



Emily Riehl

Johns Hopkins University

Path induction and the indiscernibility of identicals

Colloquium de mathématique Louvain-La-Neuve

Plan



1. Induction over the natural numbers
2. Dependent type theory
3. Identity types
4. Path induction
5. What justifies path induction?
6. Epilogue: univalent foundations



1

Induction over the natural numbers

Peano's postulates



In Dedekind's 1888 book "Was sind und was sollen die Zahlen" and Peano's 1889 paper "Arithmetices principia, nova methodo exposita," the natural numbers \mathbb{N} are characterized by:

- There is a natural number $0 \in \mathbb{N}$.
- Every natural number $n \in \mathbb{N}$ has a successor $\text{succ}(n) \in \mathbb{N}$.
- 0 is not the successor of any natural number.
- No two natural numbers have the same successor.
- The principle of mathematical induction:

$$\forall P, P(0) \rightarrow (\forall k \in \mathbb{N}, P(k) \rightarrow P(\text{succ}(k))) \rightarrow (\forall n \in \mathbb{N}, P(n))$$

By Dedekind's categoricity theorem, all triples given by a set \mathbb{N} , an element $0 \in \mathbb{N}$, and a function $\text{succ} : \mathbb{N} \rightarrow \mathbb{N}$ satisfying the Peano postulates are isomorphic.

Natural numbers induction



In the statement of the **principle of mathematical induction**:

$$\forall P, P(0) \rightarrow (\forall k \in \mathbb{N}, P(k) \rightarrow P(\text{succ}(k))) \rightarrow (\forall n \in \mathbb{N}, P(n))$$

the variable P is a **predicate** over the natural numbers.

A **predicate** over the natural numbers is a function

$$P: \mathbb{N} \rightarrow \{\top, \perp\}$$

that associates a truth value \top or \perp to each $n \in \mathbb{N}$.

Thus, to prove a sentence of the form $\forall n \in \mathbb{N}, P(n)$ it suffices to:

- prove the **base case**, showing that $P(0)$ is true, and
- prove the **inductive step**, showing for each $k \in \mathbb{N}$ that $P(k)$ implies $P(\text{succ}(k))$.

A proof by induction

Theorem. For any $n \in \mathbb{N}$, $n^2 + n$ is even.

Proof: By induction on $n \in \mathbb{N}$:

- In the base case, when $n = 0$, $0^2 + 0 = 2 \times 0$, which is even.
- For the inductive step, assume for $k \in \mathbb{N}$ that $k^2 + k = 2 \times m$ is even. Then

$$\begin{aligned}(k+1)^2 + (k+1) &= (k^2 + k) + ((2 \times k) + 2) \\ &= (2 \times m) + (2 \times (k+1)) \\ &= 2 \times (m + k + 1) \quad \text{is even.}\end{aligned}$$

By the principle of mathematical induction

$$\forall P, P(0) \rightarrow (\forall k \in \mathbb{N}, P(k) \rightarrow P(\text{succ}(k))) \rightarrow (\forall n \in \mathbb{N}, P(n))$$

this proves that $n^2 + n$ is even for all $n \in \mathbb{N}$.



A construction by induction



The induction proof not only demonstrates for all $n \in \mathbb{N}$ that $n^2 + n$ is even but also defines a function $m: \mathbb{N} \rightarrow \mathbb{N}$ so that $n^2 + n = 2 \times m(n)$.

Construction: By induction on $n \in \mathbb{N}$:

- In the base case, $0^2 + 0 = 2 \times 0$, so we define $m(0) := 0$.
- For the inductive step, assume for $k \in \mathbb{N}$ that $k^2 + k = 2 \times m(k)$. Then

$$\begin{aligned}(k+1)^2 + (k+1) &= (k^2 + k) + ((2 \times k) + 2) \\ &= (2 \times m(k)) + (2 \times (k+1)) \\ &= 2 \times (m(k) + k + 1)\end{aligned}$$

so we define $m(k+1) := m(k) + k + 1$.

By the principle of mathematical recursion, this defines a function $m: \mathbb{N} \rightarrow \mathbb{N}$ so that $n^2 + n = m(n)$ for all $n \in \mathbb{N}$.

