Discrete Mathematics

Lecture 17.

[bijections, indicators, finite & infinite cardinality]

2024-01-29

$f : A \to B$ bijection $\iff \exists^{(!)} f^{-1} : B \to A .\ f \circ f^{-1} = id \wedge f^{-1} \circ f = id$

$(A \cong B) \iff \exists f : A \to B .\ f$ is a bijection.

"A isomorphic to B"

1) Reflexivity: $A \cong A$.

B/c $id_A : A \to A$ is a bijection

2) Transitivity: $A \cong B \wedge B \cong C \implies A \cong C$

B/c if $f : A \to B$ bij. and $g : B \to C$ bij.

$g \circ f : A \to C$ bij.

"closure of bijections under identity & composition"

3) Symmetry: $A \cong B \Rightarrow B \cong A$.

B/c $f : A \to B$ bij., $f^{-1} : B \to A$ is bij. ☒

Calculus of bijections

- $\checkmark$ $A \cong A$, $A \cong B \implies B \cong A$, $(A \cong B \wedge B \cong C) \implies A \cong C$
- If $A \cong X$ and $B \cong Y$ then

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

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

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

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

Suppose $A \cong X \wedge B \cong Y$

Then $\mathrm{Rel}(A,B) \cong \mathrm{Rel}(X,Y)$.

Proof. Let $f : A \to X$ and $g : B \to Y$ be bijections.

We will define a bijection $H : \mathrm{Rel}(A,B) \to \mathrm{Rel}(X,Y)$.

To define H, we fix $R : A \nrightarrow B$ to specify $H(R) : X \nrightarrow Y$.

$$
\begin{tikzcd}
X \arrow[rr, "H(R)", "|" marking] \arrow[d, "f^{-1}"', "|" marking] & & Y \\
A \arrow[r, "R"', "|" marking] & B \arrow[ur, "g"', "|" marking] &
\end{tikzcd}
$$

i.e., $H(R) := g \circ R \circ f^{-1}$.

$H^{-1} : \mathrm{Rel}(X,Y) \to \mathrm{Rel}(A,B)$

$$
H^{-1}(S : X \nrightarrow Y) := \left(
\begin{tikzcd}
A \arrow[rr, "H^{-1}(S)", "|" marking] \arrow[d, "f"', "|" marking] & & B \\
X \arrow[r, "S"', "|" marking] & Y \arrow[ur, "g^{-1}"', "|" marking] &
\end{tikzcd}
\right)
$$

i.e. $H^{-1}(S) := g^{-1} \circ S \circ f$.

$$
\begin{aligned}
H^{-1}(H(R)) &= g^{-1} \circ H(R) \circ f \\
&= g^{-1} \circ (g \circ R \circ f^{-1}) \circ f \\
&= (g^{-1} \circ g) \circ R \circ (f^{-1} \circ f) \\
&= id \circ R \circ id \\
&= R
\end{aligned}
$$

$$
\begin{aligned}
H(H^{-1}(S)) &= g \circ H^{-1}(S) \circ f^{-1} \\
&= g \circ (g^{-1} \circ S \circ f) \circ f^{-1} \\
&= (g \circ g^{-1}) \circ S \circ (f \circ f^{-1}) \\
&= id \circ S \circ id \\
&= S.
\end{aligned}
$$

$\boxtimes$

Def. A *predicate* on a set A is defined to be a function $\varphi : A \to [2]$.

We say "φ holds of $a \in A$" when $\varphi(a) = 1$.

Def. The *indicator function* (a.k.a. "characteristic function") of a subset $S \subseteq A$ is the predicate $\chi_S : A \to [2]$ defined by

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

Def. The *comprehension* of a predicate $\varphi : A \to [2]$ is the subset $[\varphi] \subseteq A$ defined as:

$$[\varphi] = \{ a \in A \mid \varphi(a) = 1 \}.$$

__Theorem.__ The mappings $\chi_{(-)} : \mathcal{P}(A) \longrightarrow (A \Rightarrow [2])$ and $[-] : (A \Rightarrow [2]) \to \mathcal{P}(A)$ are mutually inverse.

__Proof.__ Fix $S \subseteq A$,

$$
\begin{aligned}
[\chi_S] &= \{a \in A \mid \chi_S(a) = 1\} \\
&= \{a \in A \mid a \in S\} \\
&= S
\end{aligned}
$$

Fix $\varphi : A \to [2]$.

$$
\begin{aligned}
\chi_{[\varphi]}(a) &= \begin{cases} 1 & \text{when } a \in [\varphi] \\ 0 & \text{when } a \notin [\varphi] \end{cases} \\
&= \begin{cases} 1 & \text{when } \varphi(a) = 1 \\ 0 & \text{when } \underbrace{\varphi(a) \neq 1}_{\varphi(a) = 0} \end{cases} \\
&= \varphi(a)
\end{aligned}
$$

$\blacksquare$

Characteristic (or indicator) functions

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

Lemma.

