Classical System of Martin-Löf's Inductive Definitions is not Equivalent to Cyclic Proof System

Stefano Berardi[1] and Makoto Tatsuta[2]

[1] Università di Torino
[2] National Institute of Informatics / Sokendai, Tokyo

Abstract. A cyclic proof system, called $\texttt{CLKID}^\omega$, gives us another way of representing inductive definitions and efficient proof search. The 2011 paper by Brotherston and Simpson showed that the provability of $\texttt{CLKID}^\omega$ includes the provability of Martin-Löf's system of inductive definitions, called LKID, and conjectured the equivalence. Since then, the equivalence has been left an open question. This paper shows that $\texttt{CLKID}^\omega$ and LKID are indeed not equivalent. This paper considers a statement called 2-Hydra in these two systems with the first-order language formed by 0, the successor, the natural number predicate, and a binary predicate symbol used to express 2-Hydra. This paper shows that the 2-Hydra statement is provable in $\texttt{CLKID}^\omega$, but the statement is not provable in LKID, by constructing some Henkin model where the statement is false.

1 Introduction

An inductive definition is a way to define a predicate by an expression which may contain the predicate itself. The predicate is interpreted by the least fixed point of the defining equation. Inductive definitions are important in computer science, since they can define useful recursive data structures such as lists and trees. Inductive definitions are important also in mathematical logic, since they increase the proof theoretic strength. Martin-Löf's system of inductive definitions given in [10] is one of the most popular system of inductive definitions. This system has production rules for an inductive predicate, and the production rule determines the introduction rule and the elimination rule for the predicate.

Brotherston [3] and Simpson [6] proposed an alternative formalization of inductive definitions, called a cyclic proof system. A proof, called *a cyclic proof*, is defined by proof search, going upwardly in a proof figure. If we encounter the same sequent (called a bud) as some sequent we already passed (called a companion) we can stop. The induction rule is replaced by a case rule, for this purpose. The soundness is guaranteed by some additional condition, called the *global trace condition*, which guarantees the case rule decreases some measure of a bud from that of the companion. In general, for proof search, a cyclic proof system can find an induction formula in a more efficient way than Martin-Löf's system, since a cyclic proof system does not have to choose fixed induction

formula in advance. A cyclic proof system enables us efficient implementation of theorem provers with inductive definitions[2, 4, 5, 7]. In particular, it works well for theorem provers of separation logic.

Brotherston and Simpson [6] investigated Martin-Löf's system LKID of inductive definitions in classical logic for the first-order language, and the cyclic proof system $\mathtt{CLKID}^\omega$ for the same language, showed the provability of $\mathtt{CLKID}^\omega$ includes that of LKID, and conjectured the equivalence. Since then, the equivalence has been left an open question. Simpson [11] submitted a proof of a particular case of the conjecture, for the theory of Peano Arithmetic.

This paper shows $\mathtt{CLKID}^\omega$ and LKID are indeed not equivalent. To this aim, we will consider the first-order language formed by 0, the successor s, the natural number predicate N, and a binary predicate symbol p. We introduce a statement we call 2-Hydra, which is a miniature version of the Hydra problem considered by Laurence Kirby and Jeff Paris [9]: the proviso "2" means that we only have two "heads". We define some statement, called the 2-Hydra statement, and shows that the 2-Hydra statement is provable in $\mathtt{CLKID}^\omega$ with the language, but the statement is not provable in LKID with the language. The second result is proved by constructing some model of $\mathtt{CLKID}^\omega$ where the statement is false.

For constructing the counter model $\mathcal{M}$ for the second result, we take both the universe of $\mathcal{M}$ and the interpretation of the predicate N to be $\mathtt{Nat}+\mathtt{Z}$, where Nat is the set of natural numbers and Z is the set of integers, and some predicate p which is a counter-example of 2-Hydra. We prove that $\mathcal{M}$ is a model of LKID by using a set of partial bijections on $\mathcal{M}$ and a quantifier elimination result.

The quantifier elimination theorem for a theory of partial equivalence relations is new, as far as we know, and it may have some independent interest.

This model also shows that LKID is not conservative when we add inductive predicates, namely, it is not the case that for any language L, the system of LKID with language L and any additional inductive predicate is conservative over the system of LKID with L.

Section §2 describes Brotherston-Simpson conjecture. Section §3 defines the 2-Hydra statement and proves the 2-Hydra statement in $\mathtt{CLKID}^\omega$. Section §4 defines the counter model $\mathcal{M}$ and the proof outline of it. Section §5 introduces a family of partial bijections. Section §6 proves a quantifier elimination theorem for a theory of partial bijections. Section §7 proves that the 2-Hydra statement is not provable in LKID. Section §8 shows non-conservativity of LKID with additional inductive predicates. We conclude in Section §9. Detailed proofs are in §A.

2 Brotherston-Simpson Conjecture

In this section we introduce Brotherston-Simpson Conjecture.

2.1 Martin-Löf's Inductive Definition System LKID

We briefly remind you of Martin-Löf's inductive definition system LKID, defined in detail in [6].

The language of LKID is determined by a first-order language with inductive predicate symbols. The logical system LKID is determined by production rules for inductive predicate symbols. These production rules mean that the inductive predicate denotes the least fixed point defined by these production rules.

We often abbreviate $p(t), q(t,u)$ with pt, qtu. For example, for an inductive predicate symbol N, the production rules may be written as

$$\frac{}{N0} \qquad \frac{Nx}{Nsx}$$

These production rules mean that N denotes the smallest set closed under 0 and s, namely the set of natural numbers. We call this set of production rules Φ_N.

The inference rules of LKID are standard inference rules in classical first-order logic LK with the introduction rules and the elimination rules for inductive predicates, determined by the production rules. These rules describe that the predicate actually denotes the least fixed point. In particular, the elimination rule describes the induction principle.

For example, the above production rules give the introduction rules

$$\frac{}{\Gamma \vdash N0, \Delta} \qquad \frac{\Gamma \vdash Nx, \Delta}{\Gamma \vdash Nsx, \Delta}$$

and the elimination rule

$$\frac{\Gamma \vdash F0, \Delta \quad \Gamma, Fx \vdash Fsx, \Delta \quad \Gamma, Ft \vdash \Delta}{\Gamma, Nt \vdash \Delta}$$

This elimination rule describes mathematical induction principle restricted to N. LKID is sound with respect to a class of models called Henkin models (Def. 2.10 of [6]). We omit the definition of Henkin models and we only use the following property: if a first order structure $\mathcal{M}$ satisfies the induction schema for N, then $\mathcal{M}$ is an Henkin model of LKID with the predicate N.

2.2 Cyclic Proof System $\mathtt{CLKID}^\omega$

A cyclic proof system $\mathtt{CLKID}^\omega$ [6] is defined as a system obtained from LKID by (1) replacing elimination rules by case rules, (2) allowing a bud as an open assumption and requiring a companion for each bud, (3) requiring the global trace condition.

The case rule is defined by unfolding the production rule in the antecedent. For example, the case rule for N is

$$\frac{\Gamma, t = 0 \vdash \Delta \quad \Gamma, t = sx, Nx \vdash \Delta}{\Gamma, Nt \vdash \Delta}$$

In a cyclic proof, we can have open assumptions, called *buds*, but it is required that each bud has some corresponding sequent of the same form, called a *companion*, inside the proof figure.

An example of a cyclic proof is

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash N0}}{\vdash Ns0}}{\vdash Nss0} \quad \dfrac{\dfrac{(a)Nx \vdash Nssx}{Nx' \vdash Nssx'}\ (\text{subst})}{Nx' \vdash Nsssx'}}{(a)Nx \vdash Nssx}\ (case)$$

where the mark (a) denotes the bud-companion pair. Remark that the companion (a) uses Nx, but the bud (a) uses Nx where x is x', so their actual meanings are different even though they are of the same form.

A *pre-proof* of $\texttt{CLKID}^\omega$ is obtained by recursively replacing every bud by the proof of its companion. A *trace* is a sequence of occurrences of an atom in a path of the proof tree, possibly moving to a case-descendant when passing through a case rule. Moving to a case-descendant is called a *progress point* of the trace (Def. 5.4 [6]). The *global trace condition* says that for every infinite path there is a trace with infinitely many progress points following some tail of the path (Def. 5.5 [6]). The global trace condition guarantees the soundness of a cyclic proof system for fixed-point models. $\texttt{CLKID}^\omega$ is not known to be sound for Henkin models, and this leaves the possibility of having an Henkin counter-model for a theorem of $\texttt{CLKID}^\omega$.

2.3 Brotherston-Simpson Conjecture

LKID has been often used for formalizing inductive definitions, while $\texttt{CLKID}^\omega$ is another way for formalizing inductive definitions, and moreover $\texttt{CLKID}^\omega$ is more suitable for proof search. This raises the question of the relationship between LKID and cyclic proofs: Brotherston and Simpson conjectured the equality for each inductive definition. The left-to-right inclusion is proved in [3], Lemma 7.3.1 and in [6], Thm. 7.6. Brotherston-Simpson conjecture (the conjecture 7.7 in [6]) is that the provability LKID includes that of $\texttt{CLKID}^\omega$. Simpson [11] submitted a proof of the conjecture in the case of Peano Arithmetic. The goal of this paper is to prove that it is false in general.

3 2-Hydra Problem

3.1 Hydra Problem

The Hydra of Lerna was a mythological monster, popping two smaller heads whenever you cut one. It was a swamp creature (its name means "water") and possibly was the swamp itself, whose heads are the swamp plants, with two smaller plants growing whenever you cut one. The original Hydra was defeated by fire, preventing heads to grow again. In the mathematical problem of Hydra, we ask whether we may destroy an Hydra just by cutting heads.

Laurence Kirby and Jeff Paris [9] formulated the Hydra problem as a statement for mathematical trees. We are interested about making Hydra a problem for natural numbers, representing the length of a head, and restricting to the case when the number of heads is always 2. We call our statement 2-Hydra.

3.2 2-Hydra Statement

In this subsection we give the 2-Hydra statement, which is a formula saying that any 2-hydra eventually looses its two heads. This statement actually will give a counterexample to Brotherston-Simpson conjecture.

Let Σ_N be the signature $\{0, s, N, p\}$ of a first order language, where 0, the successor s, an inductive predicate N for natural numbers, and an ordinary binary predicate symbol p. The logical system $\texttt{LKID}(\Sigma_N, \Phi_N)$ is defined as the system LKID with the signature Σ_N and the production rules Φ_N.

We consider a formal statement of 2-Hydra. The number of head is always 2. Either both heads have positive length, you reduce the length of the first head by 1 unit, and of the second head by 2 units (if possible), or there is a unique head with positive length, you duplicate it and you reduce it by 1 and by 2 units (if possible). We may express H by the convergence of the following set of transformations on $n, m \in \texttt{Nat}$: if $n \geq 1$ and $m \geq 2$ then $(n, m) \mapsto (n-1, m-2)$; if $n \geq 2$ then $(n, 0) \mapsto (n-1, n-2)$; if $m \geq 2$ then $(0, m) \mapsto (m-1, m-2)$. When no transformation applies we stop. We may define H by a formula in the language Σ_N: the intended meaning of p is the complement of the union of all infinite sequences of transformations. From now on, we write $A_1, \ldots, A_n \to B$ for $A_1 \wedge \ldots \wedge A_n \to C$ and $\forall x_1, \ldots, x_n \in N.\ A$ for $\forall x_1.\ \ldots.\ \forall x_n.\ N(x_1) \wedge \ldots \wedge N(x_n) \to A$.