Induction and recursion



Recursion can be thought of as the constructive form of induction

$$\forall P, P(0) \rightarrow (\forall k \in \mathbb{N}, P(k) \rightarrow P(\text{succ}(k))) \rightarrow (\forall n \in \mathbb{N}, P(n))$$

in which the **predicate**

$$P: \mathbb{N} \rightarrow \{\top, \perp\} \quad \text{such as} \quad P(n) := \exists m \in \mathbb{N}, n^2 + n = 2 \times m$$

is replaced by an arbitrary **family of sets**

$$P: \mathbb{N} \rightarrow \text{Set} \quad \text{such as} \quad P(n) := \{m \in \mathbb{N} \mid n^2 + n = 2 \times m\}.$$

The output of a recursive construction is a **dependent function** $p \in \prod_{n \in \mathbb{N}} P(n)$ which specifies a value $p(n) \in P(n)$ for each $n \in \mathbb{N}$.

$$\forall P, (p_0 \in P(0)) \rightarrow (p_s \in \prod_{k \in \mathbb{N}} P(k) \rightarrow P(\text{succ}(k))) \rightarrow (p \in \prod_{n \in \mathbb{N}} P(n))$$

The recursive function $p \in \prod_{n \in \mathbb{N}} P(n)$ satisfies **computation rules**:

$$p(0) := p_0 \quad p(\text{succ}(n)) := p_s(n, p(n)).$$

The natural numbers in dependent type theory



While Peano's postulates characterize the natural numbers in set theory, the following rules characterize the natural numbers in **dependent type theory**:

- There is a type \mathbb{N} .
- There is a term $0 : \mathbb{N}$ and a function $\text{succ} : \mathbb{N} \rightarrow \mathbb{N}$.
- For any family of types $P : \mathbb{N} \rightarrow \text{Type}$ there is a term

$$\mathbb{N}\text{-ind} : (p_0 : P(0)) \rightarrow (p_s : \prod_{k \in \mathbb{N}} P(k) \rightarrow P(\text{succ}(k))) \rightarrow (p : \prod_{n \in \mathbb{N}} P(n))$$

- Computation rules $p(0) := p_0$ and $p(\text{succ}(n)) := p_s(n, p(n))$.

Note the final two postulates — that 0 is not a successor and succ is injective — are missing because they are **provable**.



2

Dependent type theory

Types, terms, and contexts



Dependent type theory is a formal system for mathematical statements and proofs that has the following primitive notions:

- types, e.g., $\Gamma \vdash \mathbb{N}$, $\Gamma \vdash \mathbb{Q}$
- terms, e.g., $\Gamma \vdash 17 : \mathbb{N}$, $\Gamma \vdash \sqrt{2} : \mathbb{R}$
- dependent types, e.g., $\Gamma, n : \mathbb{N} \vdash \mathbb{R}^n$, $\Gamma, m, n : \mathbb{N} \vdash M_{m,n}(\mathbb{R})$
- dependent terms, e.g., $\Gamma, n : \mathbb{N} \vdash \vec{0}^n : \mathbb{R}^n$, $\Gamma, n : \mathbb{N} \vdash I_n : M_{n,n}(\mathbb{R})$

Types and terms can be defined in an arbitrary context of variables from previously-defined types, all of which are listed before the symbol “ \vdash ”. Here Γ is shorthand for a generic context, which has the form

$$x_1 : A_1, x_2 : A_2(x_1), x_3 : A_3(x_1, x_2), \dots, x_n : A_n(x_1, \dots, x_{n-1})$$

In a mathematical statement of the form “Let ...be ...then ...” The stuff following the “let” likely declares the names of the variables in the context described after the “be”, while the stuff after the “then” most likely describes a type or term in that context.

