Notation $f : A \cong B : g \iff f : A \to B,\ g : B \to A$
$f \circ g = id_B \wedge g \circ f = id_A$.
$(g = f^{-1} \wedge f = g^{-1})$.

Calculus of bijections

- $id_A : A \cong A : id_A$, $f : A \cong B : g \implies g : B \cong A : f$, $(f : A \cong B : g \wedge p : B \cong C : q) \implies p \circ f : A \cong C : g \circ q$
- If $A \cong X$ and $B \cong Y$ then

$$\mathcal{P}(A) \cong \mathcal{P}(X) \quad , \quad A \times B \cong X \times Y \quad , \quad A \uplus B \cong X \uplus Y \quad ,$$

$$\mathrm{Rel}(A, B) \cong \mathrm{Rel}(X, Y) \quad , \quad (A \rightharpoonup B) \cong (X \rightharpoonup Y) \quad ,$$

$$(A \Rightarrow B) \cong (X \Rightarrow Y) \quad , \quad \mathrm{Bij}(A, B) \cong \mathrm{Bij}(X, Y)$$

$$f : A \cong X : g \qquad p : B \cong Y : q$$

$$(A \Rightarrow B) \cong (X \Rightarrow Y)$$

$$F : (A \Rightarrow B) \to (X \Rightarrow Y)$$

$$F : A \xrightarrow{\varphi} B \longmapsto p \circ \varphi \circ g : X \to Y$$

$$G : (X \Rightarrow Y) \to (A \Rightarrow B)$$

$$G : X \xrightarrow{\gamma} Y \longmapsto q \circ \gamma \circ f : A \to B$$

<u>RTP</u> : $F \circ G = \mathrm{id}$ and $G \circ F = \mathrm{id}$.

$\boxtimes$

Arithmetic Laws

Recall that for finite sets A and B,

$\#(A \times B) = \#(A) \cdot \#(B)$ multiplication

$\#(A \uplus B) = \#(A) + \#(B)$ addition

$\#(A \Rightarrow B) = (\#B)^{\#(A)}$ exponentiation

- The arithmetic laws have set-theoretic counterparts

Eg: $(a+b) \cdot c = a \cdot c + b \cdot c$ $\quad (A \uplus B) \times C \cong (A \uplus C) \times (B \uplus C)$

$$A \uplus B = (\{0\} \times A) \cup (\{1\} \times B)$$

$$(x,y) \in (A \uplus B) \times C \longmapsto \begin{cases} (0,(a,y)) , & x = (0,a) \quad a \in A \\ (1,(b,y)) , & x = (1,b) \quad b \in B \end{cases}$$

- $A \cong [1] \times A \ , \ (A \times B) \times C \cong A \times (B \times C) \ , \ A \times B \cong B \times A$
- $[0] \uplus A \cong A \ , \ (A \uplus B) \uplus C \cong A \uplus (B \uplus C) \ , \ A \uplus B \cong B \uplus A$
- $[0] \times A \cong [0] \ , \ \boxed{(A \uplus B) \times C \cong (A \times C) \uplus (B \times C)}$
- $(A \Rightarrow [1]) \cong [1] \ , \ (A \Rightarrow (B \times C)) \cong (A \Rightarrow B) \times (A \Rightarrow C)$
- $([0] \Rightarrow A) \cong [1] \ , \ ((A \uplus B) \Rightarrow C) \cong (A \Rightarrow C) \times (B \Rightarrow C)$
- $([1] \Rightarrow A) \cong A \ , \ ((A \times B) \Rightarrow C) \cong (A \Rightarrow (B \Rightarrow C))$
- $(A \rightharpoonup B) \cong (A \Rightarrow (B \uplus [1]))$
- $\mathcal{P}(A) \cong (A \Rightarrow [2])$

Arithmetic-like Bijections

$$(A \uplus B) \times C \cong (A \times C) \uplus (B \times C)$$

__Proposition__ Let X, Y, Z be sets.
If X and Y are disjoint then

(i) $X \times Z$ and $Y \times Z$ are disjoint

(ii) $(X \cup Y) \times Z \cong (X \times Z) \cup (Y \times Z)$

$$c^{a \cdot b} = (c^b)^a$$

$$((A \times B) \Rightarrow C) \cong (A \Rightarrow (B \Rightarrow C))$$

In OCaml notation:

<u>curry</u>$(f) =$ fun $a \to$ fun $b \to f(a, b)$

of type $(\alpha * \beta \to \gamma) \to (\alpha \to \beta \to \gamma)$

<u>uncurry</u>$(h) =$ <u>fun</u> $(a, b) \to h\ a\ b$

of type $(\alpha \to \beta \to \gamma) \to (\alpha * \beta \to \gamma)$

Exercise: Show that <u>curry</u> and <u>uncurry</u> are inverses of each other.

