Myhill Isomorphism Theorem and a Computational Cantor-Bernstein Theorem in Constructive Type Theory

21^{st} June 2022

TYPES 2022

Yannick Forster

Gert Smolka

Felix Jahn

History of Cantor-Bernstein

Cantor-Bernstein Theorem (Set-theoretical)

For sets A and B with injections $f : A \to B$ and $g : B \to A$, there is a bijection $h : A \to B$.

History of Cantor-Bernstein

Cantor-Bernstein Theorem (Set-theoretical)

For sets A and B with injections $f : A \to B$ and $g : B \to A$, there is a bijection $h : A \to B$.

1887: Cantor firstly publishes theorem

History of Cantor-Bernstein

Cantor-Bernstein Theorem (Set-theoretical)

For sets A and B with injections $f : A \to B$ and $g : B \to A$, there is a bijection $h : A \to B$.

1887: Cantor firstly publishes theorem

1897: Proofs by Bernstein (using AC)

History of Cantor-Bernstein

Cantor-Bernstein Theorem (Set-theoretical)

For sets A and B with injections $f : A \to B$ and $g : B \to A$, there is a bijection $h : A \to B$.

1887: Cantor firstly publishes theorem

1897: Proofs by Bernstein (using AC)

1906: Proof by Kőnig (using LEM)

History of Cantor-Bernstein

Cantor-Bernstein Theorem (Set-theoretical)

For sets A and B with injections $f : A \to B$ and $g : B \to A$, there is a bijection $h : A \to B$.

1887: Cantor firstly publishes theorem

1897: Proofs by Bernstein (using AC)

1906: Proof by Kőnig (using LEM)

2019: Pradič & Brown proof implication of LEM

Reducibility Theory[1]

[1] among many others by Myhill [1955]

Reducibility Theory[1]

Definition (One-One Reducibility)

A predicate $p : X \to \mathbb{P}$ is called *one-one reducible* to $q : Y \to \mathbb{P}$ ("$p \preceq_1 q$") if there exists an function $f : X \to Y$ s.t.

$$\forall x.\, px \leftrightarrow q(fx), \qquad \forall x_1, x_2.\, f(x_1) = f(x_2) \to x_1 = x_2.$$

[1] among many others by Myhill [1955]

Reducibility Theory[1]

Definition (One-One Reducibility)

A predicate $p : X \to \mathbb{P}$ is called *one-one reducible* to $q : Y \to \mathbb{P}$ ("$p \preceq_1 q$") if there exists an function $f : X \to Y$ s.t.

$$\forall x.\, px \leftrightarrow q(fx), \qquad \forall x_1, x_2.\, f(x_1) = f(x_2) \to x_1 = x_2.$$

"Synthetic setting"[2] of only computable functions!

[1] among many others by Myhill [1955]
[2] Richman[1983]; Bauer[2006]; Forster, Kirst, Smolka[2019]

Reducibility Theory[1]

Definition (One-One Reducibility)

A predicate $p : X \to \mathbb{P}$ is called *one-one reducible* to $q : Y \to \mathbb{P}$ ("$p \preceq_1 q$") if there exists an function $f : X \to Y$ s.t.

$$\forall x.\ px \leftrightarrow q(fx), \qquad \forall x_1, x_2.\ f(x_1) = f(x_2) \to x_1 = x_2.$$

"Synthetic setting"[2] of only computable functions!

Myhill Isomorphism Theorem

Let X and Y be enumerable discrete types, $p : X \to \mathbb{P}$, and $q : Y \to \mathbb{P}$. If $p \preceq_1 q$ and $q \preceq_1 p$, then there exist $f : X \to Y$ and $g : Y \to X$ such that for all $x : X$ and $y : Y$:

$$g(fx) = x, \qquad f(gy) = y, \qquad px \leftrightarrow q(fx), \qquad qy \leftrightarrow p(gy).$$

[1] among many others by Myhill [1955]

[2] Richman[1983]; Bauer[2006]; Forster, Kirst, Smolka[2019]

Proof of Myhill's Isomorphism Theorem[1]

Definition (Correspondence Sequence)

A list of pairs $C : \mathcal{L}(X \times Y)$ is called correspondence sequence for $p : X \to \mathbb{P}$ and $q : Y \to \mathbb{P}$ if:

$$1. \forall (x, y) \in C.\ px \leftrightarrow qy$$
$$2. \forall (x, y), (x', y') \in C.\ (x = x' \leftrightarrow y = y')$$

[1] Myhill [1955], textbook presentation by Rogers [1987]

Proof of Myhill's Isomorphism Theorem[1]

Definition (Correspondence Sequence)

