# Lecture 1
# Background: Discrete mathematical structures: Sets

MIEFis - Quantum Computation, L. S. Barbosa, 2020-21

**Summary**
(1) Sets, functions, relations.
(2) Isomorphism and cardinality.

---

## Sets, relations, functions

(recall your HASKELL experience)

- Function $f : A \longrightarrow B$. Composition.
- Notation $A^B$ to represent the space of functions from $A$ to $B$.
- Injective, surjective and bijective functions.
- Set. Cardinality. Powerset ($\mathcal{P}(A)$ or $\mathbf{2}^A$).
- Binary relations; $\mathbf{2}^{A\times B} \cong \mathbf{2}^{A^B}$.
- Equivalence relations. Partition. Quotient set as a partition.

## Finite and infinite sets

- equicardinality *vs* isomorphism.
- finite *vs* infinite.
- countable *vs* uncountable:
  A set $A$ is *countable* iff there is an injective function $f : A \longrightarrow \mathbb{N}$.
  It is *infinite countable* if $f$ is a bijection.

## Ranking cardinality

$$|A| \leq |B| \;\text{ iff }\; \text{there is an injection } f : A \longrightarrow B$$

Relation $\leq$ above is a total order. Note that proving antisymmetry (i.e. the Cantor-Bernstein-Schroeder theorem) and totality (which requires the axiom of choice) is extremely hard.

Some applications:

**Theorem**

$\mathbb{N}$ and $\mathbb{Z}$ have the same cardinal

**Proof (hint).**
Consider $h : \mathbb{Z} \longrightarrow \mathbb{N}$ defined as follows and show it is a bijection

$$h(x) \;=\; \begin{cases} 2x & \Longleftarrow x \geq 0 \\ -2x+1 & \Longleftarrow \text{otherwise} \end{cases}$$

□

**Theorem**

$\mathbb{N}$ and $\mathbb{N} \times \mathbb{N}$ have the same cardinal

Look for a bijection between $\mathbb{N}$ and $\mathbb{N} \times \mathbb{N}$. Let's see some (of several) possibilities:

**Proof (1).**
Enumerate all pairs of numbers which sum $0, 1, 2, \cdots$:

$$\begin{array}{lllll} (0,0) & & & & \\ (0,1) & (1,0) & & & \\ (0,2) & (1,1) & (2,0) & & \\ (0,3) & (1,2) & (2,1) & (3,0) & \cdots \\ \quad\vdots & & & & \end{array}$$

For every sum $n$ there are only finitely many, actually $n+1$ pais $(i, j)$ that sum $n$. I.e. for every number $n$, one gets all the pairs which sum $n$. On the other hand, since every pair of numbers $(i, j)$ has a finite sum it will appear somewhere on this list. This defines a bijection

$$\begin{array}{rcl} (0,0) & \mapsto & 0 \\ (0,1) & \mapsto & 1 \\ (1,0) & \mapsto & 2 \\ (0,2) & \mapsto & 3 \\ (1,1) & \mapsto & 4 \\ & \cdots\cdots & \end{array}$$

□

**Proof (2).**

Consider the following correspondence:

$$n \;\mapsto\; (i, j)$$

such that $n = 2i + j$ (i.e. basically factoring number $n$ in its odd and even parts). Clearly the pair $(i, j)$ is unique, thus establishing a bijection

$$f : \mathbb{N} \longrightarrow \mathbb{N} \times \mathbb{N}_{\text{odd}}$$

Remains to prove that $\mathbb{N} \cong \mathbb{N}_{\mathtt{odd}}$.

□

**Theorem**

The union of a finite number of countably infinite sets is countably infinite.

**Proof (hint).**

$$\begin{tikzcd}
X & x_0 \arrow[d] & x_1 \arrow[d] & x_3 \arrow[d] & \cdots \\
Y & y_0 \arrow[d] & y_1 \arrow[d] & y_3 \arrow[d] & \cdots \\
Z & z_0 \arrow[uur] & z_1 \arrow[uur] & z_3 \arrow[uur] & \cdots
\end{tikzcd}$$

□

**Theorem**

$|\mathbb{N}| < |\mathbb{R}|$

**Proof.**
To show that $|\mathbb{N}| \leq |\mathbb{R}|$ is trivial: function $h(n) = n$ is injective.

The difficult part is to prove that $\mathbb{N} \neq \mathbb{R}$. Let us prove an even stronger statement: that there is no surjection from $\mathbb{N}$ to $[0, 1[$. Consider an arbitrary function $h : \mathbb{N} \longrightarrow [0, 1[$ with which one may enumerate an infinite sequence of real numbers

$$r_0, r_1, r_2, \cdots$$

making $r_i = h(i)$.