Definition 1 (2-Hydra Statement H). *We define $H = (H_a, H_b, H_c, H_d \to \forall x, y \in N.\ p(x, y))$, where H_a, H_b, H_c, H_d are:*

(H_a) $\forall x \in N.\ p(0,0) \wedge p(s0,0) \wedge p(x, s0)$,

(H_b) $\forall x, y \in N.\ p(x, y) \to p(sx, ssy)$,

(H_c) $\forall y \in N.\ p(sy, y) \to p(0, ssy)$,

(H_d) $\forall x \in N.\ p(sx, x) \to p(ssx, 0)$.

For all $n, m \in \texttt{Nat}$ there is a unique formula among H_a, H_b, H_c, H_d having some instance inferring $p(n, m)$. The assumption $p(n', m')$ of such a formula, if any assumption exists, satisfies $\max(n', m') < \max(n, m)$. Thus, we may prove H in PA by induction on $\max(n, m)$. We could define p as an inductive predicate: however, we preferred having p just a predicate symbol, because in this way the definition of a counter-model does not require to check the inductive rule for p.

We will prove that $\texttt{LKID}(\Sigma_N, \Phi_N) + (0, s)$-axioms does not prove 2-Hydra. We define the $(0, s)$-axioms as the axioms "0 is not successor" or $\forall x \in N.\ sx \neq 0$, and "successor is injective", or $\forall x, y \in N.\ sx = sy \to x = y$. These axioms cannot be proved in $\texttt{LKID}(\Sigma_N, \Phi_N)$, because they fail, respectively, in the model of $\texttt{LKID}(\Sigma_N, \Phi_N)$ uniquely determined by $\mathcal{M} = N_{\mathcal{M}} = \{0\}$, $s0 = 0$, in the model uniquely determined by $\mathcal{M} = N_{\mathcal{M}} = \{0, s0\}$, $0 \neq s0$ and $ss0 = s0$. Compared with PA, in $\texttt{LKID}(\Sigma_N, \Phi_N) + (0, s)$-axioms we do not have a sum nor a product on N, nor we have inductive predicate symbols for addition or multiplication.

3.3 2-Hydra Statement in Cyclic-Proof System

In this section, we give a cyclic proof of the 2-Hydra statement.

We define the logical system $\texttt{CLKID}^\omega(\Sigma_N, \Phi_N)$ as the system $\texttt{CLKID}^\omega$ with the signature Σ_N and the production rules Φ_N.

Theorem 1. *The 2-Hydra statement H is provable in* $\texttt{CLKID}^\omega(\Sigma_N, \Phi_N)$.

Proof. Let the 2-Hydra axioms $\hat{H}$ be H_a, H_b, H_c, H_d defined in Definition 1.

For simplicity, we will write the use of 2-Hydra axioms by omitting (Cut), $(\to R)$, $(\forall\ R)$, (Axiom), as in the following example.

$$\frac{\hat{H}, Nsy'', Ny'' \vdash psy''y''}{\hat{H}, Nsy'', Ny'' \vdash p0ssy''}$$

We will also write a combination of (Case) and (=L) as one rule in the following example.

$$\frac{\hat{H} \vdash p00 \quad \hat{H}, Nx' \vdash psx'0}{\hat{H}, Nx \vdash px0}\ Nx$$

For saving space, we omit writing $\hat{H}$ in every sequent int the next proof figure. For example, $Nx, Ny \vdash pxy$ actually denotes $\hat{H}, Nx, Ny \vdash pxy$.

The following is a cyclic proof of $Nx, Ny \vdash pxy$.

$$\dfrac{\dfrac{\dfrac{}{\vdash p00}\quad \dfrac{\dfrac{\dfrac{(a)Nx, Ny \vdash pxy}{Nsx'', Nx'' \vdash psx''x''}}{N0 \vdash p10}\quad Nsx'', Nx'' \vdash psx''0}{Nx' \vdash psx'0}\ Nx}{Nx \vdash px0}\quad \dfrac{\dfrac{\dfrac{(a)Nx, Ny \vdash pxy}{Nsy'', Ny'' \vdash psy''y''}}{N0, Nx \vdash px1}\quad Nsy'', Ny'' \vdash p0ssy''}{Nsy'', Nx, Ny'' \vdash pxssy''}\quad \dfrac{\dfrac{(a)Nx, Ny \vdash pxy}{Nx', Ny'' \vdash px'y''}}{Nsy'', Nx', Ny'' \vdash psx'ssy''}\ Nx}{Nx, Ny' \vdash pxsy'}\ Ny}{(a)Nx, Ny \vdash pxy}$$

The global trace condition holds for the following reason (the detailed proof is in §A). We have three possible choices for constructing an infinite path in the proof: taking a bud of the left, middle, or right. For a given bud and $z_1, z_2 \in \{x, y\}$, we write $z_1 \rightsquigarrow z_2$ for a progressing trace from Nz_1 in the companion to Nz_2 in the bud. We write $z_1 \rightsquigarrow z_2, z_3$ for $z_1 \rightsquigarrow z_2$ and $z_1 \rightsquigarrow z_3$. For the left bud, there are $x \rightsquigarrow x, y$. For the middle bud, there are $y \rightsquigarrow x, y$. For the left bud, there are $x \rightsquigarrow x$ and $y \rightsquigarrow y$. Hence, given an infinite path, there is some tail of the path with an infinitely progressing trace, by cleverly choosing x and y possibly alternatively. Hence the global trace condition holds. □

4 A Structure $\mathcal{M}$ for the Language Σ_N Falsifying 2-Hydra

In this section we define a structure $\mathcal{M}$ for the language Σ_N, we prove that $\mathcal{M}$ falsifies the 2-Hydra statement H, and we characterize the subsets of $\mathcal{M}$ which satisfy the induction schema.

4.1 Outline of Proof of Non-Provability

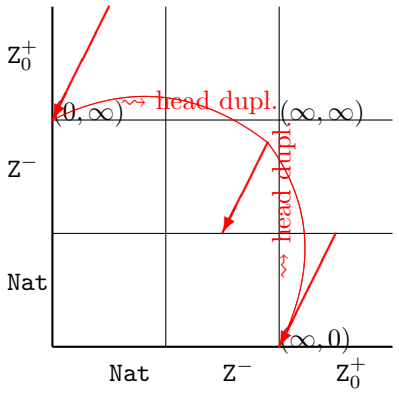
In Section 4, we define a counter model $\mathcal{M}$. The most difficult point is to prove that $\mathcal{M}$ satisfies Def. 2.10 of [6] for having an Henkin model of $\mathtt{LKID} + \Sigma_N$. We will prove a sufficient condition for it, the induction schema for N.

On one hand, we prove that in our structure $\mathcal{M}$ all unary definable predicates of $\mathcal{M}$ are sets whose measure is some dyadic rational number. This involves proving a quantifier-elimination result (§6) for a theory of partial equivalence relations (§5). This result is new, as far as we know: for an introduction to quantifier-elimination we refer to [8], §3.1, §3.2). On the other hand, §4.3 shows that a definable set of $\mathcal{M}$ with dyadic measure satisfies the induction schema. Combining them, finally we will show that $\mathcal{M}$ satisfies the induction schema for N and according to Def. 2.10 of [6] is an Henkin model of $\mathtt{LKID} + \Sigma_N$.

4.2 Definition of the Structure $\mathcal{M}$

Let $\mathtt{Z}$ be the set of relative integers. $\mathcal{M}$ is $\mathtt{Nat} + \mathtt{Z}$: we represent $\mathtt{Nat} + \mathtt{Z}$ by $\{(1,x) \mid x \in \mathtt{Nat}\} \cup \{(2,x) \mid x \in \mathtt{Z}\}$. We first define the interpretations $0_\mathcal{M}, s_\mathcal{M}, N_\mathcal{M}$. $0_\mathcal{M}$ is 0 in the component $\mathtt{Nat}$ and $s_\mathcal{M}$ is the successor on $\mathtt{Nat}$ and on $\mathtt{Z}$. We choose $N_\mathcal{M} = \mathcal{M}$: by construction, $\mathcal{M}$ satisfies the $(0,s)$-axioms. We abbreviate $x + n = s^n_\mathcal{M}(x)$, ∞ for the 0 in the component $\mathtt{Z}$, and $\infty - n$ for the relative integer $-n$ in the component $\mathtt{Z}$, for all $n \in \mathtt{Nat}$. We define the following subsets of $\mathcal{M}$: $\underline{\mathtt{Nat}} = \{0_\mathcal{M} + n | n \in \mathtt{Nat}\}$ and $\underline{\mathtt{Z}}^- = \{\infty - (n+1) | n \in \mathtt{Nat}\}$ and $\underline{\mathtt{Z}}^+_0 = \{\infty + n | n \in \mathtt{Nat}\}$. The sets $\underline{\mathtt{Nat}}$, $\underline{\mathtt{Z}}^-$, $\underline{\mathtt{Z}}^+_0$ are a partition of $\mathcal{M}$.

In order to complete the definition of $\mathcal{M}$ we have to choose the interpretation $p_\mathcal{M}$ of the binary predicate p. We first define $\pi = \{(n, 2n) | n \in \mathtt{Nat}\} \subseteq \mathtt{Nat} \times \mathtt{Nat}$. π is the set of points of the straight line $y = 2x$ whose coordinates are some pair of natural numbers. We imagine π starting from the infinite, moving at each step from some (sa, ssb) to (a,b), and ending in $(0,0)$. Given any $(m_1, m_2) \in \mathcal{M} \times \mathcal{M}$ we define $(m_1, m_2) + \pi = \{(m_1 + a, m_2 + b) | (a,b) \in \pi\}$ and $(m_1, m_2) - \pi = \{(m_1 - a, m_2 - b) | (a,b) \in \pi\}$. We define three paths in $\mathcal{M} \times \mathcal{M}$ by $\pi_1 = (0_\mathcal{M}, \infty) + \pi$ and $\pi_2 = (\infty, 0_\mathcal{M}) + \pi$ and $\pi_3 = (\infty - 1, \infty - 2) - \pi$. Eventually, we set $p_\mathcal{M} = \mathcal{M}^2 \setminus (\pi_1 \cup \pi_2 \cup \pi_3)$. As explained in the figure below, we may move forever along $\pi_1 \cup \pi_2 \cup \pi_3$ (in red) while "cutting heads" as follows: $\ldots \mapsto (0_\mathcal{M} + 2, \infty + 4) \mapsto (0_\mathcal{M} + 1, \infty + 2) \mapsto (0_\mathcal{M}, \infty) \mapsto (\infty - 1, \infty - 2) \mapsto (\infty - 2, \infty - 4) \mapsto \ldots$.



