MATH 301

INTRODUCTION TO PROOFS

Sina Hazratpour
Johns Hopkins University
Fall 2021

- Images and pre-images
- Image factorization
- Axiom of choice

Relevant sections of the textbook

- Chapter 3
- Chapter 5

Images of functions

A function $f\colon X \to Y$ induces a function

$$f_*\colon \mathcal{P}(X) \to \mathcal{P}(Y)$$

defined by

$$f_*(U) = \{y \in Y \mid \exists x \in U\,(y = f(x))\}$$

for any subset U of X. The subset $f_*(U)$ is called the image of U under f. Note that

$$\mathrm{id}_* = \mathrm{id}_{\mathcal{P}(X)}$$

Proposition

Show that a function $f\colon X \to Y$ is surjective if and only if $f_*(X) = Y$.

We sometimes denote the set $f_*(X)$ by $\mathbf{Im}(f)$.

Suppose $f\colon X \to Y$ and $g\colon Y \to Z$ are functions. We prove that

$$g_* \circ f_* = (g \circ f)_* \,.$$

Recall that in order to prove equality of functions we need to use function extensionality.
Suppose T is a subset of Z. Then

$$\begin{aligned}
(g_* \circ f_*)\, U &= g_* \{y \in Y \mid \exists x \in U\, (y = f(x))\} \\
&= \big\{z \in Z \mid \exists y \in Y\, \exists x \in U\, (y = f(x) \wedge z = g(y)\big\} \\
&= \{z \in Z \mid \exists x \in U\, (z = g(f(x)))\} \\
&= (g \circ f)_* U
\end{aligned}$$

Image factorization

Proposition

Every function $f : X \to Y$ factorizes as a surjection followed by an injection, i.e. there are surjection p and injection m such that $f = m \circ p$.

$$\begin{tikzcd} X \arrow[rr, "f"] \arrow[dr, two heads, "p"'] & & Y \\ & \bullet \arrow[ur, tail, "m"'] & \end{tikzcd}$$

Proof.

Define p to be the assignment $p\colon X \to \mathbf{Im}(f)$ which takes x to $f(x)$. This assignment is well-defined since f is well-defined and that $f(x) \in \mathbf{Im}(f)$. Note that p is surjective since for any $y \in \mathbf{Im}(f)$ there is some x such that $f(x) = y$ by the definition of $\mathbf{Im}(f)$ and therefore there is some x such that $p(x) = f(x) = y$.

Define m to be the assignment $m\colon \mathbf{Im}(f) \to Y$ which takes y to y. This assignment is well-defined since $\mathbf{Im}(f) \subseteq Y$. Note that m is injective since $m(y) = m(y')$ implies $y = y'$ simply because $m(y) = y$ for all $y \in \mathbf{Im}(f)$.

Finally we have to show that p and m compose to f. To this end, note that for every $x \in X$

$$m(p(x)) = m(f(x)) = f(x)\,.$$

By function extensionality we have that $m \circ p = f$. $\square$

$$
\begin{tikzcd}
X \arrow[rr, "f"] \arrow[dr, two heads, "p"'] & & Y \\
& f_*(X) \arrow[ur, tail, "m"'] &
\end{tikzcd}
$$

Graph surjects to image

Exercise

1. *Show that the assignment which takes* $(x, f(x))$ *to* $f(x)$ *defines a function from* $\overline{\pi_2}\colon \mathbf{Gr}(f) \to \mathbf{Im}(f)$ *which is surjective.*
2. *Show that the following diagram of functions commute:*

$$\begin{tikzcd}
\mathbf{Gr}(f) \arrow[r, tail] \arrow[d, two heads, "\overline{\pi_2}"'] & X \times Y \arrow[d, "\pi_2"] \\
\mathbf{Im}(f) \arrow[r, tail] & Y
\end{tikzcd}$$

Pre-images

A function $f\colon X \to Y$ induces a function

$$f^{-1}\colon \mathcal{P}(Y) \to \mathcal{P}(X)$$

defined by

$$f^{-1}(S) = \{x \in X \mid f(x) \in S\}$$

for any subset S of Y.

