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

Yannick Forster[1,2], Felix Jahn[1], and Gert Smolka[1]

[1] Saarland University, Saarland Informatics Campus, Saarbrücken, Germany
[2] Inria, Gallinette Project-Team, Nantes, France

Abstract

Two enumerable discrete types which can be embedded into each other in constructive type theory are isomorphic. Furthermore, the isomomorphism can be constructed to preserve a reduction property regarding predicates on the types. This (novel) result can be interpreted in two ways: First, it is a computational form of the Cantor-Bernstein theorem [2, 1] from set theory, stating that two sets which can be embedded into each other are in bijection, which is is inherently classical in its full generality [8]. Secondly, it is a synthetic form of the Myhill isomorphism theorem [7] from computability theory stating that 1-equivalent predicates are recursively isomorphic.

We give two proofs of the result: The first is following the textbook proof of the Myhill isomorphism theorem closely, and thus preserves reduction of predicates. The second is a direct proof, which seems to not be extendable to predicates. All proofs are machine-checked in Coq but should transport to other foundations – they do not rely on impredicativity, on choice principles, or on large eliminations apart from falsity elimination.

A type X is enumerable and discrete if and only if it is a retract of $\mathbb{N}$ (see e.g. [4, Corr. 4.34]), i.e. if there are $I\colon X\to\mathbb{N}$ and $R\colon\mathbb{N}\to\mathbb{O}X$ with $\forall x.\ R(Ix) = \mathsf{Some}\ x$.

1 Myhill isomorphism theorem

A predicate $p\colon X\to\mathbb{P}$ is one-one reducible to a predicate $q\colon Y\to\mathbb{P}$ if $p \preceq_1 q := \exists f\colon X\to Y.\ (\forall x.\ px \leftrightarrow q(fx)) \land f$ is injective. We prove that when two predicates are one-one reducible to each other, where the reductions functions are in no relation, one can construct one-one reductions which also invert each other. We follow Rogers [9, §7.4 Th. VI], where the isomorphism is constructed in stages, formed by *correspondence sequences* between predicates p and q, which are finitary bijections represented as lists $C\colon\mathbb{L}(X\times Y)$ such that for all $(x,y)\in C$

$$1.\ px \leftrightarrow qy \qquad 2.\ \forall y'.\ (x,y')\in C \to y = y' \qquad 3.\ \forall x'.\ (x',y)\in C \to x = x'$$

We write $x \in_1 C$ ($x \in_2 C$) if x is an element of the first (second) projection of C.

The crux of the theorem is that for any correspondence sequence C with $p \preceq_1 q$ and $x_0 \notin_1 C$ one can *compute* y_0 such that $(x_0, y_0) :: C$ is a correspondence sequence again.

Lemma 1. *Let f be a one-one reduction from p to q. There is a function* $\mathsf{find}\colon\mathbb{L}(X\times Y)\to X\to Y$ *such that if C is a correspondence sequence for p and q and $x_0 \notin_1 C$, then* $\mathsf{find}\,C\,x_0 \notin_2 C$ *and* $px_0 \leftrightarrow q(\mathsf{find}\,C\,x_0)$.

Proof. We first define a function $\gamma\colon\mathbb{L}(X\times Y)\to X\to X$ recursive in $|C|$:

$$\gamma Cx := x \ \text{ if } fx \notin_2 C \qquad \gamma Cx := \gamma\,(\mathsf{filter}(\lambda t.t \neq_{\mathbb{B}} (x', fx))\,C)\,x' \ \text{ if } (x', fx)\in C$$

For a correspondence sequence C between p and q and $x \notin_1 C$ we have (1) $px \leftrightarrow p(\gamma Cx)$, (2) $\gamma Cx = x$ or $\gamma Cx \in_1 C$, and (3) $f(\gamma Cx) \notin_2 C$. The proof is by induction on the length of C, exploiting the injectivity of f. Now $\mathsf{find}\ Cx_0 := f(\gamma Cx_0)$ is the wanted function. □

For the rest of this section we fix enumerable discrete types X and Y such that (I_X, R_X) and (I_Y, R_Y) are retractions from X and Y respectively to $\mathbb{N}$. We construct the isomorphism via a cumulative correspondence sequence C_n with $I_X x < n \to x \in_1 C_n$ and $I_Y y < n \to y \in_2 C_n$.

$$C'_n := \begin{cases} (x, \mathsf{find}\, C_n\, x) :: C_n \text{ if } R_X n = \mathsf{Some}\ x \wedge x \notin_1 C_n \\ C_n \text{ otherwise} \end{cases} \quad C_{n+1} := \begin{cases} (\mathsf{find}\, \overleftrightarrow{C'_n}\, y, y) :: C'_n \text{ if } R_Y n = \mathsf{Some}\ y \wedge y \notin_2 C'_n \\ C'_n \text{ otherwise} \end{cases}$$

where $C_0 := []$ and $\overleftrightarrow{C} := \mathsf{map}\,(\lambda(x,y).(y,x))\, C$.