A list of pairs $C : \mathcal{L}(X \times Y)$ is called correspondence sequence for $p : X \to \mathbb{P}$ and $q : Y \to \mathbb{P}$ if:

$$1. \forall (x, y) \in C.\ px \leftrightarrow qy$$

$$2. \forall (x, y), (x', y') \in C.\ (x = x' \leftrightarrow y = y')$$

0	4	2	1	3
4	3	0	2	5

[1] Myhill [1955], textbook presentation by Rogers [1987]

Proof of Myhill's Isomorphism Theorem

Lemma

Let X and Y be enumerable and discrete, and $p \preceq_1 q$ via $f : X \to Y$.
One can define a function find : $\mathcal{L}(X \times Y) \to X \to Y$ such that:
If C is correspondence sequence for p and q and $x_0 \notin_1 C$,
then also $(x_0, \text{find}\, C\, x_0) :: C$ is correspondence sequence for p and q.

Proof of Myhill's Isomorphism Theorem

Lemma

Let X and Y be enumerable and discrete, and $p \preceq_1 q$ via $f : X \to Y$.
One can define a function find : $\mathcal{L}(X \times Y) \to X \to Y$ such that:
If C is correspondence sequence for p and q and $x_0 \notin_1 C$,
then also $(x_0, \text{find}\, C\, x_0) :: C$ is correspondence sequence for p and q.

0	4	2	1	3
4	3	0	2	5

Proof of Myhill's Isomorphism Theorem

Lemma

Let X and Y be enumerable and discrete, and $p \preceq_1 q$ via $f : X \to Y$.
One can define a function find : $\mathcal{L}(X \times Y) \to X \to Y$ such that:
If C is correspondence sequence for p and q and $x_0 \notin_1 C$,
then also $(x_0, \text{find}\, C\, x_0) :: C$ is correspondence sequence for p and q.

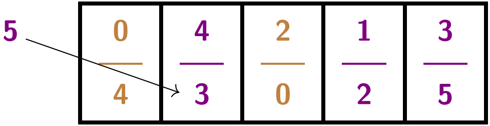
5

0	4	2	1	3
4	3	0	2	5

Proof of Myhill's Isomorphism Theorem

Lemma

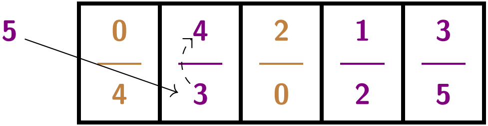
Let X and Y be enumerable and discrete, and $p \preceq_1 q$ via $f : X \to Y$.
One can define a function find : $\mathcal{L}(X \times Y) \to X \to Y$ such that:
If C is correspondence sequence for p and q and $x_0 \notin_1 C$,
then also $(x_0, \text{find}\, C\, x_0) :: C$ is correspondence sequence for p and q.



Proof of Myhill's Isomorphism Theorem

Lemma

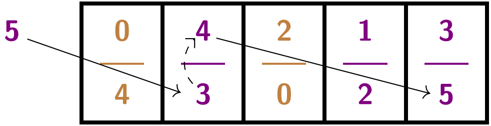
Let X and Y be enumerable and discrete, and $p \preceq_1 q$ via $f : X \to Y$.
One can define a function find : $\mathcal{L}(X \times Y) \to X \to Y$ such that:
If C is correspondence sequence for p and q and $x_0 \notin_1 C$,
then also $(x_0, \text{find}\, C\, x_0) :: C$ is correspondence sequence for p and q.



Proof of Myhill's Isomorphism Theorem

Lemma

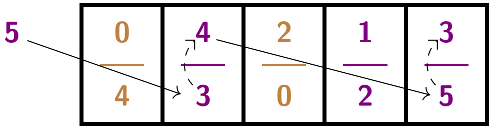
Let X and Y be enumerable and discrete, and $p \preceq_1 q$ via $f : X \to Y$.
One can define a function find : $\mathcal{L}(X \times Y) \to X \to Y$ such that:
If C is correspondence sequence for p and q and $x_0 \notin_1 C$,
then also $(x_0, \mathsf{find}\, C\, x_0) :: C$ is correspondence sequence for p and q.



Proof of Myhill's Isomorphism Theorem

Lemma

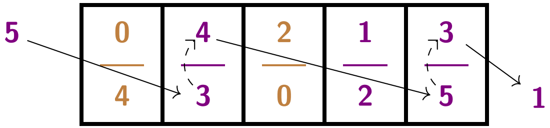
Let X and Y be enumerable and discrete, and $p \preceq_1 q$ via $f : X \to Y$.
One can define a function find : $\mathcal{L}(X \times Y) \to X \to Y$ such that:
If C is correspondence sequence for p and q and $x_0 \notin_1 C$,
then also $(x_0, \text{find}\, C\, x_0) :: C$ is correspondence sequence for p and q.