The subset $f^{-1}(S)$ is called the pre-image of S under f.

Note that

$$\mathrm{id}_X^{-1} = \mathrm{id}_{\mathcal{P}(X)}$$

Suppose $f\colon X \to Y$ and $g\colon Y \to Z$ are functions. We prove that

$$f^{-1} \circ g^{-1} = (g \circ f)^{-1}\,.$$

Recall that in order to prove equality of functions we need to use function extensionality.
Suppose T is a subset of Z. Then

$$\begin{aligned}
(f^{-1} \circ g^{-1})T &= f^{-1}\,\{y \in Y \mid g(y) \in T\} \\
&= \big\{x \in X \mid f(x) \in \{y \in Y \mid g(y) \in T\}\big\} \\
&= \{x \in X \mid g(f(x)) \in T\} \\
&= (g \circ f)^{-1}\,T
\end{aligned}$$

Fibres

Definition

For a function $f\colon X \to Y$, and an element $y \in Y$, the subset

$$f^{-1}(y) = \{x \in X \mid f(x) = y\}$$

of X is called the fibre of f at y and also the pre-image of y under f.
Although, technically incorrect, people write $f^{-1}(y)$ instead of $f^{-1}(\{y\})$.

Example

Consider the function $\lfloor - \rfloor \colon \mathbb{R} \to \mathbb{Z}$ which takes a real number to the greatest integer less than it. What are the fibres

- $\lfloor - \rfloor^{-1}(0)$?
- $\lfloor - \rfloor^{-1}(\lfloor \pi \rfloor)$?

Injections and subsingletons

Definition

A set U is said to be a subsingleton if it is a subset of the one-element set $\mathbf{1}$.

Proposition

A function $f\colon X \to Y$ is injective if and only if for every $y \in Y$ the fibres $f^{-1}(y)$ are all subsingletons.

The operation of taking fibres of a function is itself a function. More specifically, given a function f, taking fibres of f at different elements $y \in Y$ as a function is equal to the composite

$$Y \xrightarrow{\{-\}} \mathcal{P}(Y) \xrightarrow{f^{-1}} \mathcal{P}(X)\,,$$

that is for all $y \in Y$,

$$f^{-1}(y) = f^{-1}\{y\}$$

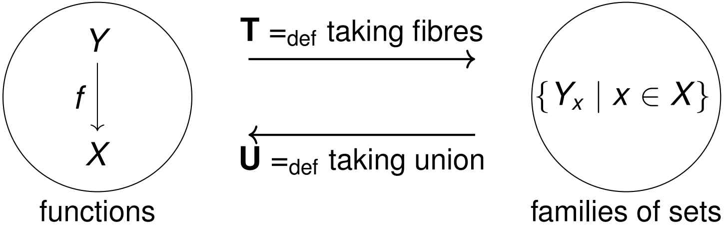
Exercise

Consider the family $\{f^{-1}(y) \mid y \in Y\}$. Show that all members of this family are mutually disjoint, and that their union is fact X.

$$\coprod_{y \in Y} f^{-1}(y) \cong \bigcup_{y \in Y} f^{-1}(y) = X$$

As the last exercise suggests, we can associate to every function a family of sets given by fibres of that function at different elements of the codomain.

Interestingly, we also have the converse association: to a family $\{Y_x \mid x \in X\}$ we associate a function as follows: let the domain to be the disjoint union $\coprod_{x \in X} Y_x$ and let the codomain be X. The associated function $p \colon \{Y_x \mid x \in X\} \to X$ takes an element $\mathrm{in}(x) \in \coprod_{x \in X} Y_x$ to $x \in X$.