$$\mathcal{P}(X \uplus [1]) \cong \mathcal{P}(X) \uplus \mathcal{P}(X)$$

$$\cong$$

$$(X \uplus [1]) \Rightarrow [2]$$

$$\cong$$

$$(X \Rightarrow [2]) \times ([1] \Rightarrow [2])$$

$$\cong$$

$$\begin{aligned}
\mathcal{P}(X) \times [2] &\cong \mathcal{P}(X) \times ([1] \uplus [1]) \\
&\cong (\mathcal{P}(X) \times [1]) \uplus (\mathcal{P}(X) \times [1]) \\
&\cong \mathcal{P}(X) \uplus \mathcal{P}(X) \qquad \square
\end{aligned}$$

Finite cardinality

Definition 160 *A set A is said to be* finite *whenever $A \cong [n]$ for some $n \in \mathbb{N}$, in which case we write $\#A = n$.*

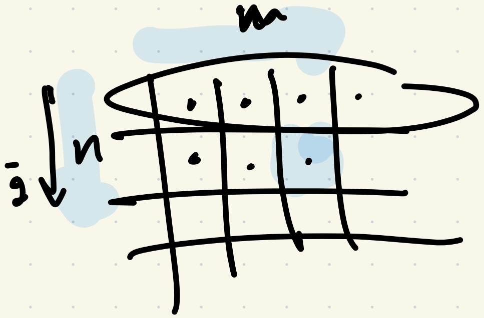
Theorem 161 *For all* $m, n \in \mathbb{N}$,

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. $\mathrm{Bij}\big([n], [n]\big) \cong [n!]$

Theorem
For all $m, n \in \mathbb{N}$, we have $[m] \times [n] \cong [m \cdot n]$

Proof. An element of $[m] \times [n]$ is a pair (i, j) with $i \in [m]$ and $j \in [n]$.
Independently choose i and j out of m and n possibilities resp.,
so $m \cdot n$ many possibilities in sum.

Proof. $I : [m] \times [n] \to [m \cdot n]$
$I(i, j) = m \cdot j + i$



Need $m \cdot j + i < m \cdot n$

Check $j := n-1 \quad i := m-1$

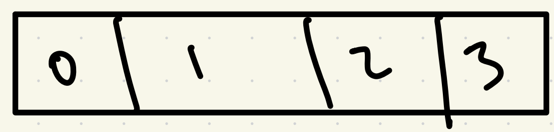
$$\begin{aligned} I(m-1, n-1) &= m \cdot (n-1) + (m-1) \\ &= m \cdot n - m + m - 1 \\ &= m \cdot n - 1 < m \cdot n \end{aligned}$$ $\square$

$I^{-1} : [m \cdot n] \to [m] \times [n]$
$I^{-1}(i) = (\mathrm{rem}(i, m), \mathrm{quo}(i, m)).$

$\square$

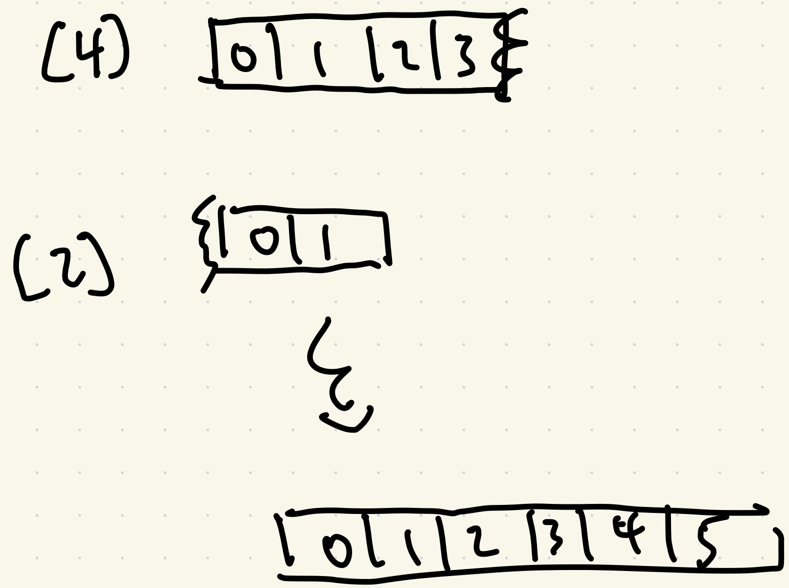
Theorem.

$$[m] \uplus [n] \cong [m+n]$$



[4]

Proof. Think of $[m] \uplus [n]$ as the set of slots in two strips of cells w/ $[m]$ slots and $[n]$ slots respectively.



$$I : [m] \uplus [n] \longrightarrow [m+n]$$

$$I(0, i \in [m]) = i \qquad < m+n$$

$$I(1, j \in [n]) = m+j$$

$$I^{-1}(k < m+n) = \begin{cases} (0,k) & \text{when } k < m \\ (1, k-m) & \text{when } k \geq m \end{cases}$$

$\square$

Infinity axiom

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