Lemma 1 (The 2-Hydra Lemma). *H is false in $\mathcal{M}$*

$\mathcal{M}$ satisfies by construction the closure of N under 0 and s, and the $(0,s)$-axioms. In order to prove that $\mathcal{M}$ is a model for $\mathtt{LKID}(\Sigma_N, \Phi_N) + (0,s)$-axioms, we have to prove that $\mathcal{M}$ satisfies Def. 2.10 of [6], Def. 2.10). Let $\mathcal{H}$ be the set of definable predicates of $\mathcal{M}$. A predicate $P \subseteq \mathcal{M}^n$ is definable in $\mathcal{M}$ if for some formula A in the language Σ_N plus constants denoting the elements of $\mathcal{M}$, and with free variables in $x_1, \ldots, x_n$, we have $P = \{(m_1, \ldots, m_n) \in \mathcal{M}^n | \mathcal{M} \models A[m_1/x_1, \ldots, m_n/x_n]\}$. We write $\mathcal{H}_n$ for the subset of definable predicates of arity n: we call $\mathcal{H}_1$ the set of definable *sets* of $\mathcal{M}$. According to Def. 2.10 of [6], we have to prove that $\mathcal{M}$ is the smallest pre-fixed point in $\mathcal{H}_1$ for the inductive definition of N: a sufficient condition is to prove the induction schema, that all $X \in \mathcal{H}_1$ which are closed under 0 and s are equal to $\mathcal{M}$.

4.3 The Measure of the Subsets of $\mathcal{M}$ Closed Under 0 and s

In this subsection we define a sufficient condition for a predicate on $\mathcal{M}$ to satisfy the induction schema, by using a finitely additive measure $\mu(X)$, defined on some subsets $X \subseteq \mathcal{M}$. We will prove that all definable subsets of $\mathcal{M}$ satisfy this condition.

Definition 2 (Measure of a Subset of $\mathcal{M}$). *For any $X \subseteq \mathcal{M}$ we set: $\mu(X) = \lim_{x\to\infty} \frac{\mathtt{card}(\{0_{\mathcal{M}}+n, \infty-n, \infty+n \in \mathcal{M} | n \in [0,x]\} \cap X)}{3(x+1)}$ whenever this limit exists.*

For instance, $\mu(\underline{\mathtt{Nat}}) = 1/3$ and if $E = \{0_{\mathcal{M}}, 0_{\mathcal{M}}+2, \ldots, \infty-2, \infty, \infty+2, \ldots\}$, then $\mu(E) = 1/2$. We may now provide a sufficient condition for a predicate to satisfy the induction rule.

Lemma 2 (Measure Lemma). *If $\mu(P)$ is a dyadic rational, then P satisfies the induction schema.*

An example: if $P = \underline{\mathtt{Nat}} \cup \underline{\mathtt{Z}}_0^+$, then P is closed under 0, s and $\infty - 1 \notin P$. P does *not* satisfy the induction schema and $\mu(P) = 2/3$ is *not* dyadic.

5 A Set $\mathcal{R}$ of Partial Bijections on $\mathcal{M}$

In this section we introduce some set $\mathcal{R}$ of partial bijections on $\mathcal{M}$, whose domain have measure some dyadic rational. In §6, 7 we will prove that all definable predicates in $\mathcal{M}$ are a boolean combination of atomic formulas of the language $\mathcal{R}$, and that all definable sets in $\mathcal{M}$ are domains of bijections in $\mathcal{R}$, therefore all have measure some dyadic rational, and by Lemma 2 satisfy the induction schema. We will conclude that $\mathcal{M}$ is an Henkin model of $\mathtt{LKID} + \Sigma_N$.

We say that a relation R is finite if there are finitely many pairs $(x,y) \in R$. For any set X and any binary relations R, S we write: $\mathtt{id}_X = \{(x,x) | x \in X\}$, $\mathtt{dom}(R) = \{x | \exists y.(x,y) \in R\}$, $\mathtt{codom}(R) = \{y | \exists x.(x,y) \in R\}$, $R^{-1} = \{(y,x) | (x,y) \in R\}$, $R \circ S = \{(x,z) | \exists y.((x,y) \in S) \wedge ((y,z) \in R)\}$ and $R\lceil X = \{(x,y) \in R | x \in X\}$. Remark that we defined relation composition *in the same order as function composition*: the reason is that we will only consider relations which are partial bijections.

5.1 The Set $\mathcal{D}$ of Subsets of $\mathcal{M}$

In this subsection we propose a candidate $\mathcal{D}$ for the definable subsets of $\mathcal{M}$.

For any sets I, J we define $I \subseteq_\sim J$ as "$(I \setminus J)$ is finite": this means "$I \subseteq J$ up to finitely many elements. We define $I \sim J$ as $I \subseteq_\sim J \wedge J \subseteq_\sim I$: this means "$I, J$ are equal up to finitely many elements". $I \sim J$ is equivalent to: $(I \setminus J) \cup (J \setminus I)$ is finite.

For any $r, s \in \mathtt{Q}$ we introduce the formal notations $0_{\mathcal{M}}+r$, $\infty+s$: they denote elements of $\mathcal{M}$ if and only if $r \in \mathtt{Nat}$, $s \in \mathtt{Z}$. For any $z \in \mathtt{Z}$, $r \in \mathtt{Q}$, we define the set of formal notations $M(2^z, r) = \{0_{\mathcal{M}} + (2^z * n + r), \infty + (2^z * w + r) | (n \in \mathtt{Nat}) \wedge (w \in \mathtt{Z})\}$. We denote with $\mathcal{B}$ the set of all sets $M(2^z, r)$, for some $z \in \mathtt{Z}$, $r \in \mathtt{Q}$.

We define $\mathcal{D}$ as the family of subsets of $\mathcal{M}$ which are equivalent, up to finitely many elements, to some finite union of sets in $\mathcal{B}$.

Definition 3 (The Family $\mathcal{D}$). *$D \in \mathcal{D}$ if and only if $D \sim (B_1 \cup \ldots \cup B_n)$ for some $B_1, \ldots, B_n \in \mathcal{B}$. We call $\mathcal{D}$ the dyadic family.*

Since $2^z > 0$, all sets $M(2^z, r)$ are infinite. We have $M(2^z, r) \subseteq_\sim \mathcal{M}$ if and only if $(2^z * n + r) \in \mathtt{Nat}$ for all but finitely many $n \in \mathtt{Nat}$ and $(2^z * w + r) \in \mathtt{Z}$ for all but finitely many $w \in \mathtt{Z}$. We may check that this is equivalent to: $z \in \mathtt{Nat}$ and $r \in \mathtt{Z}$.

We prove that every set in $\mathcal{D}$ has measure some dyadic rational.

Lemma 3 ($\mathcal{D}$-Lemma). *Let $a_0, a \in \mathtt{Z}$ and $D \in \mathcal{D}$.*

1. *All finite subsets of $\mathcal{M}$ are in $\mathcal{D}$.*
2. *For all $a \geq a_0$ there are $0 \leq b_1 < \ldots < b_i < 2^a$ such that $M(2^{a_0}, b) = (M(2^a, b_1) \cup \ldots \cup M(2^a, b_i))$.*
3. *For some a_0 and for all $a \geq a_0$ there are $0 \leq b_1, \ldots, b_i < 2^a$ such that $D \sim (M(2^a, b_1) \cup \ldots \cup M(2^a, b_i))$.*
4. *$\mu(D)$ is some dyadic rational.*
5. *$\mathcal{D}$ is closed under $\sim$ and all boolean operations.*

5.2 The Family $\mathcal{R}$ of Partial Bijections on $\mathcal{M}$

In this subsection we define a family $\mathcal{R}$ of partial bijections on $\mathcal{M}$ with domain in $\mathcal{D}$. The elements of $\mathcal{R}$ up to finitely many elements are empty or are some power of the complement of $p_{\mathcal{M}}$, restricted to some $D \in \mathcal{D}$.

We define first some set $\mathcal{F}$ of straight lines. $\mathcal{F}$ is the set of maps $\phi : \mathtt{Q} \to \mathtt{Q}$, defined by $\phi(x) = 2^z x + r$ for some $z \in \mathtt{Z}$ and some $r \in \mathtt{Q}$. $\mathcal{F}$ is closed under inverse: if $\phi(x) = 2^z x + r$, then $\phi^{-1}(x) = 2^{-z} x - r/2^z$. $\mathcal{F}$ is closed under composition: if $\phi_i(x) = 2^{z_i} x + r_i$ for $i = 1, 2$, then $\phi_2(\phi_1(x)) = 2^{z_1+z_2} x + (2^{z_2} r_1 + r_2)$.

Let $\mathtt{Q} + \mathtt{Q} = \{(i, r) | i = 1, 2 \wedge r \in \mathtt{Q}\}$. We extend $\phi : \mathtt{Q} \to \mathtt{Q}$ to a map $: \mathcal{M} \to \mathtt{Q} + \mathtt{Q}$ by $\phi((i, r)) = (i, \phi(r))$ (recall that each element of $\mathcal{M}$ is coded by some pair (i, r)). For any $D \subseteq \mathcal{M}$ we define $\phi(D) = \{\phi(d) | d \in D\} \subseteq \mathtt{Q} + \mathtt{Q}$. We provide a sufficient condition for having $\phi(D) \subseteq \mathcal{M}$ and $\phi(D) \in \mathcal{D}$.

Lemma 4 (ϕ-Lemma). *Let $\phi(x) = 2^{z_1}x + r_1$ for some $z_1 \in \mathtt{Z}$ and some $r_1 \in \mathtt{Q}$ and all $x \in \mathtt{Q}$. Assume $M(2^z, r) \in \mathcal{B}$.*

1. *$\phi(M(2^z, r)) \in \mathcal{B}$.*
2. *If $D \in \mathcal{D}$ and $\phi(D) \overset{\subseteq}{\sim} \mathcal{M}$ then $\phi(D) \in \mathcal{D}$.*

Proof. 1. We have $\phi(M(2^z, r)) = M(2^{z+z_1}, 2^{z_1}r + r_1) \in \mathcal{B}$.

2. If $D \in \mathcal{D}$ then $D \sim M(2^{a_1}, b_1) \cup \ldots \cup M(2^{a_i}, b_i)$ for some $a_1, \ldots, a_i \in \mathtt{Z}$ and some $b_1, \ldots, b_i \in \mathtt{Q}$. Then $\phi(D) \sim \phi(M(2^{a_1}, b_1)) \cup \ldots \cup \phi(M(2^{a_i}, b_i))$, and by point 1 above $\phi(M(2^{a_1}, b_1)) \cup \ldots \cup \phi(M(2^{a_i}, b_i)) \in \mathcal{B}$. Thus, $\phi(D) \in \mathcal{D}$.

A *partial bijection* on $\mathcal{M}$ is a bijection between two subsets of $\mathcal{M}$. We now define a family $\mathcal{R}$ of partial bijections on $\mathcal{M}$. For instance, one bijection in $\mathcal{R}$ is defined by $\phi(x) = 4x$, with domain $\mathcal{M}$ and codomain $M(4, 0)$, mapping $0_\mathcal{M} + n \mapsto 0_\mathcal{M} + 4n$ and $\infty + z \mapsto \infty + 4z$.