Type constructors



Type constructors build new types from given ones:

- given $A, B \rightsquigarrow$ products $A \times B$, coproducts $A + B$, function types $A \rightarrow B$,
- given $x : A \vdash P(x) \rightsquigarrow$ dependent pairs $\sum_{x:A} P(x)$, dependent functions $\prod_{x:A} P(x)$
- given $A \rightsquigarrow$ identity types $x, y : A \vdash x =_A y$

Each type constructor comes with rules:

- (i) **formation**: a way to construct new types
- (ii) **introduction**: ways to construct terms of these types
- (iii) **elimination**: ways to use them to construct other terms
- (iv) **computation**: the way (ii) and (iii) relate

The rules suggest a logical naming for certain types:

$A \times B$	“A and B”	$\sum_{x:A} P(x)$	“ $\exists x. P(x)$ ”
$A + B$	“A or B”	$\prod_{x:A} P(x)$	“ $\forall x. P(x)$ ”
$A \rightarrow B$	“A implies B”	$x =_A y$	“x equals y”

Product types and function types



Product types are governed by the rules

\times -form: given types A and B there is a type $A \times B$

\times -intro: given terms $a : A$ and $b : B$ there is a term $(a, b) : A \times B$

\times -elim: given $p : A \times B$ there are terms $\text{pr}_1 p : A$ and $\text{pr}_2 p : B$

plus computation rules that relate pairings and projections.

Function types are governed by the rules

\rightarrow -form: given types A and B there is a type $A \rightarrow B$

\rightarrow -intro: if in the context of a variable $x : A$ there is a term $b_x : B$

there is a term $\lambda x. b_x : A \rightarrow B$

\rightarrow -elim: given terms $f : A \rightarrow B$ and $a : A$ there is a term $f(a) : B$

plus computation rules that relate λ -abstractions and evaluations.

Mathematics in dependent type theory



\times -form: $A, B \rightsquigarrow A \times B$

\times -intro: $a : A, b : B \rightsquigarrow (a, b) : A \times B$

\times -elim: $p : A \times B \rightsquigarrow \text{pr}_1 p : A, \text{pr}_2 p : B$

\rightarrow -form: $A \text{ and } B \rightsquigarrow A \rightarrow B$

\rightarrow -intro: $x : A \vdash b_x : B \rightsquigarrow \lambda x. b_x : A \rightarrow B$

\rightarrow -elim: $f : A \rightarrow B, a : A \rightsquigarrow f(a) : B$

To prove a mathematical proposition in dependent type theory, one constructs a term in the type that encodes its statement.

Proposition. For any types A and B , $\text{modus-ponens} : (A \times (A \rightarrow B)) \rightarrow B$.

Construction: By \rightarrow -intro, it suffices to assume given a term $p : (A \times (A \rightarrow B))$ and define a term of type B . By \times -elim, p provides terms $\text{pr}_1 p : A$ and $\text{pr}_2 p : A \rightarrow B$. By \rightarrow -elim, these combine to give a term $\text{pr}_2 p(\text{pr}_1 p) : B$. Thus we have

$$\lambda p. \text{pr}_2 p(\text{pr}_1 p) : (A \times (A \rightarrow B)) \rightarrow B. \quad \square$$



3

Identity types

The traditional view of equality



In first order logic, the binary relation “=” is governed by the following rules:

- Reflexivity: $\forall x, x = x$.
- Indiscernibility of Identicals:

$\forall x, y, x = y$ implies that for all predicates P , $P(x) \leftrightarrow P(y)$

As a consequence of these rules:

Principle of substitution: To prove that every x, y with $x = y$ has property $P(x, y)$:

- it suffices to prove that every pair x, x (for which $x = x$) has property $P(x, x)$.

Symmetry and **transitivity** of equality can be proven using the principle of substitution.

Identity types



The following rules for **identity types** were developed by Martin-Löf:

=-form: given a type A and terms $x, y : A$, there is a type $x =_A y$

=-intro: given a type A and term $x : A$ there is a term $\text{refl}_x : x =_A x$

The elimination rule for the identity type is an enhanced version of the **principle of substitution**: to prove that every x, y with $x = y$ have property P , it suffices to prove that every pair x, x (for which $x = x$) has property P .

=-elim: for any type family $x, y : A, p : x =_A y \vdash P(x, y, p)$, to prove $P(x, y, p)$ for all x, y, p it suffices to assume y is x and p is refl_x . That is

$$\text{=-ind} : \left(\prod_{x:A} P(x, x, \text{refl}_x) \right) \rightarrow \left(\prod_{x,y:A} \prod_{p:x=_A y} P(x, y, p) \right)$$

A computation rule establishes that the proof of $P(x, x, \text{refl}_x)$ is the given one.