Characteristic (or indicator) functions

$$\mathcal{P}(\mathbf{A}) \cong (\mathbf{A} \Rightarrow [2])$$

notation

$f(S) = \chi_S$

$$f : \mathcal{P}(A) \longrightarrow (A \Rightarrow [2])$$

$$S \subseteq A \longmapsto f(S) : A \to [2] :$$

$$\text{def } f(S)(a) = \begin{cases} 0 & a \notin S \\ 1 & a \in S \end{cases}$$

$$g : (A \Rightarrow [2]) \longrightarrow \mathcal{P}(A)$$

$$A \xrightarrow{h} [2] \longmapsto g(h) = \{ a \in A \mid h(a) = 1 \}$$

$\boxtimes$

<u>Example</u>

$$([m]\times[n] \Rightarrow [2]) \cong \mathcal{P}([m]\times[n])$$

$$\mathcal{P}([m]\times[n]) = \underline{Rel}([m],[n]).$$

boolean $(m \times n)$-matrices.

Finite cardinality

Definition 136 *A set A is said to be* finite *whenever $A \cong [n]$ for some $n \in \mathbb{N}$, in which case we write $\#A = n$.*

Theorem 137 *For all* $m, n \in \mathbb{N}$,

1. $\mathcal{P}\big([n]\big) \cong [2^n]$
2. $[m] \times [n] \cong [m \cdot n]$
3. $[m] \uplus [n] \cong [m + n]$
4. $\big([m] \rightharpoonup [n]\big) \cong \big[(n+1)^m\big]$
5. $\big([m] \Rightarrow [n]\big) \cong [n^m]$
6. $\mathrm{Bij}\big([n], [n]\big) \cong [n!]$

For $m, n \in \mathbb{N}$

(i) $[m] \times [n] \cong [m \cdot n]$

(ii) $[m] \uplus [n] \cong [m+n]$

(i) Consider

$$[m] \times [n] \longrightarrow [m \cdot n]$$
$$(q, r) \longmapsto q \cdot n + r$$

and show it is a bijection

(ii) Consider

$$\begin{aligned}
[m] \uplus [n] &\longrightarrow [m+n] \\
(0,i) &\longmapsto i \\
(1,j) &\longmapsto m+j
\end{aligned}$$

and show it is a bijection.

$$\forall m \in \mathbb{N}.\ \forall n \in \mathbb{N}.\ ([m] \Rightarrow [n]) \cong [\cancel{m^n}\, n^m]$$

By induction:

<u>$m=0$</u>: $([0] \Rightarrow [n]) \overset{?}{\cong} [n^0] = [1]$

$x^0 = 1$ ...

There is a unique function from $\emptyset$ to any other set; namely the empty relation.

<u>$m=k+1$</u>. $[k] \Rightarrow [n] \cong [n^k]$

<u>RTP</u> $[k+1] \Rightarrow [n] \overset{?}{\cong} [n^{k+1}]$

$$[k+1] \Rightarrow [n] \cong [n^{k+1}]$$

$$c^{a+b} = c^a \cdot c^b$$

$$([k+1] \Rightarrow [n]) \cong ([k] \uplus [1]) \Rightarrow [n]$$

$$\cong ([k] \Rightarrow [n]) \times ([1] \Rightarrow [n])$$

$$a^1 = a$$

$$\cong [n^k] \times [n]$$

$$\cong [n^k \cdot n]$$

$$= [n^{k+1}]$$

$\boxtimes$

Infinity axiom

$\boxed{\text{There is an infinite set, containing } \emptyset \text{ and closed under successor.}}$

Bijections

Proposition 138 *For a function $f : A \to B$, the following are equivalent.*

1. f *is bijective.*

2. $\forall\, b \in B.\, \exists!\, a \in A.\, f(a) = b$.