Let $\phi \in \mathcal{F}$, $\phi(x) = 2^z x + r$ with $z \in \mathtt{Z}$ and $r \in \mathtt{Q}$. We say that ϕ is *even* if z even, and that ϕ is *odd* if z is odd. We divide infinite bijections in $\mathcal{R}$ between "even" and "odd". They will be restrictions of an even or odd power of the relation $Q = \mathcal{M}^2 \setminus p_\mathcal{M}$, up to finitely many point. We will prove that the first order definable predicates of $\mathcal{M}$ are the propositional formulas of $\mathcal{R}$.

Definition 4 (Even Bijections). *Let $D, E \in \mathcal{D}$ and $\phi \in \mathcal{F}$ be even. R is an even (D, E, ϕ)-bijection if D, E are infinite, R is a bijection between D, E, and R is equal up to finitely many elements to the graph of ϕ restricted to D, E: $R \sim \{(x, y) \in D \times E | y = \phi(x)\}$. We denote the set of even bijections with $\mathcal{R}^+$.*

Q is a partial bijection on $\mathcal{M}$, and by definition Q maps $0_\mathcal{M} + n \mapsto \infty + 2n$ and $\infty + n \mapsto 0_\mathcal{M} + 2n$, and Q is associated to the odd map $\phi(x) = 2x$.

Definition 5 (Odd Bijections). *Let $\phi \in \mathcal{F}$ be odd. An odd (D, E, ϕ)-bijection is any bijection R between some infinite $D, E \in \mathcal{D}$, such that, up to finitely many points, R maps: (1) $\infty - n - 1 \mapsto \infty + \phi(-n - 1)$, (2) $0_\mathcal{M} + n \mapsto \infty + \phi(n)$ and $\infty + n \mapsto 0_\mathcal{M} + \phi(n)$. We denote the set of odd bijections with $\mathcal{R}^-$.*

Q is an example of odd bijection. Let $\phi \in \mathcal{F}$ be even and $D, E \in \mathcal{D}$. A (D, E, ϕ)-even bijection may alternatively be defined as any bijection between D, E such that, up to finitely many points: (1) $\infty - n - 1 \mapsto \infty + \phi(-n - 1)$, (2) $0_\mathcal{M} + n \mapsto 0_\mathcal{M} + \phi(n)$ and $\infty + n \mapsto \infty + \phi(n)$.

We define $\mathcal{R}_0$ as the set of all bijections between finite sets $D, E \in \mathcal{D}$. Eventually, we define a family $\mathcal{R}$ of partial bijections by $\mathcal{R} = \mathcal{R}^+ \cup \mathcal{R}_0 \cup \mathcal{R}^-$.

If $R \in \mathcal{R}^+ \cup \mathcal{R}^-$, associated to the map $\phi \in \mathcal{F}$ with domain D and codomain E, then we may prove that $E \sim \phi(D)$. $\mathcal{R}$ and $\mathcal{D}$ satisfy the following closure properties.

Lemma 5 (Partial bijections). *Assume that $R, S \in \mathcal{R}$ and $D \in \mathcal{D}$.*

1. *$\mathtt{id}_D \in \mathcal{R}$*
2. *If $D \in \mathcal{D}$ then $R(D) \in \mathcal{D}$*

3. $R \circ S \in \mathcal{R}$.
4. $R^{-1} \in \mathcal{R}$
5. $\mathcal{D}$ *is closed under complement.*

$\mathcal{R}$ is closed under intersection.

Lemma 6 (Closure Under Intersection). *Assume that $R, S \in \mathcal{R}$ are associated to $\phi, \psi \in \mathcal{F}$.*

1. *If $\phi = \psi$ then $R \cap S \in \mathcal{R}$*
2. *If $\phi \neq \psi$ then $R \cap S \in \mathcal{R}$*
3. $\mathcal{R}$ *is closed under intersections.*
4. *For all $R \in \mathcal{R}$ there is some $D \in \mathcal{D}$ such that $R \cap \mathtt{id}_{\mathcal{M}} = \mathtt{id}_D$.*

Our goal is to prove that every first-order definable subset of $\mathcal{M}$ is in $\mathcal{D}$. Since the sets definable in the language of $\mathcal{R}$ include those definable in $\mathcal{M}$, it is enough to prove that any first-order definable set in language of $\mathcal{R}$ is in $\mathcal{D}$. To this aim, we need a quantifier-elimination result for the language of $\mathcal{R}$.

6 A Quantifier Elimination Result for Partial Bijections

In this section we prove a quantifier elimination result for a theory of partial equivalence relation, which is the abstract counterpart of the families $\mathcal{R}$ and $\mathcal{D}$ introduced in the previous section. This is a simple, self-contained result introducing a model-theoretical tool of some interest.

Theorem 2 (Quantifier Elimination for Partial Bijections).
Let U be a set and $\mathcal{R}$ a set of partial bijections on U. Assume that all finite partial bijections on U are in $\mathcal{R}$, that $\mathcal{D} = \{\mathtt{dom}(R) | R \in \mathcal{R}\}$ is closed under complement, and that for all $R, S \in \mathcal{R}$, $D \in \mathcal{D}$ we have $\mathtt{id}_U, R^{-1}, R \circ S \in \mathcal{R}$ and $R \cap S, R\lceil D \in \mathcal{R}$. Let $\mathcal{U}$ be the structure with universe U, one constant denoting each element of U, and one predicate symbol denoting each $R \in \mathcal{R}$. Then:

1. *The theory of $\mathcal{U}$ has quantifier-elimination.*
2. *Any set definable in $\mathcal{U}$ is in $\mathcal{D}$ and is $R(x, x)$ for some $R \in \mathcal{R}$.*

In order to give a flavor of our quantifier elimination procedure, we give an example: detailed proofs are in §A.

$$\exists x_4 (R_1 x_1 x_4 \wedge R_2 x_2 x_4 \wedge \neg R x_3 x_4)$$

is equivalent to

$$\exists x_4 (R_{1,4} x_1 x_4 \wedge R_{2,4} x_2 x_4 \wedge \neg R x_3 x_4)$$

where $D_4 = \mathtt{codom}(R_1) \cap \mathtt{codom}(R_2)$, $D_1 = R_1^{-1}(D_4)$, $D_2 = R_2^{-1}(D_4)$, and $R_{1,4} = R_1 \cap (D_1 \times D_4)$, $R_{2,4} = R_2 \cap (D_2 \times D_4)$. Note domain restriction here. It is equivalent to

$$\exists x_4 (R_{1,4} x_1 x_4 \wedge R_{2,4} x_2 x_4 \wedge R_{1,2} x_1 x_2 \wedge \neg R x_3 x_4)$$

where $R_{1,2} = R_{2,4}^{-1} \circ R_{1,4}$. Note composition of relations here. It is equivalent to

$$\exists x_4 (R_{1,4} x_1 x_4 \wedge R_{2,4} x_2 x_4 \wedge R_{1,2} x_1 x_2 \wedge \neg R' x_3 x_2)$$

where $R' = R_{2,4}^{-1} \circ R$. Note partial bijections here. It is equivalent to

$$\exists x_4 (R_{1,4} x_1 x_4 \wedge R_{2,4} x_2 x_4) \wedge R_{1,2} x_1 x_2 \wedge \neg R' x_3 x_2$$

Using the properties of partial bijections, finally this is equivalent to

$$R_{1,2} x_1 x_2 \wedge \neg R' x_3 x_2.$$

In the proof we identify each constant symbol with the element $c \in U$ it denotes, and each predicate symbol with the relation $R \in \mathcal{R}$ it denotes. We prove quantifier elimination for $\mathcal{U}$ as defined in [8], §3.1, §3.2, namely that each formula A with possibly free variables in the language $U \cup \mathcal{R}$ is equivalent in $\mathcal{U}$ to some formula B in the same language but without quantifiers. We will in fact prove a little more, namely that B may be chosen without constants.

We derive some closure properties for $\mathcal{R}$. For any $D \in \mathcal{D}$ we have $\mathtt{id}_D = (\mathtt{id}_{\mathcal{M}} \lceil D) \in \mathcal{R}$. We will abbreviate $\mathtt{id}_D(x, x)$ with $(x \in D)$. $\mathcal{D}$ is closed under intersection, because if $D, E \in \mathcal{D}$ then $\mathtt{id}_D, \mathtt{id}_E \in \mathcal{R}$, hence $\mathtt{id}_{D \cap E} = (\mathtt{id}_D \cap \mathtt{id}_E) \in \mathcal{R}$ and $D \cap E \in \mathcal{D}$. $\mathcal{D}$ includes $\mathcal{M} = \mathtt{dom}(\mathtt{id}_{\mathcal{M}})$ and it is closed under complement, therefore $\mathcal{D}$ is closed under all boolean operations. For all $x \in \mathcal{M}$ the partial bijection $\mathtt{id}_{\{x\}}$ is finite and by assumption it is in $\mathcal{R}$: thus, all singletons of $\mathcal{M}$ are in $\mathcal{D}$. Assume $R \in \mathcal{R}$ and $D \in \mathcal{D}$: then $\mathtt{codom}(R) = \mathtt{dom}(R^{-1}) \in \mathcal{D}$ and $R(D) = (R \lceil D)(D) = \mathtt{codom}(R \lceil D) \in \mathcal{D}$. If $R \in \mathcal{R}$ and $D, E \in \mathcal{D}$, then $R \cap (D \times E) \in \mathcal{R}$ follows from $R \cap (D \times E) = (((R \lceil D)^{-1}) \lceil E)^{-1}$.

In the next statement, recall that we defined the relation composition in the same order as function composition.

Lemma 7 (Composition and Product). *Let R, S be any relation and D, E, F be any sets. Assume $R(D) \cap S^{-1}(F) \subseteq E$. Then composition and Cartesian product commute: $(S \cap (E \times F)) \circ (R \cap (D \times E)) = (S \circ R) \cap (D \times F)$*

6.1 A Notion of Normal Form for the Language $\mathcal{R}$

Let $n > 0$ be any positive integer. Assume $R \in \mathcal{R}$ and $i, j \in \{1, \ldots, n\}$. We call any formula $R(x_i, x_j)$ a *positive* $(\mathcal{R}, n)$-atom and any formula $\neg R(x_i, x_j)$ a *negative* $(\mathcal{R}, n)$-atom. A $(\mathcal{R}, n)$-atom is either a positive or a negative $(\mathcal{R}, n)$-atom. A $(\mathcal{R}, n)$-propositional formula is any formula obtained from positive $(\mathcal{R}, n)$-atoms by repeatedly applying disjunction and negation. Any $(\mathcal{R}, n)$-propositional formula has free variables in $x_0, \ldots, x_{n-1}$. We denote by $\mathcal{A}_n$ the set of $(\mathcal{R}, n)$-propositional formula, and by $\mathcal{H}_n$ the set of n-ary predicates definable in $\mathcal{U}$.

Our goal is to prove that for all $n \in \mathtt{Nat}$, any first-order predicate P of $\mathcal{R}$ is definable by some $A \in \mathcal{A}_n$, and if $n = 1$ then $P \in \mathcal{D}$. We have to prove that formulas of $\mathcal{A}_n$ are closed under existential.