The homotopical interpretation of dependent type theory



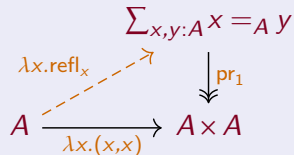
Note that identity types can be iterated:

given $x, y : A$ and $p, q : x =_A y$ there is a type $p =_{x=_A y} q$.

Does this type always have a term? In other words, are identity proofs unique?

No! From the existence of homotopical models of dependent type theory — in which **types** are interpreted as “**spaces**” and **terms** are interpreted as **points** — we know that iterated identity types can have interesting higher structure.

The total space of the identity type family $\sum_{x,y:A} x =_A y$ is interpreted as the **path space** of A and a term $p : x =_A y$ may be thought of as a **path** from x to y in A .





4

Path induction

Path induction



The homotopical interpretation of dependent type theory reflects the fundamental structure of Martin-Löf's identity types — even though it was discovered decades later!

Now that terms $p : x =_A y$ are called **paths**,
we re-brand **=-elim** as:

$$\begin{array}{ccc} & \Sigma_{x,y:A} x =_A y & \\ \lambda x. \text{refl}_x \nearrow & & \downarrow \text{pr}_1 \\ A & \xrightarrow{\lambda x. (x, x)} & A \times A \end{array}$$

Path induction: For any type family $x, y : A, p : x =_A y \vdash P(x, y, p)$, to prove $P(x, y, p)$ for all x, y, p it suffices to assume y is x and p is refl_x . That is

$$\text{path-ind} : \left(\prod_{x:A} P(x, x, \text{refl}_x) \right) \rightarrow \left(\prod_{x,y:A} \prod_{p:x=_A y} P(x, y, p) \right).$$

Reversal and concatenation of paths

Path induction: For any type family $P(x, y, p)$ over $x, y : A, p : x =_A y$

$$\text{path-ind} : \left(\prod_{x:A} P(x, x, \text{refl}_x) \right) \rightarrow \left(\prod_{x,y:A} \prod_{p:x=_A y} P(x, y, p) \right).$$

Proposition. Paths can be reversed: $(-)^{-1} : \prod_{x,y:A} x =_A y \rightarrow y =_A x$.

Construction: It suffices to assume $p : x =_A y$ and then define a term in the type $P(x, y, p) := y =_A x$. By path induction, we may reduce to the case $P(x, x, \text{refl}_x) := x =_A x$, for which we have the term $\text{refl}_x : x =_A x$. □

Proposition. Paths can be concatenated: $*$: $\prod_{x,y,z:A} x =_A y \rightarrow (y =_A z \rightarrow x =_A z)$.

Construction: It suffices to assume $p : x =_A y$ and then define a term in the type $Q(x, y, p) := \prod_{z:A} y =_A z \rightarrow x =_A z$. By path induction, we may reduce to the case $Q(x, x, \text{refl}_x) := \prod_{z:A} x =_A z \rightarrow x =_A z$, for which we have the term $\text{id} := \lambda q. q : x =_A z \rightarrow x =_A z$. □

The ∞ -groupoid of paths



Identity types can be iterated: given $x, y : A$ and $p, q : x =_A y$ there is a type $p =_{x=Ay} q$.

Theorem (Lumsdaine, Garner–van den Berg). The terms belonging to the iterated identity types of any type A form an ∞ -groupoid.

The ∞ -groupoid structure of A has

- terms $x : A$ as objects
- paths $p : x =_A y$ as 1-morphisms
- paths of paths $h : p =_{x=Ay} q$ as 2-morphisms, ...

The required structures are proven from the path induction principle:

- **constant paths** (reflexivity) $\text{refl}_x : x = x$
- **reversal** (symmetry) $p : x = y$ yields $p^{-1} : y = x$
- **concatenation** (transitivity) $p : x = y$ and $q : y = z$ yield $p * q : x = z$

and furthermore concatenation is associative and unital, the associators are coherent ...

