Discrete Mathematics

Lecture 19.

{images, families, diagonalisation,
well-foundedness}

Images

Let $R: A \nrightarrow B$.

Def. The 'direct image' of a subset $X \subseteq A$ under R is the subset $R_* X \subseteq B$ defined below:

$R_*: P(A) \to P(B)$

$\vec{R}$

$$R_* X = \{b \in B \mid \exists x \in X.\ x \, R \, b\} = \{b \in B \mid \exists x \in A.\ xRb \wedge x \in X\}$$

Def. The 'inverse image' of $Y \subseteq B$ is $R^* Y \subseteq A$

$\Big\{ R^*: P(B) \to P(A)$

$$R^* Y = \{a \in A \mid \forall b \in B.\ a \, R \, b \Rightarrow b \in Y\}$$

If $f: A \to B$, then $f^*\{x\}$ for $x \in B$ is $\{a \in A \mid f(a) = x\}$.

$$f^*\{x\} = \{a \in A \mid \forall b \in B.\ a \, f \, b \Rightarrow b \in \{x\}\}$$
$$= \{a \in A \mid f(a) \in \{x\}\}$$
$$= \{a \in A \mid f(a) = x\} \quad ■$$

Def. A family of sets indexed in a set I is:

A set S together with a function $\pi_S : S \to I$.

Notation: Let S be a family ix'd in I.

For $i \in I$, define S_i to be $\{s \in S \mid \pi_S(s) = i\} = \pi_S^*\{i\}$

$$\Rightarrow \quad \biguplus_{i \in I} S_i = S.$$

Theorem. Let I be enumerable ($\exists e_I : \mathbb{N} \twoheadrightarrow I$), and let A be a family of enumerable sets indexed in I

$$\left(\text{i.e. } \forall i \in I.\ \exists e_i : \mathbb{N} \twoheadrightarrow \underset{\pi_A^*\{i\}}{\underset{\parallel}{A_i}}\right).$$

$\forall x \in X, \exists y \in Y.\ P(x,y)$

$\Downarrow$ A.C.

$\exists f : X \to Y.\ \forall x \in X.\ P(x, f(x))$.

Then the disjoint union $A = \biguplus_{i \in I} A_i$ is enumerable.

Proof. We have $e_I : \mathbb{N} \twoheadrightarrow I$. For every $i \in I$, there exists an enumeration $\mathbb{N} \twoheadrightarrow A_i$. By choice, we have an assignment $f_i : \mathbb{N} \twoheadrightarrow A_i$ for each $i \in I$.

$k : \mathbb{N} \times \mathbb{N} \twoheadrightarrow A$

$k(m,n) = f_{e_I(m)}(n)$

k is surj. Fix $a \in A$. Need (m,n) s.t. $k(m,n) = a$.
Let $i := \pi_A(a)$; b/c e_I surj., have $m \in \mathbb{N}$ s.t. $e_I(m) = i = \pi_A(a)$.
B/c $f_{\pi_A(a)}$ is surjection, we have $n \in \mathbb{N}$ s.t. $f_{\pi_A(a)}(n) = a$.

$k(m,n) = f_{e_I(m)}(n) = f_{\pi_A(a)}(n) = a$.

Choose any $h : \mathbb{N} \twoheadrightarrow \mathbb{N} \times \mathbb{N}$.
$k \circ h : \mathbb{N} \twoheadrightarrow A$. ∎

Thm. (Cantor). There can be no surjection $A \twoheadrightarrow P(A)$.

Proof. Assume we have $e : A \twoheadrightarrow P(A)$.

Define $U \in P(A)$

$$U = \{x \in A \mid x \notin e(x)\}$$

B/c $e : A \twoheadrightarrow P(A)$, we may find some $a \in A$ s.t. $e(a) = U$.

$\Downarrow$ For all $x \in A$, $\quad x \in e(a) \iff x \in U \iff x \notin e(x)$.

If we consider $x = a$. Have $\quad a \in e(a) \iff a \notin e(a)$.

Contradiction!! $\blacksquare$

Def. A <u>fixed point</u> of a function $f: X \to X$ is an element $x \in X$ s.t. $f(x) = x$. ("f fixes x").

<u>**Theorem.**</u> (<u>Lawvere</u>)

Given a set A and a set X, if there exists a surjection $A \twoheadrightarrow (A \Rightarrow X)$, then every function $X \to X$ has a fixed point.

<u>**Proof.**</u> Let $e: A \twoheadrightarrow (A \Rightarrow X)$. Let $f: X \to X$ be a function. Define $h: A \to X$ by

$$h(a) = f\big(\underbrace{e(a)(a)}_{\in X}\big)$$

B/c e is surjective, have $a_h \in A$ s.t. $e(a_h) = h$

$$e(a_h)(a_h) \in X \qquad \text{is a fixed point of } f: X \to X.$$

$$e(a_h) = h$$

$$e(a_h)(a_h) = h(a_h) = f(e(a_h)(a_h))$$

$\boxtimes$

Thm. A set X satisfies $(\forall f: X \to X.\ f \text{ has f.p.})$
iff $\# X = 1$.

$\# X \geq 1$. (B/c $1_X: X \to X$ has f.p.)

Now $\overset{\text{spse}}{}$ $x_0 \neq x_1$ to obtain contradiction.

Define $f: X \to X$
$f x_0 = x_1$
$f(y \neq x_0) = x_0$

Let $p \in X$ be a f.p. of f.
1) If $p = x_0$, then
$f(p) = x_1$, $f(p) = p$ $\Rightarrow$ $x_1 = p$. Boom!
2) If $p \neq x_0$, then $f(p) = x_0$ and $f(p) = p$.
Boom!

∎

Cantor via Lawvere

$$A \twoheadrightarrow P(A).$$

$$\iff \quad A \twoheadrightarrow (A \Rightarrow [2])$$

$$\Big\Downarrow \text{ Lawvere}$$

$[2]$ is a singleton

(Bang!)

$\mathbb{R}$ is not enumerable

$$\mathbb{R} \cong [0,1] \cong (\mathbb{N} \to [2]) \cong P(\mathbb{N}).$$

Complete Induction

To prove $\forall n \in \mathbb{N}. P(n)$, suff to prove

$$\forall n \in \mathbb{N}. \ (\forall m < n. \ P(m)) \to P(n).$$

Let $R : A \leftrightarrow A$. R is "well-founded" when:

for any $P \subseteq A$.

$$(\forall a \in A. \ a \in P) \iff \Big(\forall a \in A. \ (\forall b \in A. \ b \ R \ a \Rightarrow b \in P) \Rightarrow a \in P \Big).$$