This is the plan of the proof. We will define a notion of $(\mathcal{R}, n)$-normal form for formulas of $\mathcal{A}_n$, and prove that every $A \in \mathcal{A}_n$ has some $(\mathcal{R}, n)$-normal form. Then we will prove that if $A \in \mathcal{A}_n$ is in $(\mathcal{R}, n)$-normal form, then $\exists x_n.A$ (with possibly free variables) may be expressed in $\mathcal{A}_{n-1}$ in one of the following ways: either as some finite disjunction $A[c_1/x_1] \vee \ldots \vee A[c_k/x_n]$ for some constants $c_1, \ldots, c_k \in U$, or by the formula $B \in \mathcal{A}_{n-1}$, obtained from A by erasing all $(\mathcal{R}, n)$-atoms including x_n.

Assume $n > 0$ is any positive integer. Let $\mathcal{G}$ be any binary relation on $\{1, \ldots, n\}$. A $(\mathcal{G}, n)$-*family* is any family $\mathcal{F} = \{R_{i,j}(x_i, x_j) | (i, j) \in \mathcal{G}\}$ of *positive* $(\mathcal{R}, n)$-atoms such that $\mathtt{dom}(R_{i,j}) = \mathtt{dom}(R_{i,k})$ for all $i, j, k = 1, \ldots, n$. $\mathcal{F}$ is a *symmetric family* if $\mathcal{G}$ is a symmetric relation, and for all $(i, j) \in \mathcal{G}$ we have $R_{i,j} = R_{i,j}^{-1}$. $\mathcal{F}$ is a *equivalence family* if $\mathcal{G}$ is an equivalence relation, and for all $i = 1, \ldots, n$ we have $R_{i,i} = \mathtt{id}_{D_i}$ for some D_i, for all $(i, j) \in \mathcal{G}$ we have $R_{i,j} = R_{i,j}^{-1}$, for all $(i, j), (j, k) \in \mathcal{G}$ we have $R_{j,k} \circ R_{i,j} = R_{i,k}$. In this case $D_i = \mathtt{dom}(R_{i,j})$ for all $i, j = 1, \ldots, n$ and we call $D_1, \ldots, D_n$ the domains of the family.

A $(\mathcal{G}, n)$-*symmetric conjunction* is any conjunction of a $(\mathcal{G}, n)$-symmetric family. A $(\mathcal{G}, n)$-*equivalence conjunction* is any conjunction of a $(\mathcal{G}, n)$-equivalence family.

We recall some basic graph theory. We call an indirect, simple graph on $\{1, \ldots, n\}$ just a *graph*, and we represent it by any irreflexive and symmetric relation $\mathcal{G}$ on $\{1, \ldots, n\}$. A *simple cycle* in $\mathcal{G}$ is any sequence $\sigma = \{(i_0, i_1), (i_1, i_2), \ldots (i_{m-1}, i_m), (i_m, i_0)\} \subseteq \mathcal{G}$ of pairwise distinct $i_0, \ldots, i_m$ with $m \geq 2$. $\mathcal{G}$ is *acyclic* if $\mathcal{G}$ has no simple cycle. A path is any sequence $\pi = \{(i_0, i_1), (i_1, i_2), \ldots (i_{m-1}, i_m)\}$ with pairwise distinct $i_1, \ldots, i_m$, with possibly $m = 0$. The connection relation on $\mathcal{G}$ is: "there is some path from i to j" In any acyclic graph $\mathcal{G}$ the path from i to j if it exists then it is unique. Given any equivalence relation $\mathcal{P}$, there is some minimal graph $\mathcal{G} \subseteq \mathcal{P}$ among those such that $\mathcal{P}$ is the smallest equivalence relation including $\mathcal{G}$. All these minimal graphs are acyclic.

Definition 6 ($(\mathcal{R}, n)$-Normal Forms). *$C = C_1 \wedge C_2$ is a $(\mathcal{R}, n)$-normal conjunction if C_1 is some conjunction of positive $(\mathcal{R}, n)$-atoms, C_2 is some conjunction of negative $(\mathcal{R}, n)$-atoms, and for some equivalence relation $\mathcal{P}$*

1. *C_1 is some $(\mathcal{P}, n)$-equivalence conjunction*
2. *for any $\neg S(x_i, x_j)$ in C_2 we have $i < j$*
3. *if $[n]_{\mathcal{P}} \neq \{n\}$ then x_n does not occur in C_2*

Any $A \in \mathcal{A}_n$ is an $(\mathcal{R}, n)$-normal form if A is some disjunction of $(\mathcal{R}, n)$-normal conjunctions.

We first prove that any $(\mathcal{G}, n)$-symmetric conjunction, with $\mathcal{G}$ some acyclic graph, is equivalent to some $(\mathcal{P}, n)$-equivalence conjunction, where $\mathcal{P}$ is the reflexive and transitive closure of $\mathcal{G}$.

Lemma 8 (Transitive Closure Lemma). *Let $n > 0$ be any positive integer. Assume $\mathcal{G}$ is any acyclic graph on $\{1, \ldots, n\}$ and $A = \wedge_{i,j \in \mathcal{G}} R_{i,j}(x_i, x_j)$ is any $(\mathcal{G}, n)$-symmetric conjunction. Let $\mathcal{P}$ be the reflexive, symmetric and transitive closure of $\mathcal{G}$. Then A is equivalent to some* unique *$(\mathcal{P}, n)$-equivalence conjunction B whose family of atoms extends the family of atoms of A.*

Now we prove that the $(\mathcal{P}, n)$-equivalence conjunctions are closed under conjunction with a positive $(\mathcal{R}, n)$-atom $R(x_i, x_j)$. For all $i = 1, \ldots, n$, we denote with $[i]_{\mathcal{P}}$ the equivalence class of i in $\mathcal{P}$.

Lemma 9 (Partition Lemma). *Assume $A = \wedge_{i,j \in \mathcal{P}} R_{i,j}(x_i, x_j)$ is any $(\mathcal{P}, n)$-equivalence conjunction, and $i, j \in \{1, \ldots, n\}$. Assume $D \in \mathcal{D}$ and $R \in \mathcal{R}$.*

1. *$A \wedge (x_i \in D)$ is equivalent to some $(\mathcal{P}, n)$-equivalence conjunction*
2. *Assume $[i]_{\mathcal{P}} = [j]_{\mathcal{P}}$. Then $A \wedge R(x_i, x_j)$ is equivalent to some $(\mathcal{P}, n)$-equivalence conjunction*
3. *Assume $[i]_{\mathcal{P}} \neq [j]_{\mathcal{P}}$ and $\mathtt{dom}(R) = \mathtt{dom}(R_{i,i})$ and and $\mathtt{codom}(R) = \mathtt{dom}(R_{j,j})$. Then $A \wedge R(x_i, x_j)$ is equivalent to some $(\mathcal{P}, n)$-equivalence conjunction*
4. *Any $A \wedge R(x_i, x_j)$ is equivalent to some $(\mathcal{P}, n)$-equivalence conjunction*

6.2 A Quantifier Elimination Result for $\mathcal{R}$

Now we prove a quantifier-elimination result for the language with symbols the binary predicates in $\mathcal{R}$, using Lemma 6 and Lemma 9.

Lemma 10 (Quantifier Elimination for $\mathcal{R}$). *Let $n > 0$ be any positive integer.*

1. *Any finite conjunction of positive $(\mathcal{R}, n)$-atoms has some $(\mathcal{P}, n)$-equivalence form.*
2. *Any finite conjunction of positive and negative $(\mathcal{R}, n)$-atoms has some $(\mathcal{P}, n)$-equivalence form.*
3. *If A is some finite conjunction of positive and negative $(\mathcal{R}, n)$-atoms, then $\exists x_n.A$ is equivalent to some $B \in \mathcal{A}_{n-1}$.*
4. *If $A \in \mathcal{A}_n$, then $\exists x_n.A$ is equivalent to some $B \in \mathcal{A}_{n-1}$.*

We may now finish the proof of Theorem 2.

7 Main Theorem

Let $\mathcal{R}$, $\mathcal{D}$ as in §5. From the properties of the partial bijections in $\mathcal{R}$ and from the quantifier elimination result (§6) we derive our main result.

Theorem 3 (Counterexample to Brotherston-Simpson Conjecture). *Let H be the formula defined in Definition 1. Then H has a proof in $\mathtt{CLKID}^{\omega}(\Sigma_N, \Phi_N)$, and no proof in $\mathtt{LKID}(\Sigma_N, \Phi_N) + (0, s)$-axioms.*

Proof. The proof in $\texttt{CLKID}^\omega$ is shown in Theorem 1. The non-provability in LKID is shown as follows. Any atomic formulas in $\mathcal{M}$ is in $\mathcal{R}$. By definition, $\mathcal{R}$ contains all finite bijections and is closed under restriction to any set $D \in \mathcal{D}$. Thus, by Lemma 6, $\mathcal{R}$ satisfies all hypothesis of Theorem 2. We deduce that all definable sets of $\mathcal{M}$ are in $\mathcal{D}$. By Lemma 3 point 4, all sets in $\mathcal{D}$ have a dyadic measure, and by Lemma 2 satisfy the induction schema. According to Def. 2.10 of [6], this is a sufficient condition for $\mathcal{M}$ being an Henkin model of $\texttt{LKID}(\Sigma_N, \Phi_N)$. $\mathcal{M}$ satisfies the $(0, S)$-axioms by construction. $\mathcal{M}$ falsifies H by Lemma 1. □

8 Non-Conservativity of Martin-Löf's Inductive Definition System

This section shows non-conservativity of LKID with respect to additional inductive predicates, by giving a counterexample.

We assume the inductive predicate $\leq$ and the production rules for it:

$$\frac{}{x \leq x} \qquad \frac{x \leq y}{x \leq sy}$$

We call the set of these production rules $\Phi_{\leq}$. Let 0-axiom be $\forall x \in N.\ sx \neq 0$. In $\texttt{LKID}(\Sigma_N + \{\leq\}, \Phi_N + \Phi_{\leq})$, we can show any number ≤ 0 is only 0.

Lemma 11. *0-axiom*, $Nx, Ny, x \leq y \vdash y = 0 \to x = 0$

The proof is in §A.

The next theorem shows 2-Hydra is provable in LKID with $\leq$.

Theorem 4. *0-axiom* $\vdash H$ *is provable in* $\texttt{LKID}(\Sigma_N + \{\leq\}, \Phi_N + \Phi_{\leq})$.

We may show $\forall n.\ (n \geq x \wedge n \geq y \to p(x, y))$ by induction on n. The proof is given in §A in case.

In the standard model, the truth of formula does not change when we extend the model with inductive predicates that do not appear in the formula. On the other hand, this is not the case for provability in Martin-Löf's inductive definition system LKID. Namely, a system may change the provability of a formula even when we add inductive predicates that do not appear in the formula. Namely, for a given system, the system with additional inductive predicates may not be conservative over the original system. Theorems 3 and 4 give such an example: the sequent 0-axiom $\vdash H$ is in the language of LKID but it is not provable in LKID, while it is provable in LKID extended with $\leq$.

9 Conclusion

We proved in Thm. 3 that $\texttt{CLKID}^\omega$, the formal system of cyclic proofs ([6]) proves strictly more that LKID, Martin-Löf formal system of inductive definitions with classical logic. This settles an open question given in [6]. Our proof also shows that if we add more inductive predicates to LKID we may obtain a non-conservative extension (Thm. 4).