Factorization of function via quotient

Recall from problem 5 of homework #4 that for each equivalence $\sim$ on a set X we can construct a set $X/\sim$ whose elements are equivalence classes

$$[x]_\sim = \{y \in X \mid x \sim y\}$$

for all $x \in X$. Now collect all such equivalence classes into one set:

$$X/\sim =_{\text{def}} \{[x]_\sim \mid x \in X\}$$

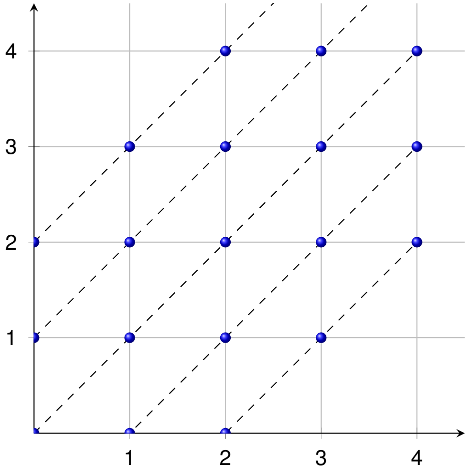
We call the set $X/\sim$ the quotient of X by equivalence relation $\sim$.

Example of quotient by an equivalence relation

Consider the relation $\sim$ on $\mathbb{N} \times \mathbb{N}$ where

$$(m, n) \sim (m', n') \Leftrightarrow m + n' = n + m' \,.$$

For instance, the equivalence class $[(0, 0)]$ is the set $\{(0, 0), (1, 1), (2, 2), ...\}$.



4
3
2
1
1
2
3
4

We can define the operation of addition on $\mathbb{N} \times \mathbb{N}/\sim$ by an assignment $+_\sim : \mathbb{N} \times \mathbb{N}/\sim \times \mathbb{N} \times \mathbb{N}/\sim \longrightarrow \mathbb{N} \times \mathbb{N}/\sim$ which assigns to the pair $([(m,n)],[(m',n')])$ the class $[(m+m', n+n')]$.

Exercise

Show that the assignment $+_\sim$ is well-defined, i.e. it defines a function.

Exercise

Show that the quotient $\mathbb{N} \times \mathbb{N}/\sim$ is isomorphic to the set $\mathbb{Z}$ of integers. Does your isomorphism preserve addition?

Exercise

Define multiplication on the quotient $\mathbb{N} \times \mathbb{N}/\sim$. Does your isomorphism preserve addition?

Image factorization

Proposition

Suppose $f\colon A \to B$ is a function. We can factor f into three functions

$$
\begin{tikzcd}
A \arrow[rrr, "f"] \arrow[dr, two heads, "q"'] & & & B \\
& C \arrow[r, "g"'] & D \arrow[ur, hook, "i"'] &
\end{tikzcd}
$$

that is $f = i \circ g \circ q$, where q is a surjection, g is a bijection, and i is an injection.

Proof.

We have to construct the sets C, D and a surjection q, a bijection g and an injection i. We define an equivalence relation $\sim$ on A by

$$x \sim y \Leftrightarrow f(x) = f(y).$$

Now we define C to be $A/\sim$, and D to be the image $f_*(A)$ of A under f. We also define q to be the obvious quotient map and i to be the obvious inclusion. Clearly, q is surjective and i is injective. We define g to be the assignment which takes an equivalence class $[x]$ to the element $f(x) \in B$. Note that g is well-defined, since if $[x] = [y]$ then $x \sim y$ and therefore, by the definition of $\sim$, we have $f(x) = f(y)$. We now show that g is a bijection. g is injective since for every $x, y \in A$, if $g([x]) = g([y])$ then $f(x) = f(y)$ and therefore, $[x] = [y]$. Also, g is surjective: given b in $f_*(A)$ there is some $a \in A$ such that $b = f(a) = g([a])$. $\square$

Our factorization diagram becomes

$$
\begin{tikzcd}
A \arrow[rrr, "f"] \arrow[dr, two heads, "q"'] & & & B \\
& A/\sim \arrow[r, "g"'] & f_*(A) \arrow[ur, tail, "i"'] &
\end{tikzcd}
$$

In fact, $g \circ q = p \colon X \to \mathbf{Im}(f)$.