Lemma 2. *C_n is a correspondence sequence for p and q such that*

1. $n \le m \to C_n \subseteq C_m$ 2. $I_X x < n \to x \in_1 C_n$ 3. $I_Y y < n \to y \in_2 C_n$

Theorem 1 (Myhill)**.** *Let X and Y be enumerable discrete types, $p\colon X \to \mathbb{P}$, and $q\colon Y \to \mathbb{P}$. If $p \preceq_1 q$ and $q \preceq_1 p$, then there exist $f\colon X \to Y$ and $g\colon Y \to X$ such that for all $x\colon X$ and $y\colon Y$:*

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

Proof. fx is defined as the unique y for which $(x,y) \in C_{I_X x+1}$ (which exists by Lemma 2 (2) and is unique because $C_{I_X x+1}$ is a correpsondence sequence), and gy is symmetrically defined as the unique x for which $(x,y) \in C_{I_Y y+1}$. (1) and (2) are immediate since C_n is a correspondence sequence. (3) and (4) are by case analysis whether $I_X x \le I_Y y$ or vice versa. ☐

Proofs of the theorem have appeared in different forms in [6], [4], and [5].

2 Computational Cantor-Bernstein Theorem

The Cantor-Bernstein theorem is inherently classical in set theory [8]. Recently, the classical proof has been generalised to all boolean toposes by Escardó [3]. We give a direct, fully constructive proof of the Cantor-Bernstein theorem for enumerable discrete types via a novel alignment theorem. We say that a type X is aligned if there are $A\colon X \to \mathbb{N}$ and $B\colon X \to \mathbb{N} \to \mathbb{O}X$ s.t. $\forall x. \forall n \le Ax. \exists y.\ Bxn = \mathsf{Some}\ y \wedge Ay = n$. We write $\#l$ if a list l is duplicate-free.

Theorem 2 (Alignment)**.** *Every enumerable discrete type is aligned.*

Proof. Let (I, R) be a retraction from X to $\mathbb{N}$. We define Ax to be the position of x in L_{Ix}, where L_n is the list of all x s.t. $\exists m \le n.\ Rm = \mathsf{Some}\ x$. Bxn is the n-th element of L_{Ix} if it exists, and x otherwise. ☐

Lemma 3. *Let X be aligned by $s\colon X \to \mathbb{N}$.*

1. *There is $F'_X\colon \mathbb{N} \to X \to \mathbb{L}X \to X$ s.t. if $\#l$ and $|l| = n+1$ then $s(F'_X x_0 n l) = n$.*
2. *There is $F_X\colon X \to \mathbb{L}X$ s.t. $\#(F_X x)$ and $|F_X x| = 1 + sx$.*

Proof. (1) uses a function $\mathsf{get}\colon \mathbb{L}\mathbb{N} \to \mathbb{N}$ s.t. if $\#l$ and $|l| = n+1$, then $\mathsf{get}\ l \in l$ and $\mathsf{get}\ l \ge n$. ☐

Lemma 4. *Aligned types X, Y with injections $X \to Y$ and $Y \to X$ are isomorphic.*

Proof. Let X and Y be aligned and $f\colon X \to Y$ and $g\colon Y \to X$ be injections. Define $f'x := F'_Y(A_X x)(fx)(\mathsf{map}\ f\ (F_X x))$ and $g'y := F'_X(A_Y y)(gy)(\mathsf{map}\ g\ (F_Y y))$. We have that $\#(\mathsf{map}\ f\ (F_X x))$, which follows because f is injective and $\#(F_X x)$, and $|\mathsf{map}\ f\ (F_X x)| = s_X x + 1$, which is immediate. This suffices with the dual properties for $\mathsf{map}\ g\ (F_Y y)$. ☐

Theorem 3 (Computational Cantor-Bernstein)**.** *For enumerable discrete types X, Y with injections $X \to Y$ and $Y \to X$ there are functions $X \to Y$ and $Y \to X$ inverting each other.*

Proof. Either by applying the preceding lemma and the alignment theorem, or by applying the Myhill isomorphism theorem with $px := \top$ and $qy := \top$. ☐

References

[1] Felix Bernstein. Untersuchungen aus der mengenlehre. *Mathematische Annalen*, 61(1):117–155, March 1905. doi:10.1007/bf01457734.

[2] Georg Cantor. Mitteilungen zur Lehre vom Transfiniten. In *Zeitschrift für Philosophie und philosophische Kritik 91*, 1887.

[3] Martín Hötzel Escardó. The cantor–schröder–bernstein theorem for $$\infty $$-groupoids. *Journal of Homotopy and Related Structures*, 16(3):363–366, June 2021. doi:10.1007/s40062-021-00284-6.

[4] Yannick Forster. *Computability in Constructive Type Theory*. PhD thesis, Saarland University, 2021. URL: https://ps.uni-saarland.de/~forster/thesis.

[5] Yannick Forster, Felix Jahn, and Gert Smolka. A Constructive and Synthetic Theory of Reducibility: Myhill's Isomorphism Theorem and Post's Problem for Many-one and Truth-table Reducibility in Coq (Full Version). preprint, February 2022. URL: https://hal.inria.fr/hal-03580081.

[6] Felix Jahn. *Synthetic One-One, Many-One, and Truth-Table Reducibility in Coq*. Bachelor's thesis, Saarland University, 2020. URL: https://ps.uni-saarland.de/~jahn/bachelor.php.

[7] John Myhill. Creative sets. 1957. doi:10.1002/malq.19550010205.

[8] Pierre Pradic and Chad E. Brown. Cantor-Bernstein implies excluded middle. *CoRR*, abs/1904.09193, 2019. arXiv:1904.09193.

[9] Hartley Rogers. Theory of recursive functions and effective computability. 1987.