References

1. Stefano Berardi, Makoto Tatsuta, The Classic Martin-Löf's System of Inductive Definitions is not Equivalent to Cyclic Proofs (Full Paper), unpublished draft, 2017.
2. James Brotherston, Cyclic Proofs for First-Order Logic with Inductive Definitions, In: *Proceedings of TABLEAUX 2005*, 2005.
3. James Brotherston, Sequent calculus proof systems for inductive definitions, phd. thesis, Laboratory for Foundations of Computer Science School of Informatics University of Edinburgh 2006.
4. James Brotherston, Richard Bornat and Cristiano Calcagno, Cyclic Proofs of Program Termination in Separation Logic, In: *Proceedings of POPL 2008*, 2008.
5. James Brotherston, Dino Distefano and Rasmus L. Petersen, Automated Cyclic Entailment Proofs in Separation Logic, In: *Proceedings of CADE-23*, 2011.
6. J. Brotherston, A Simpson, Sequent calculi for induction and infinite descent, *Journal of Logic and Computation 21* (6) (2011) 1177–1216.
7. James Brotherston, Nikos Gorogiannis and Rasmus L. Petersen, A Generic Cyclic Theorem Prover, In: *Proceedings of APLAS 2012*, 2012.
8. H. B. Enderton, *A Mathematical Introduction to Logic, Second Edition*, Academic Press, 2000.
9. Laurence Kirby and Jeff Paris, Accessible Independence Results for Peano Arithmetic, Bulletin of London Mathematical Society, 1982; 14: 285-293.
10. P. Martin-Löf. Haupstatz for the intuitionistic theory of iterated inductive definitions. In Proceedings of the Second Scandinavian Logic Symposium, pp. 179216. North-Holland, 1971.
11. Alex Simpson. Cyclic Arithmetic is Equivalent to Peano Arithmetic. Submitted to Fossacs 2017.

Appendix

A Proofs of the Results of the Paper

In this section we include an example of quantifier elimination and all remaining proofs with the same method we use to prove this result in general.

An Example of Quantifier Elimination. Assume $R_1, R_2, R \in \mathcal{R}$ and $\exists x_4.A$ is the existential formula in the language $\mathcal{R}$ defined by $A = (R_1x_1x_4 \wedge R_2x_2x_4 \wedge \neg Rx_3x_4)$. We produce some equivalent quantifier-free formula in the same language.

1. The first step is to replace R_1, R_2 by some $R_{1,4}$, $R_{2,4}$ with equal codomain. Let $D_4 = \mathtt{codom}(R_1) \cap \mathtt{codom}(R_2)$: then A implies that $x_4 \in D_4$. Let $D_1 = R_1^{-1}(D_4)$ and $D_2 = R_2^{-1}(D_4)$: then A implies that $x_1 \in D_1$ and $x_2 \in D_2$. If we define $R_{1,4} = R_1 \cap (D_1 \times D_4)$ and $R_{2,4} = R_2 \cap (D_2 \times D_4)$, then A implies that $R_{1,4}x_1, x_4$ and $R_{2,4}x_2x_4$. Since $R_{1,4} \subseteq R_1$ and $R_{2,4} \subseteq R_2$, we obtain that
$$A \Leftrightarrow (R_{1,4}x_1x_4 \wedge R_{2,4}x_2x_4 \wedge \neg Rx_3x_4)$$
2. The next step is closing the relations with arguments in $\{x_1, x_2, x_4\}$ by composition. We set $R_{1,2} = R_{2,4}^{-1} \circ R_{1,4}$: then
$$A \Leftrightarrow (R_{1,4}x_1x_4 \wedge R_{2,4}x_2x_4 \wedge R_{1,2}x_1x_2 \wedge \neg Rx_3x_4)$$
By construction we have $R_{2,4} \circ R_{1,2} = R_{2,4} \circ R_{2,4}^{-1} \circ R_{1,4} = R_{1,4}$ and $\mathtt{dom}(R_{1,2}) = D_1$ and $\mathtt{codom}(R_{1,2}) = D_2$.
3. The third step is removing the occurrences of x_4 in negative atoms. Let $R' = R_{2,4}^{-1} \circ R$. Set $B = R_{1,4}x_1x_4 \wedge R_{2,4}x_2x_4 \wedge R_{1,2}x_1x_2$. Assume B. Then Rx_3x_4 implies $R'x_3x_2$, and $R'x_3x_2$ implies $R_{2,4}x_2x$ and Rx_3x for some x. Since $R_{2,4}$ is a partial bijection and B implies $R_{2,4}x_2x_4$, we deduce $x = x_4$ and Rx_3x. We proved that B implies $Rx_3x_4 \Leftrightarrow R'x_3x_2$: thus,
$$A \Leftrightarrow (R_{1,4}x_1x_4 \wedge R_{2,4}x_2x_4 \wedge R_{1,2}x_1x_2 \wedge \neg R'x_3x_2)$$
4. Let
$$C = (R_{1,2}x_1x_) \wedge \neg R'x_3x_2)$$
be the formula obtained by erasing all remaining atoms including x_4. The last step is proving that $\exists x_4.A \Leftrightarrow C$. If we assume C, we deduce $R_{1,2}x_1x_2$, hence $x_1 \in D_1$ and $x_2 \in D_2$. Thus, for some x, x' we have $R_{1,4}x_1x \wedge R_{2,4}x_2x'$. From $\{x\} = R_{1,4}(\{x_1\}) = R_{2,4}(R_{1,2}(\{x_1\}) = R_{2,4}(\{x_2\}) = \{x'\}$ we get $x = x'$. We conclude $\exists x.A[x/x_4]$. Conversely, if we assume A we prove C, and since x_4 is not in C, we conclude $\exists x_4.A \Rightarrow C$.

Proof (Lemma 1 (the 2-Hydra Lemma)). We have to prove that all $(x, y) \notin p_{\mathcal{M}}$ satisfy a,b,c,d.

1. Assume $(x,y) \in \pi_1 \cup \pi_2$ and there is some point $(x',y')\pi_1 \cup \pi_2$ before (x,y) in $\pi_1 \cup \pi_2$. Then $x = sa \in \mathcal{M}$ and $y = ssb \in \mathcal{M}$: we only have to check condition *(b)*. By definition of π, the point $(x',y') = (a,b)$ is in $\pi_1 \cup \pi_2$.
2. Assume $(x,y) \in \pi_1 \cup \pi_2$ and (x,y) is the first point of π_1 or of π_2: then $(x,y) = (0_{\mathcal{M}}, \infty)$ or $(x,y) = (\infty, 0_{\mathcal{M}})$ and we only have to check *(c)*, respectively, *(d)*. If $(x,y) = (0_{\mathcal{M}}, \infty) \in \pi_1$ it is enough to prove $(\infty - 1, \infty - 2) \notin p_{\mathcal{M}}$. If $(x,y) = (\infty, 0_{\mathcal{M}}) \in \pi_2$ it is enough to prove $(\infty - 1, \infty - 2) \notin p_{\mathcal{M}}$. $(\infty - 1, \infty - 2) \in\notin p_{\mathcal{M}}$ follows from $(\infty - 1, \infty - 2) \in \pi_3 \subseteq \mathcal{M}^2 \setminus p_{\mathcal{M}}$
3. Assume $(x,y) \in \pi_3 = (\infty - 1, \infty - 1) - \pi$. Then $x = sa \in \mathcal{M}$ and $y = ssb \in \mathcal{M}$ and we only have to check condition *(b)*. By assumption, if $(x,y) \in \pi_3 = (\infty - 1, \infty - 1) - \pi$ then the next point in π_3 is some $(x-1, y-2) \in \pi_3$, as wished.

Proof (Lemma 2 (Measure)). Assume that P is closed under 0, s (hence $P \supseteq \underline{\texttt{Nat}}$) and there is some $a \in \mathcal{M} \setminus P$. From $P \supseteq \underline{\texttt{Nat}}$ we deduce that $a \notin \underline{\texttt{Nat}}$: for any such a we have $a = \infty + z$ for some $z \in \texttt{Z}$. Let $S_a = \{a, a-1, a-2, a-3, \ldots\}$: by the contrapositive of closure under s, we deduce that $S_a \subseteq \mathcal{M} \setminus P$. Thus, $\mathcal{M} \setminus P = \bigcup\{S_a | a \in \mathcal{M} \setminus P\}$. If there is a maximum $a \in \mathcal{M} \setminus P$ we conclude that $\mathcal{M} \setminus P = S_a = \{\ldots, a-3, a-2, a-1, a\}$, while if there is no maximum for $\mathcal{M} \setminus P$ then $\mathcal{M} \setminus P = \underline{\texttt{Z}}$. In the first case we have $\mu(\mathcal{M} \setminus P) = 1/3$, in the second one we have $\mu(\mathcal{M} \setminus P) = 2/3$. Thus, if P is a counter-example to induction rule for N then $\mu(P) = 1/3, 2/3$ and $\mu(P)$ is not a dyadic rational.

Proof (Lemma 3 ($\mathcal{D}$-Lemma)).

1. $\emptyset$ is a finite union, therefore $\mathcal{D}$ includes all $D \sim \emptyset$: that is, $\mathcal{D}$ includes all finite subsets of $\mathcal{M}$.
2. By repeatedly applying the equation $M(2^a, b) = M(2^a, b + 2^a)$ we may assume that $0 \leq b < 2^a$. Then we repeatedly apply the equation $M(2^a, b) = M(2^{a+1}, b) \cup M(2^{a+1}, b + 2^a)$.
3. By induction on n and point 2 above we may prove our thesis for any $D \sim (B_1 \cup \ldots \cup B_n)$.
4. From point 3 above there are a and $0 \leq b_1 < \ldots < b_i < 2^a$ in $\texttt{Nat}$ such that $D \sim (M(2^a, b_1) \cup \ldots \cup M(2^a, b_i))$. If $M(2^a, b) \subsetneq \mathcal{M}$ then $a \in \texttt{Nat}$, $b \in \texttt{Z}$ and $\mu(M(2^a, b) \cap \mathcal{M}) = 1/2^a$. Since $0 \leq b_1 < \ldots < b_i < 2^a$ for some $i \leq 2^a$, the sets $M(2^a, b_1), \ldots, M(2^a, b_i)$ are pairwise disjoint. From $\mu(D)$ additive, we deduce that $\mu(D) = i/2^a \leq 1$ is some dyadic rational. By Lemma 2, D satisfies induction rule for N.
5. By construction, $\mathcal{D}$ is closed under $\sim$ and under union. Thus, we have to prove that if $D \in \mathcal{D}$ then $(\mathcal{M} \setminus D) \in \mathcal{D}$. By point 3 above there are a and $0 \leq b_1 < \ldots < b_i < 2^a$ in $\texttt{Nat}$ such that $D \sim (M(2^a, b_1) \cup \ldots \cup M(2^a, b_i))$. Assume that $[0, 2^a[\setminus \{b_1, \ldots, b_i\} = \{c_1, \ldots, c_j\}$: then $(\mathcal{M} \setminus D) \sim (\mathcal{M} \setminus M(2^a, b_1) \cup \ldots \cup M(2^a, b_i)) = (M(2^a, c_1) \cup \ldots \cup M(2^a, c_j)) \in \mathcal{D}$. By closure of $\mathcal{D}$ under $\sim$, we conclude that $(\mathcal{M} \setminus D) \in \mathcal{D}$.