Proof of Myhill's Isomorphism Theorem

Lemma

Let X and Y be enumerable and discrete, and $p \preceq_1 q$ via $f : X \to Y$.
One can define a function find : $\mathcal{L}(X \times Y) \to X \to Y$ such that:
If C is correspondence sequence for p and q and $x_0 \notin_1 C$,
then also $(x_0, \text{find}\, C\, x_0) :: C$ is correspondence sequence for p and q.



Proof of Myhill's Isomorphism Theorem

Lemma

Let X and Y be enumerable and discrete, and $p \preceq_1 q$ via $f : X \to Y$.
One can define a function find : $\mathcal{L}(X \times Y) \to X \to Y$ such that:
If C is correspondence sequence for p and q and $x_0 \notin_1 C$,
then also $(x_0, \text{find}\, C\, x_0) :: C$ is correspondence sequence for p and q.

5	0	4	2	1	3
1	4	3	0	2	5

Proof of Myhill's Isomorphism Theorem

Now, let $p \preceq_1 q$ and $q \preceq_1 p$.

Proof of Myhill's Isomorphism Theorem

Now, let $p \preceq_1 q$ and $q \preceq_1 p$.

$\frac{0}{6}$

Proof of Myhill's Isomorphism Theorem

Now, let $p \preceq_1 q$ and $q \preceq_1 p$.

$\frac{10}{0}$	$\frac{0}{6}$

Proof of Myhill's Isomorphism Theorem

Now, let $p \preceq_1 q$ and $q \preceq_1 p$.

1	10	0
8	0	6

Proof of Myhill's Isomorphism Theorem

Now, let $p \preceq_1 q$ and $q \preceq_1 p$.

7	1	10	0
1	8	0	6

Proof of Myhill's Isomorphism Theorem

Now, let $p \preceq_1 q$ and $q \preceq_1 p$.

4	2	7	1	10	0
2	13	1	8	0	6

Proof of Myhill's Isomorphism Theorem

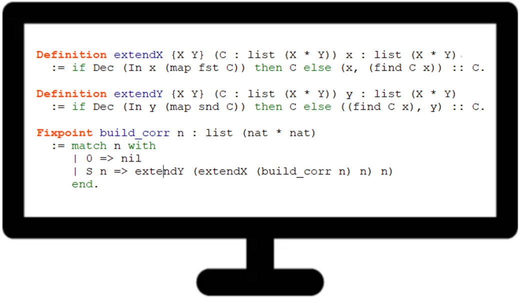
Now, let $p \preceq_1 q$ and $q \preceq_1 p$.

12	3	4	2	7	1	10	0
3	9	2	13	1	8	0	6

Proof of Myhill's Isomorphism Theorem

Now, let $p \preceq_1 q$ and $q \preceq_1 p$.

12	3	4	2	7	1	10	0
3	9	2	13	1	8	0	6



From Myhill to Cantor-Bernstein

Synthetic Myhill Isomorphism Theorem

Let X and Y be enumerable discrete types, $p : X \to \mathbb{P}$, and $q : Y \to \mathbb{P}$. If $p \preceq_1 q$ and $q \preceq_1 p$, then there exist $f : X \to Y$ and $g : Y \to X$ such that for all $x : X$ and $y : Y$:

$$px \leftrightarrow q(fx), \quad qy \leftrightarrow p(gy), \quad g(fx) = x, \quad f(gy) = y.$$

From Myhill to Cantor-Bernstein

Synthetic Myhill Isomorphism Theorem

Let X and Y be enumerable discrete types, $p : X \to \mathbb{P}$, and $q : Y \to \mathbb{P}$. If $p \preceq_1 q$ and $q \preceq_1 p$, then there exist $f : X \to Y$ and $g : Y \to X$ such that for all $x : X$ and $y : Y$:

$$px \leftrightarrow q(fx), \qquad qy \leftrightarrow p(gy), \qquad g(fx) = x, \qquad f(gy) = y.$$

$\rightsquigarrow$ instantiating $p := \lambda x.\top$ and $q := \lambda y.\top$

From Myhill to Cantor-Bernstein

Synthetic Myhill Isomorphism Theorem

Let X and Y be enumerable discrete types, $p : X \to \mathbb{P}$, and $q : Y \to \mathbb{P}$. If $p \preceq_1 q$ and $q \preceq_1 p$, then there exist $f : X \to Y$ and $g : Y \to X$ such that for all $x : X$ and $y : Y$:

$$px \leftrightarrow q(fx), \quad qy \leftrightarrow p(gy), \quad g(fx) = x, \quad f(gy) = y.$$