3. $$\big(\forall\, b \in B.\, \exists\, a \in A.\, f(a) = b\big) \quad \text{surjection}$$
   $$\wedge$$
   $$\big(\forall\, a_1, a_2 \in A.\, f(a_1) = f(a_2) \implies a_1 = a_2\big) \quad \text{injection.}$$

Surjections

Definition 139 *A function* $f : A \longrightarrow B$ *is said to be* <u>surjective</u>*, or a* <u>surjection</u>*, and indicated* $f : A \twoheadrightarrow B$ *whenever*

$$\forall\, b \in B.\, \exists\, a \in A.\, f(a) = b \quad .$$

Theorem 140 *The identity function is a surjection, and the composition of surjections yields a surjection.*

The set of surjections from A to B is denoted

$$\mathrm{Sur}(A, B)$$

and we thus have

$$\mathrm{Bij}(A, B) \subseteq \mathrm{Sur}(A, B) \subseteq \mathrm{Fun}(A, B) \subseteq \mathrm{PFun}(A, B) \subseteq \mathrm{Rel}(A, B) \ .$$

Enumerability

Definition 142

1. *A set A is said to be* enumerable *whenever there exists a surjection $\mathbb{N} \overset{e}{\twoheadrightarrow} A$, referred to as an* enumeration.

2. *A* countable *set is one that is either empty or enumerable.*

$e(0), e(1), e(2), \ldots, e(n), \ldots$

$n \in \mathbb{N}$

$$\mathbb{N} \overset{e}{\twoheadrightarrow} \mathbb{Z}$$

Examples:

1. A bijective enumeration of $\mathbb{Z}$.

	$\cdots$	-3	-2	-1	0	1	2	3	$\cdots$
e:	$\cdots$	$\uparrow$ 6	$\uparrow$ 4	$\uparrow$ 2	$\uparrow$ 0	$\uparrow$ 1	$\uparrow$ 3	$\uparrow$ 5	$\cdots$

$$\mathbb{N}\times\mathbb{N} \xrightarrow{\cong} \mathbb{N}^+ \xrightarrow{\cong} \mathbb{N}$$

$$(m, n) \longmapsto 2^m\cdot(2n+1)$$

2. A bijective enumeration of $\mathbb{N}\times\mathbb{N}$.

	0	1	2	3	4	5	$\cdots$
0	0	1	3	6			
1	2	4	7				
2	5	8					
3	9						
4							
$\vdots$							

Proposition 143 *Every non-empty subset of an enumerable set is enumerable.*

PROOF:

$$\begin{tikzcd} \mathbb{N} \arrow[r, two heads, "e"] \arrow[dr, two heads, "e'"'] & A \\ & S \ni a \arrow[u, phantom, "\rotatebox[origin=c]{90}{$\subseteq$}"] \end{tikzcd}$$

$$e'(n) = \begin{cases} e(n) & , e(n) \in S \\ a & , \text{otw.} \end{cases}$$

$\boxtimes$

Countability

Proposition 144

1. *$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ are countable sets.*
2. *The product and disjoint union of countable sets is countable.*
3. *Every finite set is countable.*
4. *Every subset of a countable set is countable.*

Proposition: The product of enumerable sets is enumerable.

$$\mathbb{N} \xrightarrow{e_1} A_1$$

$$\mathbb{N} \xrightarrow{e_2} A_2$$

$$\begin{tikzcd} \mathbb{N} \arrow[r, two heads] \arrow[rr, bend left, two heads, "e"] & \mathbb{N}\times\mathbb{N} \arrow[r, two heads] & A_1 \times A_2 \\ & (n,m) \arrow[r, mapsto] & (e_1(n), e_2(m)) \end{tikzcd}$$

Corollary: $\mathbb{Q}$ is enumerable.

$$\begin{tikzcd}
\mathbb{N} \arrow[r, two heads] \arrow[rr, bend left] & \mathbb{Z} \times \mathbb{N}^+ \arrow[r, two heads] & \mathbb{Q} \\
& p, q \arrow[r, mapsto] & p/q
\end{tikzcd}$$