The set of functions

Suppose X and Y are sets. We can define a new set consisting of all the functions from X to Y. We denote this set by Y^X. Explicitly,

$$Y^X = \{f\colon X \to Y\} \cong \{R \subset X \times Y \mid R \text{ is a functional relation}\}$$

Exercise

Suppose X is a finite set with m elements and Suppose Y is a finite set with n elements. Then the set Y^X has n^m elements.

The set of functions behaves like exponentials

Proposition

Suppose X, Y, Z are sets. We have

- $X^{\emptyset} \cong 1$
- $\emptyset^{X} \cong 1$ *if and only if* $X = \emptyset$*. In particular* $\emptyset^{\emptyset} \cong 1$.
- $(X^{Y})^{Z} \cong X^{Y \times Z}$.
- $X^{Y+Z} \cong X^{Y} \times X^{Z}$

Let Ω be a set with two elements, for instance $\{\top, \bot\}$. We show that

$$\Omega^X \cong \mathcal{P}(X)$$

that is the power set of X is isomorphic to the set of functions from X to Ω. To this end we construct two functions f and g and prove that they are inverse of each other. We have functions $\lambda(\varphi : \Omega^X).\{x \in X \mid \varphi(x) = \top\} : \Omega^X \to \mathcal{P}(X)$, and $\lambda(S : \mathcal{P}(X)).\chi_S : \mathcal{P}(X) \to \Omega^X$ where, we recall, that χ_S is the characteristic function of $S \subseteq X$.

Dependent product of sets

Let $\{X_i \mid i \in I\}$ be a family of sets.
Define the set $\prod_{i \in I} X_i$ to be

$$\{h \colon I \to \bigcup_{i \in I} X_i \mid \forall i \, (h(i) \in X_i)\}$$

Note that if I is a finite set, say $I = \{1, 2, \cdots, n\}$ then

$$\prod_{i \in I} X_i \cong X_1 \times X_2 \times \cdots \times X_n$$

In case where I is a finite set, if each X_i is inhabited then the cartesian product $\prod_{i \in I} X_i$ is also inhabited. But we cannot prove this for a general I.

Axiom of choice

Axiom of Choice (AC) asserts that the set $\prod_{i \in I} X_i$ is inhabited for *any* indexing set I and any family $(X_i \mid i \in I)$ of *inhabited* sets.

Warning

The axiom of choice is highly non-constructive: if a proof of a result that does not use the axiom of choice is available, it usually provides more information than a proof of the same result that does use the axiom of choice.

Logical incarnation of Axiom of Choice

Proposition

The axiom of choice is equivalent to the statement that for any sets X and Y and any formula $p(x, y)$ with free variables $x \in X$ and $y \in Y$, the sentence

$$\forall x \in X \, \exists y \in Y \, p(x, y) \Rightarrow \exists (f : X \to Y) \, \forall x \in X, \, p(x, f(x)) \tag{1}$$

holds.

Proof. Assume axiom of choice. Let X and Y be arbitrary sets and $p(x, y)$ any formula with free variables $x \in X$ and $y \in Y$. For each $x \in X$, define $Y_x = \{y \in Y \mid p(x, y)\}$. Note that Y_x is inhabited for each $x \in X$ by the assumption $\forall x \in X, \exists y \in Y, p(x, y)$. By the axiom of choice there exists a function $h\colon X \to \bigcup_{x \in X} Y_x$ such that $h(x) \in Y_x$ for all $x \in X$. We compose the function h with the inclusion $\cup_{x \in X} Y_x \rightarrowtail Y$, which we get from the fact that $Y_x \subseteq Y$ for each $x \in X$, to obtain a function $f\colon X \to Y$. But then $p(x, f(x)) = p(x, h(x))$ is true for each $x \in X$ by definition of the sets Y_x.