Proof (Lemma 4 (ϕ-Lemma)).

1. We have $\phi(M(2^z, r)) = M(2^{z+z_1}, 2^{z_1} * r + r_1) \in \mathcal{B}$.
2. If $D \in \mathcal{D}$ then $D \sim M(2^{a_1}, b_1) \cup \ldots \cup M(2^{a_i}, b_i)$ for some $a_1, \ldots, a_i \in \mathtt{Z}$ and some $b_1, \ldots, b_i \in \mathtt{Q}$. Then $\phi(D) \sim \phi(M(2^{a_1}, b_1)) \cup \ldots \cup \phi(M(2^{a_i}, b_i))$, and by point 1 above $\phi(M(2^{a_1}, b_1)) \cup \ldots \cup \phi(M(2^{a_i}, b_i)) \in \mathcal{B}$. Thus, $\phi(D) \in \mathcal{D}$.

Proof (Lemma 5 (Partial Bijections)).

1. Assume D is finite. Then $\mathtt{id}_D$ is, therefore $\mathtt{id}_D \in \mathcal{R}_0 \subseteq \mathcal{R}$. Assume D is infinite. Then $\mathtt{id}_D$ is some even $(D, D, \mathtt{id})$-bijection.
2. If R is finite then $R(D)$ is finite, hence $R(D)\mathcal{D}$. If R is a (A, B, ϕ)-bijection, then by $\phi(D) \sim R(D) \subseteq D \subseteq \mathcal{M}$ we deduce $\phi(D) \subsetneq_{\sim} \mathcal{M}$. By Lemma 4.2, from $D \in \mathcal{D}$ and $\phi(D) \subsetneq_{\sim} \mathcal{M}$ we deduce $\phi(D) \in \mathcal{D}$, hence $R(D) \in \mathcal{D}$ by $\sim$-closure of $\mathcal{D}$ by 3.5.
3. If $R \circ S$ is finite then $R \circ S \in \mathcal{R}_0 \subseteq \mathcal{R}$.
   Assume $R \circ S$ is infinite. Then both R and S are infinite, R is some (A, B, ϕ)-bijection and S is some (C, D, ψ)-bijection, for some $\phi, \psi \in \mathcal{F}$. Then $\phi(n) \geq 0$ and $\phi(-n-1) < 0$ for all but finitely many $n \in \mathtt{Nat}$. If R is an even bijection, then, up to finitely many elements R maps $\mathtt{Nat}$ in $\mathtt{Z}_0^+$, $\mathtt{Z}_0^+$ in $\mathtt{Nat}$, and $\mathtt{Z}^-$ in $\mathtt{Z}^-$. The same holds for ψ and S. Thus, $R \circ S \in \mathcal{R}$ is even if both are even or both are odd, and it is odd if one is odd and one is even, and it is some $(\phi^{-1}(B \cap C), \psi(B \cap C), \psi \circ \phi)$-bijection. Here we use the fact that $B, C \in \mathcal{D}$, $\phi^{-1} \in \mathcal{F}$ and $\phi^{-1}(B \cap C) \subseteq A \subseteq \mathcal{M}$ imply $B \cap C \in \mathcal{D}$ by closure of $\mathcal{D}$ under intersection, then $\phi^{-1}(B \cap C) \in \mathcal{D}$ by Lemma 4.2. In the same way we prove that $\psi(B \cap C) \in \mathcal{D}$.
4. Assume R is finite. Then R^{-1} is finite, hence $R^{-1} \in \mathcal{R}$. Assume that R is some (D, E, ϕ)-bijection. Then R^- is even or odd according what is R, and it some (E, D, ϕ^{-1})-bijection.
5. We have $D = \mathtt{dom}(R) \in \mathcal{D}$ by definition of $\mathcal{R}$, and $E = \mathcal{M} \setminus D \in \mathcal{D}$ by Lemma 3.5. We take $S = \mathtt{id}_E$.

Proof (Lemma 6 (Closure Under Intersection)). Assume $R, S \in \mathcal{R}$ are associated to $\phi, \psi \in \mathcal{F}$.

1. Assume $\phi = \psi$. Then R, S are both even or both odd, and by definition for all but finitely many $a \in \mathtt{dom}(R) \cap \mathtt{dom}(S)$ we have $R(a) = \phi(a) = \psi(a) = S(a)$, hence $\mathtt{dom}(R \cap S) \sim \mathtt{dom}(R) \cap \mathtt{dom}(S) \in \mathcal{D}$. We deduce that $\mathtt{dom}(R \cap S) \in \mathcal{D}$, therefore $R \cap S$ is a partial bijection of domain in $\mathcal{D}$ and associated to ϕ
2. Assume $\phi \neq \psi$. Then R is defined from ϕ with at most three cases, and S from ψ with at most three cases. Since ϕ, ψ are different straight lines, for each case there is at most one pair $a, b \in \mathcal{M}$, such that $\phi(a) = \psi(a) = b$, therefore there are at most three pairs (a, b) such that $\phi(a) = \psi(a) = b$. Up to finitely many elements, any $(a, b) \in R \cap S$ satisfies $\phi(a) = \phi(a) = b$. Thus, $R \cap S$ is finite, hence it is in $\mathcal{R}^0$.
3. Assume $R', S' \in \mathcal{R}$. If R' or S' are finite then $R' \cap S'$ is finite, hence in $\mathcal{R}^0$. If both R' and S' are infinite, we deduce $R' \cap S' \in \mathcal{R}$ by point 1 or 2, according if R', S' are associated to the same map $\phi \in \mathcal{F}$ or not.

4. By $\mathtt{id}_{\mathcal{M}} \in \mathcal{R}$ and point 3 above the we have $R \cap \mathtt{id}_M \in \mathcal{R}$, therefore $D = \mathtt{dom}(R \cap \Delta) \in \mathcal{D}$ by definition of $\mathcal{R}$. From $R \cap \mathtt{id}_{\mathcal{M}} \subseteq \mathtt{id}_{\mathcal{M}}$ we deduce that $R \cap \mathtt{id}_{\mathcal{M}} = \mathtt{id}_D$.

Proof (Lemma 7 (Composition and Product)). Assume that $(x, z) \in (S \cap (E \times F)) \circ (R \cap (D \times E))$. Then $x \in D$, $z \in F$, and for some $y \in E$ we have $R(x, y)$, $S(y, z)$. We conclude that $(x, z) \in (S \circ R) \cap (D \times F)$.

Assume that $(x, z) \in (S \circ R) \cap (D \times F)$. Then $x \in D$, $z \in F$, and for some y we have $R(x, y)$, $S(y, z)$. From $x \in D$ and $R(x, y)$ we deduce that $y \in R(D)$; from $z \in F$ and $S(y, z)$ we deduce that $y \in S^{-1}(F)$. By $y \in R(D)$, $y \in S^{-1}(F)$ and our assumption we obtain that $y \in E$. Thus, $(x, y) \in (R \cap (D \times E))$ and $(y, z) \in (S \cap (E \times F))$. We conclude that $(x, z) \in (S \cap (E \times F)) \circ (R \cap (D \times E))$.

Proof (Lemma 8 (Transitive Closure)). By definition, there are $D_1, \ldots, D_n \in \mathcal{D}$ such that $\mathtt{dom}(R_{i,j}) = D_i$ for all $(i, j) \in \mathcal{G}$. Assume $(i, j) \in \mathcal{P}$. Then there is some path $\pi_{i,j} = \{(i_0, i_1), \ldots, (i_{m-1}, i_m)\}$ from $i = i_0$ to $j = i_m$ in $\mathcal{G}$. $\pi_{i,j}$ is unique, because from two different paths we would define a simple cycle. We define $S_{i,j} = R_{i_m,i_{m-1}} \circ \ldots \circ R_{i_1,i_0}$, with $S_{i,j} = \mathtt{id}_{D_i}$ if $i = j$: $S_{i,j}$ belongs to any $(\mathcal{P}, n)$-equivalence conjunction, if we prove that it is some $(\mathcal{P}, n)$-equivalence conjunction we have uniqueness. Let $B = \wedge_{i,j \in \mathcal{P}} S_{i,j}(x_i, x_j)$. By construction, for all $(i, j) \in \mathcal{G}$ we have $\pi_{i,j} = \{(i, j)\}$ (the unique path from i to j is $\{(i, j)\}$), therefore $S_{i,j} = R_{i,j}$. Thus, B implies A. Conversely, if $S_{i,j} = R_{i_n,i_{n-1}} \circ \ldots \circ R_{i_1,i_0}$ with $i = i_0$, $j = i_m$, then $S_{i,j}(x_i, x_j)$ is implied by $R_{i_m,i_{m-1}}(x_{i_m}, x_{i_{m-1}}) \wedge \ldots \wedge R_{i_1,i_0}(x_{i_1}, x_{i_0})$. Thus, B is equivalent to A and $S_{i,i} = \mathtt{id}_{D_i}$. By construction, $\mathtt{dom}(S_{i,j}) = D_i$. By induction on the length of the path between j, k in $\mathcal{G}$ we may prove that $S_{j,k} \circ S_{i,j} = S_{i,k}$. We conclude that B is the unique $(\mathcal{P}, n)$-equivalence conjunction including all atoms of A.

Proof (Lemma 9 (Partition Lemma)). By assumption on A, there are $D_1, \ldots, D_n \in \mathcal{D}$ such that $D_j = \mathtt{dom}(R_{j,k})$ for all $(j, k) \in \mathcal{P}$.

1. Fix any $i = 1, \ldots, n$, and any $D \in \mathcal{D}$, any $j \in [i]_{\mathcal{P}}$. Let $D'_j = R_{i,j}(D) \subseteq D_j$: we have $D'_j \in \mathcal{D}$ by assumption on $\mathcal{R}$. For all $(j, k) \in \mathcal{P}$ we define $R'_{j,k} = R_{j,k} \cap (D'_j \times D'_k)$ if $j, k \in [i]_{\mathcal{P}}$, and $R'_{j,k} = R_{j,k}$ otherwise. We define A' as the conjunction of $R'_{j,k}(x_j, x_k)$ for all $(j, k) \in \mathcal{P}$.
   Claim: $A \wedge (x_i \in D) \Leftrightarrow A'$. Assume $A \wedge (x_i \in D)$. Assume $(j, k) \in \mathcal{P}$ in order to prove $R'_{j,k}(x_j, x_k)$. From $x_i \in D$ and $R_{i,h}(x_i, x_h)$ for all $h \in [i]_{\mathcal{P}}$, we deduce $x_h \in R_{i,h}(D) = D'_h$. Thus, if $j, k \in [i]_{\mathcal{P}}$ we have $(x_j, x_k) \in D'_j \times D'_k$, and by $R_{j,k}(x_j, x_k)$ we conclude $R'_{j,k}(x_j, x_k)$. If $j, k \notin [i]_{\mathcal{P}}$ then $R'_{j,k} = R_{j,k}$, and by $R_{j,k}(x_j, x_k)$ again we conclude $R'_{j,k}(x_j, x_k)$. *Assume A'.* Then for all $(j, k) \in \mathcal{P}$ we conclude $R_{j,k}(x_j, x_k)$ by $R'_{j,k} \subseteq R_{j,k}$.
   We have $D'_i = R_{i,i}(D) = \mathtt{id}_{D_i}(D) = D \cap D_i$, therefore for all $(j, k) \in [i]_{\mathcal{P}}$ we have $R_{j,k}(D'_j) = R_{j,k}(R_{i,j}(D)) = R_{i,k}(D) = D'_k$.
   We have to prove that A' is an $(\mathcal{P}, n)$-equivalence conjunction. Assume $(j, k), (k, h) \in \mathcal{P}$.
   (1) If $j, k \in [i]_{\mathcal{P}}$ we have $\mathtt{dom}(R'_{j,k}) = D'_j$ because $R_{j,k}(D'_j) = D'_k$. If $j, k \notin [i]_{\mathcal{P}}$ we have $\mathtt{dom}(R'_{j,k}) = \mathtt{dom}(R_{j,k}) = D_j$.

