcal{N}| = |P(\mathcal{N})|$ then we will have shown that $|\mathcal{N}| < |P(\mathcal{N})|$.
Assume that $|\mathcal{N}| = |P(\mathcal{N})|$, then there has to be a 1-1 mapping $F$ from $\mathcal{N}$ to $\mathcal{P}(\mathcal{N})$. So mapping $F$ is 1-1 from the set:

$$\mathcal{N} = \{1, 2, 3, \ldots\}$$

to the set:

$$\begin{array}{rll} \mathcal{P}(\mathcal{N}) = & \{ & \{\}, \\ & & \{1\}, \{2\}, \{3\}, \ldots, \\ & & \{1,2\}, \{1,3\}, \ldots, \\ & & \{2,3\}, \{2,4\}, \ldots, \\ & & \{3,4\}, \{3,5\}, \ldots, \\ & & \ldots \\ & & \{1,2,3\}, \{1,3,4\}, \ldots \\ & & \{2,3,4\}, \{2,4,5\}, \ldots \\ & & \ldots \\ & \} & \end{array}$$

The 1-1 mapping $F$ will look something like this:

$$\mathcal{N} \left\{ \begin{array}{lcl} 1 & \leftrightarrow & \{1\} \\ 2 & \leftrightarrow & \{2,3\} \\ 3 & \leftrightarrow & \{2,3,4\} \\ 4 & \leftrightarrow & \{2,3,4,5\} \\ 5 & \leftrightarrow & \{2,3,4,6\} \\ & \ldots & \end{array} \right\} \mathcal{P}(\mathcal{N})$$

Convince yourself that some numbers in $\mathcal{N}$ will be mapped to sets that contain that number, while others will not. The reason for this is that there are many subsets that contain each number $y$ in $\mathcal{N}$, so some of these subsets have to be mapped to a number in $\mathcal{N}$ that is not contained in that subset.

$$\mathcal{N} \left\{ \begin{array}{lcl} x_1 & \leftrightarrow & \{x_1, \ldots\} \\ x_2 & \leftrightarrow & \{\ldots, x_2, \ldots\} \\ x_3 & \leftrightarrow & \{\ldots, \ldots, x_3, \ldots\} \\ x_4 & \leftrightarrow & \{\ldots, \ldots, \ldots, x_4, \ldots\} \\ x_5 & \leftrightarrow & \{\ldots, \ldots, \ldots, \ldots, x_5, \ldots\} \\ & \ldots & \\ x_n & \leftrightarrow & \{\ldots, \ldots, \ldots, \ldots, \ldots, x_n\} \end{array} \right\} \mathcal{P}(\mathcal{N})$$

For the set $\{x_1, x_2, \ldots, x_n\}$ in $\mathcal{P}(\mathcal{N})$ we need to establish a mapping with some number, say $y$, which has to be distinct from the numbers $x_1, x_2, \ldots, x_n$ from $\mathcal{N}$. By definition, $y$ is not in the set $\{x_1, x_2, \ldots, x_n\}$ in $\mathcal{P}(\mathcal{N})$.

Let $B = \{x \in \mathcal{N} | x \notin F(x)\}$ which is the set of all numbers $x$ in $\mathcal{N}$ that are mapped to some set element $s_x$ in $\mathcal{P}(\mathcal{N})$ (a different $s_x$ for each $x$) such that $x$ is not a member of $s_x$.
But, $B$ **itself is a subset of** $\mathcal{N}$ and so must belong to $\mathcal{P}(\mathcal{N})$. By definition, $F$ is a 1-1 mapping so there must be a $y$ in $\mathcal{N}$ which maps to $B$.
But this leads to two possible contradictions:

- either $y \in B$ but in this case, $y \in \mathcal{N}$ maps to $B \in \mathcal{P}(\mathcal{N})$ and $B$ includes $y$, which violates the definition of $B$ above,
- or $y \notin B$ but then since we have a mapping from $y \in \mathcal{N}$ to $B$, and $y$ is not in $B$ this is an example of a mapping from $y$ to a set which does not include it, and so by definition of $B$, $y$ should be in $B$.

Therefore, we can conclude that $|\mathcal{N}| < |\mathcal{P}(\mathcal{N})|$