Conversely, suppose that we have a family $(X_i \mid i \in I)$ of inhabited sets. Consider the cartesian product $\prod_{i \in I} X_i$. We want to show that this product is inhabited. Define

$$p(i, x) =_{\mathrm{def}} (x \in X_i)$$

Now, we apply the sentence (1) to the sets I, $\bigcup\limits_{i \in I} X_i$ and the formula $p(i, x)$ just defined: we find a function $f\colon I \to \bigcup\limits_{i \in I} X_i$ such that $p(i, f(i))$ for all $i \in I$. But, by definition of $p(i, x)$, we conclude that $f(i) \in X_i$ for all $i \in I$. Hence, f is a member of $\prod_{i \in I} X_i$. $\square$

Axiom of Choice and surjections

Given a function $p \colon Y \to X$, consider the associated family $\{Y_x \mid x \in X\}$ of sets obtained by taking fibres of p at different elements of x.

Axiom of Choice and surjections

Given a function $p\colon Y \to X$, consider the associated family $\{Y_x \mid x \in X\}$ of sets obtained by taking fibres of p at different elements of x.

Lemma

A maps $p\colon Y \to X$ is surjective if and only if the fibres Y_x are inhabited for all $x \in X$.

Axiom of Choice and surjections

Given a function $p\colon Y \to X$, consider the associated family $\{Y_x \mid x \in X\}$ of sets obtained by taking fibres of p at different elements of x.

Lemma

A maps $p\colon Y \to X$ is surjective if and only if the fibres Y_x are inhabited for all $x \in X$.

Lemma

An element of $\prod_{x \in X} Y_x$ is the same thing as a section of $p\colon Y \to X$.

Axiom of Choice and surjections

Proposition

Axiom of choice is equivalent to the statement that every surjection has a section.

Proof.

Assume AC. Let $p\colon Y \to X$ be a surjection. Therefore all the fibres Y_x are inhabited. By AC, the product $\prod_{x \in X} Y_x$ is inhabited. Hence, by the last lemma above, p has a section. $\square$

Axiom of Choice and surjections

Proposition

Axiom of choice is equivalent to the statement that every surjection has a section.

Proof.

Assume AC. Let $p\colon Y \to X$ be a surjection. Therefore all the fibres Y_x are inhabited. By AC, the product $\prod_{x \in X} Y_x$ is inhabited. Hence, by the last lemma above, p has a section. $\square$

Axiom of Choice and surjections

Proposition

Axiom of choice is equivalent to the statement that every surjection has a section.

Proof.

Assume AC. Let $p\colon Y \to X$ be a surjection. Therefore all the fibres Y_x are inhabited. By AC, the product $\prod_{x \in X} Y_x$ is inhabited. Hence, by the last lemma above, p has a section. Conversely, suppose that every surjection has a section. Let $\{Y_x \mid x \in X\}$ be family of sets where the set Y_x is inhabited for every $x \in X$. Consider the associated function $\sqcup_{x \in X} Y_x \to X$. Note that this map is surjective by our assumption and the first lemma above. Hence, it has a section which is the same thing as an element of $\prod_{x \in X} Y_x$. Therefore AC holds. $\square$

Theorem (Diaconescu, Goodman-Myhill)

The axiom of choice implies the law of excluded middle.

Cantors' theorem: $A < P(A)$

Lemma

If a function $\sigma : A \to B^A$ is surjective then every function $f : B \to B$ has a fixed point.

Proof.

Because σ is a surjection, there is $a \in A$ such that $\sigma(a) = \lambda x : A \,.\, f(\sigma(x)(x))$, but then $\sigma(a)(a) = f(\sigma(a)(a))$. $\square$

Corollary

There is no surjection $A \to P(A)$.

Let's associate to each *finite set* X a number $\texttt{card}(X)$, called the "cardinality" of X, which measures how many (distinct) elements the set X has. We then have

- $\texttt{card}(X + Y) = \texttt{card}(X) + \texttt{card}(Y)$ and
- $\texttt{card}(X \times Y) = \texttt{card}(X) \times \texttt{card}(Y)$.

More generally, for any finite set I and a family of finite sets $\{X_i \mid i \in I\}$, we have

- $\texttt{card}(\bigsqcup\limits_{i\in I} X_i) = \sum\limits_{i\in I} \texttt{card}(X_i)$ and
- $\texttt{card}(\prod_{i\in I} X_i) = \prod_{i\in I} \texttt{card}(X_i)$

Questions

Thanks for your attention!