$\rightsquigarrow$ instantiating $p := \lambda x.\top$ and $q := \lambda y.\top$

Computational Cantor-Bernstein Theorem

Let X and Y be enumerable discrete types with injections $X \to Y$ and $Y \to X$. Then there exist $f : X \to Y$ and $g : Y \to X$ such that for all $x : X$ and $y : Y$:

$$g(fx) = x, \quad f(gy) = y.$$

Summary

- Formalization of Myhill Isomorphism Theorem &
  Computational Cantor-Bernstein in Constructive Type Theory

Summary

- Formalization of Myhill Isomorphism Theorem & Computational Cantor-Bernstein in Constructive Type Theory
- Machine-checked proofs in Coq

Summary

- Formalization of Myhill Isomorphism Theorem &
  Computational Cantor-Bernstein in Constructive Type Theory
- Machine-checked proofs in Coq
- Results do not rely on impredicativity nor on choice principles nor on strong elimination principles
  $\Rightarrow$ Formalization should transport to other foundations

Summary

- Formalization of Myhill Isomorphism Theorem &
Computational Cantor-Bernstein in Constructive Type Theory
- Machine-checked proofs in Coq
- Results do not rely on impredicativity nor on choice principles nor on strong elimination principles
$\Rightarrow$ Formalization should transport to other foundations
- Type theory as sweet spot for synthetic computability theory, results as beautiful and concise case studies

Backup Slides

Synthetic Computability Theory

Definition (Traditional One-One Reducibility)

Definition 8. A set α is called *one-one reducible* to a set β if

$$x \in \alpha \longleftrightarrow f(x) \in \beta$$

for a one-one recursive function f.

(Screenshot out of Myhill[1955])

Definition (Synthetic One-One Reducibility)

A predicate $p : X \to \mathbb{P}$ is called *one-one reducible* to a predicate $p : Y \to \mathbb{P}$ if

$$px \leftrightarrow q(fx)$$

for an injective function $f : X \to Y$.

Enumerable and Discrete Types

Definition (Enumerable Type)

A type X is called enumerable if there exists $f : \mathbb{N} \to \mathcal{O}X$ s.t.

$$\forall x : X.\ \exists n. fx = \text{Some } x.$$

Definition (Discrete Type)

A type X is called discrete if equality of his elements is decidable, i.e. if there is a decider $f : X \to X \to \mathbb{B}$ s.t.

$$\forall x_1, x_2.\ f x_1 x_2 = \text{true} \leftrightarrow x_1 = x_2.$$

Myhill Isomorphism Theorem

Synthetic Myhill Isomorphism Theorem

Let X and Y be enumerable discrete types, $p : X \to \mathbb{P}$, and $q : Y \to \mathbb{P}$. If $p \preceq_1 q$ and $q \preceq_1 p$, then there exist $f : X \to Y$ and $g : Y \to X$ such that for all $x : X$ and $y : Y$:

$$px \leftrightarrow q(fx), \quad qy \leftrightarrow p(gy), \quad g(fx) = x, \quad f(gy) = y.$$

Myhill formulated the theorem in terms of computability degrees:

p and q 1-equivalent $\Leftrightarrow$ p and q isomorphic.

Step-wise Bijection (Proof Myhill)

Now, let $p \preceq_1 q$ and $q \preceq_1 p$.

10	0
0	6

7	1	10	0
1	8	0	6

4	2	7	1	10	0
2	13	1	8	0	6

12	3	4	2	7	1	10	0
3	9	2	13	1	8	0	6

Step-wise Bijection - Skip Case (Proof Myhill)

Now, let $p \preceq_1 q$ and $q \preceq_1 p$.

3	0
0	6

7	1	3	0
1	8	0	6

4	2	7	1	3	0
2	13	1	8	0	6

12	4	2	7	1	3	0
3	2	13	1	8	0	6

Direct Proof of Cantor-Bernstein (Sketch)

Computational Cantor-Bernstein Theorem

Let X and Y be enumerable discrete types with injections $X \to Y$ and $Y \to X$. Then there exist $f : X \to Y$ and $g : Y \to X$ such that for all $x : X$ and $y : Y$:

$$g(fx) = x, \qquad f(gy) = y.$$

1. Notion of aligned types: A type X is called to be aligned if there exist $A : X \to \mathbb{N}$ and $B : X \to \mathbb{N} \to \mathcal{O}\mathbb{N}$ such that

$$\forall x. \forall n \leq Ax. \exists y.\ Bxn = \text{Some } y \wedge Ay = n.$$

2. Alignment theorem: Enumerable and discrete types are aligned
3. Aligned types with injections between each other have bijections between each other