The higher coherences in path algebra



Path induction proves the (higher) coherences in the ∞ -groupoid of paths:

Proposition. For any type A and terms $w, x, y, z : A$

$$\text{assoc} : \prod_{p:w=A \times} \prod_{q:x=A \times y} \prod_{r:y=A \times z} (p * q) * r =_{w=A \times z} p * (q * r).$$

Construction: By path induction, it suffices to assume x is w and p is refl_w , reducing to the case

$$\prod_{q:w=A \times y} \prod_{r:y=A \times z} (\text{refl}_w * q) * r =_{w=A \times z} \text{refl}_w * (q * r).$$

By the **computation rules** for path induction $\text{refl}_w * -$ is the identity function. Thus, we must show

$$\prod_{q:w=A \times y} \prod_{r:y=A \times z} q * r =_{w=A \times z} q * r,$$

for which we have the proof $\text{refl}_{q*r} : q * r =_{w=A \times z} q * r$.



Indiscernibility of Identicals as path lifting



Indiscernibility of Identicals: $x = y$ implies that for all predicates P , $P(x) \leftrightarrow P(y)$

Let $x : A \vdash P(x)$ be any family of types over A .

Proposition. For any $x, y : A$ if $p : x =_A y$ then $\text{tr}_{P,p} : P(x) \rightarrow P(y)$.

Construction: By path induction, it suffices to assume y is x and p is refl_x , in which case we have the identity function $\lambda x.x : P(x) \rightarrow P(x)$. □

Corollary. For any $x, y : A$ if $p : x =_A y$ then $P(x) \simeq P(y)$.

Construction: By path induction, it suffices to assume y is x and p is refl_x , in which case we have the identity equivalence. □



5

What justifies path induction?

The Curry-Howard-Voevodsky Correspondence



type theory	logic	set theory	homotopy theory
A	proposition	set	space
$x : A$	proof	element	point
$\emptyset, 1$	\perp, \top	$\emptyset, \{\emptyset\}$	$\emptyset, *$
$A \times B$	A and B	set of pairs	product space
$A + B$	A or B	disjoint union	coproduct
$A \rightarrow B$	A implies B	set of functions	function space
$x : A \vdash P(x)$	predicate	family of sets	fibration
$x : A \vdash p_x : P(x)$	conditional proof	family of elements	section
$\prod_{x:A} P(x)$	$\forall x. P(x)$	product	space of sections
$\sum_{x:A} P(x)$	$\exists x. P(x)$	disjoint union	total space
$p : x =_A y$	proof of equality	$x = y$	path from x to y
$\sum_{x,y:A} x =_A y$	equality relation	diagonal	path space for A

Contractible types



The homotopical perspective on type theory suggests new definitions:

A type A is **contractible** if it comes with a term of type

$$\text{is-contr}(A) := \sum_{a:A} \prod_{x:A} a =_A x$$

By Σ -elim a proof of contractibility provides:

- a term $c : A$ called the **center of contraction** and
- a dependent function $h : \prod_{x:A} c =_A x$ called the **contracting homotopy**, which can be thought of as a continuous choice of paths $h(x) : c =_A x$ for each $x : A$.

The hierarchy of types



Contractible types, those types A for which the type

$$\text{is-contr}(A) := \sum_{a:A} \prod_{x:A} a =_A x$$

has a term, form the bottom level of **Voevodsky's hierarchy of types**.

A type A is

- a **proposition** if

$$\text{is-prop}(A) := \prod_{x,y:A} \text{is-contr}(x =_A y)$$

- a **set** or **0-type** if

$$\text{is-set}(A) := \prod_{x,y:A} \text{is-prop}(x =_A y)$$

- a **succ(n)-type** for $n : \mathbb{N}$ if

$$\text{is-succ}(n)\text{-type}(A) := \prod_{x,y:A} \text{is-}n\text{-type}(x =_A y)$$

Equivalences



Similarly, homotopy theory suggests definitions of when two types A and B are **equivalent** or when a function $f : A \rightarrow B$ is an **equivalence**:

An **equivalence** between types A and B is a term of type:

$$A \simeq B := \sum_{f:A \rightarrow B} \left(\sum_{g:B \rightarrow A} \prod_{a:A} g(f(a)) =_A a \right) \times \left(\sum_{h:B \rightarrow A} \prod_{b:B} f(h(b)) =_B b \right)$$

A term of type $A \simeq B$ provides:

- functions $f : A \rightarrow B$ and $g, h : B \rightarrow A$ and
- homotopies α and β relating $g \circ f$ and $f \circ h$ to the identity functions.