To show that $h$ in not surjective, we have to find a real $x$ such that $r_n \neq x$ for all $n \in \mathbb{N}$. Let us build $x$ as an infinite dizime

$$0.x[0]x[1]x[2]\cdots$$

such that

$$x[i] \;=\; \begin{cases} 1 \;\Leftarrow\; r_i[i] = 0 \\ 0 \;\Leftarrow\; \text{otherwise} \end{cases}$$

Observe that any real $h(n)$ differs from number $x$ exactly in position $n$, and conclude that $x$ does not belong to the image of $h$.

□

**Theorem**

$\mathbf{2}^{\mathbb{N}}$ is uncountable.

**Proof.**
If this is not the case, and $\mathbf{2}^{\mathbb{N}}$ is countably infinite, there is an enumeration of sets such that

$$\mathbf{2}^{\mathbb{N}} = \{R_1, R_2, \cdots\}$$

Let $D = \{n \in \mathbb{N} \mid n \notin R_n\}$. Set D is a set of natural numbers and thus should appear somewhere in the enumeration $R_1, R_2, \cdots$. Suppose $D = R_j$ for some value $j$. Does $j \in R_j$? If yes, by definition of D, $j \notin D$, which contradicts $D = R_j$. If, alternatively, $j \notin R_j$ then $j \in D$ which is again a contradiction.

□

Exercise (Cantor Theorem)

Generalise the previous proof to show that, for any set X, $|X| < |\mathbf{2}^X|$.

**Proof (Cantor Theorem).**

Function

$$\eta : x \longrightarrow \{x\}$$

is trivially injective. However there is no surjection $h : X \longrightarrow \mathbf{2}^X$.

To argue by contradiction, suppose such a function $h$ exists and consider a set

$$W = \{x \in X \mid x \notin h(x)\}$$

If $h$ is indeed surjective it must exist an element $w \in X$ such that $h(w) = W$ and $w$ may or may not belong to $h(w)$.
These two cases are as follows as both lead to a contradiction:

- $w \in h(w)$ but then $w \notin W$,
- $w \notin h(w)$ but then $w \in W$

which invalidates our assumption that $h$ is a surjection.

□

**Remark (problems and algorithms).** This theorem sheds light on the limits of computability: *there are more problems that we might want to solve than there are programs to solve them, even though both are infinite*.

To see this, restrict your attention to one type of problem: deciding whether a string has some property (e.g. having even length, being a palindrome, or a legal Haskell program). A property can be identified with the set of strings that happen to share it. Clearly, the number of possible programs is no bigger than the number of strings, while the number of sets of strings is strictly greater.

This shows the existence of unsolvable problems, i.e. problems that can be formulated but not possibly solved.

**Theorem: the pigeonhole principle**

Let $m$ objects be distributed into $n$ containers. If $m > n$, then some container contains at least two objects

**Proof.**
By contrapositive: let us show that if every container contains at most one object, then $m \leq n$.

If $c_i$ is the number of objects in container $i$, then

$$m = \sum_{i=1}^{n} c_i$$

but, every container contains at most one object, we get

$$m = \sum_{i=1}^{n} c_i \leq \sum_{i=1}^{n} 1 = n$$

□

**Applications**: Given a large enough number of objects with a bounded number of properties, eventually at least two of them will share a property.

Ex. 1

Suppose that every point in the real plane is coloured either red or blue. Then for any distance $d > 0$, there are two points exactly distance d from one another that are the same color.

Ex. 2

Similarly, there are at least 2 Portuguese citizens with exactly the same number of individual hair in their heeads.

Ex. 3

For any natural number $n$, there is a nonzero multiple of n whose digits are all 0s and 1s.

**Remark (non constructive proofs).**

The proofs applying the pigeonhole proofs are non-constructive, i.e. although they prove the existence of something, they fail to provide an explicit example that proves the theorem. Constructive proofs are the ones more suitable for Computer Science (why?).

This may be illustrated with two proofs of the following result:

**Theorem: There exist irrational numbers $x$ and $y$ for which $x^y$ is rational**

**Proof (non-constructive).**
Let $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$. Number $y$ is irrational, but we do not know whether $x$ is rational or irrational. Thus,

- If $x$ is irrational, then we have an irrational number to an irrational power that is rational:

$$x^y \;=\; (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} \;=\; \sqrt{2}^{(\sqrt{2}\times\sqrt{2})} \;=\; \sqrt{2}^{2} \;=\; 2$$

- If $x$ is rational, then

$$y^y \;=\; x$$

  is rational. Either way, we conclude that there is an example of a power of irrational numbers tthat is rational.

□