Using this data, one can define a homotopy from g to h .

So why not say $f : A \rightarrow B$ is an equivalence just when:

$$\sum_{g:B \rightarrow A} \left(\prod_{a:A} g(f(a)) =_A a \right) \times \left(\prod_{b:B} f(g(b)) =_B b \right)?$$

This type is not a **proposition** and may have non-trivial higher structure.

What justifies the path induction principle?

Path induction: For any type family $x, y : A, p : x =_A y \vdash P(x, y, p)$, to prove $P(x, y, p)$ for all x, y, p it suffices to assume y is x and p is refl_x .

$$\text{path-ind} : \left(\prod_{x:A} P(x, x, \text{refl}_x) \right) \rightarrow \left(\prod_{x,y:A} \prod_{p:x=_A y} P(x, y, p) \right).$$

Path induction asserts that to map out of a **path space** $\sum_{x,y:A} x =_A y$ it suffices to define the images of the reflexivity paths.

Proposition. For each $x : A$, the **based path space** $\sum_{y:A} x =_A y$ is contractible with center of contraction given by the point (x, refl_x) .

Corollary. The function $\lambda x. (x, x, \text{refl}_x) : A \rightarrow (\sum_{x,y:A} x =_A y)$ is an equivalence.

The equivalence $A \simeq (\sum_{x,y:A} x =_A y)$ gives rise to an equivalence

$$\left(\prod_{x:A} P(x, x, \text{refl}_x) \right) \simeq \left(\prod_{x,y:A} \prod_{p:x=_A y} P(x, y, p) \right).$$



6

Epilogue: univalent foundations

The univalence axiom

Another notion of sameness between types is provided by the **universe** \mathcal{U} of types, which has (small) types A, B as its terms $\rightsquigarrow A, B : \mathcal{U}$.

Q: How do the types $A =_{\mathcal{U}} B$ and $A \simeq B$ compare?

By path induction, there is a canonical function

$$\text{id-to-equiv} : (A =_{\mathcal{U}} B) \rightarrow (A \simeq B)$$

defined by sending refl_A to the identity equivalence id_A .

Univalence Axiom: The function $\text{id-to-equiv} : (A =_{\mathcal{U}} B) \rightarrow (A \simeq B)$ is an equivalence.

“Identity is equivalent to equivalence.”

$$(A =_{\mathcal{U}} B) \simeq (A \simeq B)$$

Consequences of univalence



There are myriad consequences of the univalence axiom $(A =_{\mathcal{U}} B) \simeq (A \simeq B)$:

- The **structure-identity principle**, which specializes to the statement that for set-based structures (monoids, groups, rings) **isomorphic** structures are **identical**.
- **Function extensionality**: for any $f, g : A \rightarrow B$, the canonical function defines an equivalence between the identity type and the type of homotopies:

$$\text{id-to-htpy} : (f =_{A \rightarrow B} g) \rightarrow \left(\prod_{a:A} f(a) =_B g(a) \right)$$

- By **indiscernibility of identicals**, if $x, y : A$ and $x =_A y$ then $P(x) \simeq P(y)$ for any $a : A \vdash P(a)$. By univalence, whenever $A \simeq B$ then $A =_{\mathcal{U}} B$ and thus any type constructed from A is equivalent to the corresponding type constructed from B .

Via **path induction**, Voevodsky's univalence axiom — which is justified by the homotopical model of type theory — captures the common mathematical practice of applying results proven about one object to any other object that is equivalent to it!

References



Homotopy Type Theory: Univalent Foundations of Mathematics

<https://homotopytypetheory.org/book/>

Egbert Rijke, Introduction to Homotopy Type Theory

hott.zulipchat.com

github.com/HoTT-Intro/Agda

HoTTEST Summer School, July–August 2022

<https://discord.gg/tkhJ9zCGs9>

Merci & Dankuwel!