(2) If $j \in [i]_{\mathcal{P}}$ then $R'_{j,j} = R_{j,j} \cap (D'_j \times D'_j) = \mathtt{id}_{D_j} \cap \cap (D'_j \times D'_j) = \mathtt{id}_{D'_j}$. If $j \notin [i]_{\mathcal{P}}$ then $R'_{j,j} = R_{j,j} = \mathtt{id}_{D_j}$.

(3) If $j, k \in [i]_{\mathcal{P}}$ then $R'_{k,j} = R_{k,j} \cap (D'_k \times D'_j) = R^{-1}_{j,k} \cap (D'_k \times D'_j) = (R_{j,k} \cap (D'_j \times D'_k))^{-1} = R'^{-1}_{j,k}$. If $j, k \notin [i]_{\mathcal{P}}$ then $R'_{k,j} = R_{k,j} = R^{-1}_{j,k} = R'^{-1}_{j,k}$.

(4) If $j, k, h \in [i]_{\mathcal{P}}$ we have $R'_{k,h} \circ R'_{j,k} = R_{k,h} \cap (D'_k \times D'_h) \circ R_{j,k} \cap (D'_j \times D'_k)$ = (by Lemma 7 and $D'_k = R_{j,k}(D'_j)$, $D'_k = R_{h,k}(D'_h) = R^{-1}_{k,h}(D'_h)$) = $(R_{k,h} \circ R_{j,k}) \cap (D'_j \times D'_h) = R_{j,h} \cap (D'_j \times D'_h) = R'_{j,h}$. If $j, k, h \notin [i]_{\mathcal{P}}$ we have $R'_{k,h} \circ R'_{j,k} = R_{k,h} \circ R_{j,k} = R_{j,h} = R'_{j,h}$.

2. Let $R' = R_{i,j} \cap R$ and $D = \mathtt{dom}(R')$. Then $R' \in \mathcal{R}$, $D\mathcal{D}$ and $R' = R_{i,j}\lceil D$: any partial equivalence included in $R_{i,j}$ is determined by its domain. Thus, $R_{i,j}(x_i, x_j) \wedge R(x_i, x_j)$ is equivalent to $R_{i,j}(x_i, x_j) \wedge (x_i \in D)$. The thesis follows by point 1 above.

3. Fix any two disjoint equivalence classes $[i]_{\mathcal{P}}, [j]_{\mathcal{P}}$ and some bijection $R \in \mathcal{R}$ from D_i to D_j. Let $\mathcal{G}$ be any minimal (hence acyclic) graph such that the smallest equivalence relation including $\mathcal{G}$ is $\mathcal{P}$. Assume B is the conjunction of atoms $R_{a,b}(x_a, x_b)$ for all $(a, b) \in \mathcal{G}$: the family of atoms of B is included in the family of atoms of A. By Lemma 8 there is a unique $(\mathcal{P}, n)$-equivalence conjunction A' whose family of atoms extend the family of atoms of B, and $A' \Leftrightarrow B$. Thus, $A' = A$, and A is equivalent to B. Let $\mathcal{G}' = \mathcal{G} \cup \{(i, j)\}$: $\mathcal{G}'$ is an acyclic graph by $(i, j) \notin \mathcal{P}$. $B \wedge R(x_i, x_j)$, is a $(\mathcal{G}', n)$-symmetric conjunction. By Lemma 8 and $\mathcal{G}'$ acyclic we deduce that $B \wedge R(x_i, x_j)$ is equivalent some $(\mathcal{P}', n)$-equivalence conjunction C, with $\mathcal{P}'$ = the smallest equivalence relation including $\mathcal{G}'$. Thus, $A \wedge R(x_i, x_j)$ is equivalent to C. Remark that $\mathcal{P}'$ defines partition obtained from the partition of $\mathcal{P}$ by merging the two equivalence classes $[i]_{\mathcal{P}}, [j]_{\mathcal{P}}$.

4. If $[i]_{\mathcal{P}} = [j]_{\mathcal{P}}$ the thesis follows from point 2 above. Assume that $[i]_{\mathcal{P}} \neq [j]_{\mathcal{P}}$. $A \wedge R(x_i, x_j)$ is equivalent to $A \wedge R(x_i, x_j) \wedge (x_i \in D_i) \wedge (x_j \in D_j)$. By assumption we have $R' = R \cap (D_i \times D_j) \in \mathcal{R}$, therefore $D'_i = \mathtt{dom}(R') \in \mathcal{D}$, $D'_j = \mathtt{codom}(R') \in \mathcal{D}$ and $A \wedge R(x_i, x_j) \wedge (x_i \in D_i) \wedge (x_j \in D_j)$ is equivalent to $A \wedge R'(x_i, x_j)$. If we apply twice point 1, we obtain some $(\mathcal{R}, n)$-equivalence conjunction A' equivalent to A, with D_i, D_j replaced respectively by D'_i, D'_j. Then the thesis follows by point 3 above.

Proof (Lemma 10 (Quantifier Elimination Lemma)).

1. Assume A is any finite conjunction of positive $(\mathcal{R}, n)$-atoms. We prove that A is equivalent to some $(\mathcal{P}, n)$-equivalence conjunction by induction on the number of the positive atoms $R(x_i, x_j)$ in A.

   (1) Assume that A is the empty conjunction, hence the always true n-ary predicate. We take the partition $\mathcal{P}$ of $\{1, \ldots, n\}$ with equivalence classes of one element: $\{1\}, \ldots, \{n\}$. As $R_{i,i}$ we take the equality relation $\mathtt{id} : \mathcal{U} \to \mathcal{U}$. Let B be the conjunction of all $x_i = x_i$. B is a conjunction of positive $(\mathcal{R}, n)$-atoms, and B is some $(\mathcal{R}, n)$-equivalence conjunction by construction. B is always true, hence B is equivalent to A.

(2) Assume that A is some equivalence conjunction of positive $(\mathcal{R}, n)$-atoms and $R(x_i, x_j)$ is any positive $(\mathcal{R}, n)$-atom. Our thesis is that $A \wedge R(x_i, x_j)$ is equivalent to some equivalence conjunction B of positive $(\mathcal{R}, n)$-atoms. This follows by Lemma 9.4.

2. Assume $A = C_1 \wedge C_2$, with C_1 any finite conjunction of positive $(\mathcal{R}, n)$-atoms and C_2 any finite conjunction of negative $(\mathcal{R}, n)$-atoms.
We first remove all negative atoms of the form $\neg S(x_i, x_i)$, for all $i = 1, \ldots, n$. Indeed, by Lemma 6.4 this atom is equivalent to $\neg D(x)$ for some $D \in \mathcal{D}$, hence to $E(x)$ for some $E \in \mathcal{D}$ by closure of $\mathcal{D}$ under complement. Then we replace all atoms $\neg S(x_i, x_j)$ with $i > j$ with $\neg S^{-1}(x_j, x_i)$, where have $j < i$. We obtain some $C_2' \Leftrightarrow C_2$, with C_2' conjunction of negative $(\mathcal{R}, n)$-atoms of the form $\neg S(x_i, x_j)$, for some S, some $i < j$.
By the previous point we may replace C_1 with some equivalence conjunction C_1' of positive $(\mathcal{R}, n)$-atoms.
Assume that there is some $a \neq n$ such that $a \in [n]_{\mathcal{P}}$. We claim that for all $R \in \mathcal{R}$, $i \leq n$ if $R' = R_{n,a} \circ R$ then we have $C_1' \Rightarrow (R(x_i, x_a) \Leftrightarrow R'(x_i, x_n))$. Indeed, $C_1' \Rightarrow R_{n,a}(x_n, x_a)$, therefore $C_1' \Rightarrow (R(x_i, x_a) \Rightarrow R'(x_i, x_n))$. Assume $R'(x_i, x_n)$: then for some $z \in U$ we have $R_{n,a}(x_n, z) \wedge R(x_i, z)$. From $C_1' \Rightarrow R_{n,a}(x_n, x_a)$ and $R_{n,a}$ partial bijection we deduce $z = x_a$, therefore $C_1' \Rightarrow R'(x_i, x_n) \Rightarrow R_{n,a}(x_n, x_a)$. Thus, we may replace each $\neg R(x_i, x_n)$ for $i < n$ with some equivalent condition $\neg R'(x_i, x_a)$ where $R' = R_{n,a} \circ R$. We obtain an equivalent formula $C_1 \wedge C_2''$ in which x_n occurs in no negative atom.

3. By point 2 above we may assume that A is some $(\mathcal{R}, n)$-normal conjunction. In particular, there is some equivalence relation $\mathcal{P}$ on $\{1, \ldots, n\}$ such that the positive atoms of A form some $(\mathcal{P}, n)$-equivalence conjunction. Let $D_j = \mathtt{dom}(R_{i,i})$ for $i = 1, \ldots, n$. If D_n is equal to some finite set $\{a_1, \ldots, a_k\} \subseteq \mathcal{U}$, then $\exists x_n.A$ is equivalent to some propositional formula $A[a_1/x] \vee \ldots \vee A[a_k/x]$. Assume D_n is infinite. We distinguish two cases, according if $[n]_{\mathcal{P}} = \{n\}$ or $[n]_{\mathcal{P}} \neq \{n\}$. In both cases we prove that $\exists x_n \ldots$ acts as an "eraser", removing all $(\mathcal{R}, n)$-atoms in which x_n occurs.
Assume that $[n]_{\mathcal{P}} = \{n\}$. Then $R_{n,n} = \mathtt{id}_{D_n}$. There are finitely many conditions $\neg R(x_i, x_n)$ for $i < n$. All R are bijection, therefore each condition $\neg R(x_i, x_n)$ discards a single value of x_n, given x_i. We assumed that there are infinitely many values of x_n in D_n, therefore at least one verifies all requests $\neg R(x_i, x_n)$. Thus, $\exists x_n.A$ is equivalent to B, with B obtained by removing all $(\mathcal{R}, n)$-atoms including x_n.
Assume that $[n]_{\mathcal{P}} \neq \{n\}$. Then x_n occurs in no negative $(\mathcal{R}, n)$-atom in A. Assume that B is obtained by removing all (necessarily positive) $(\mathcal{R}, n)$-atoms $R_{j,n}(x_j, x_n)$ including x_n, with $j \in [n]_{\mathcal{P}}$, $j \neq n$. We prove that $\exists x_n.A \Leftrightarrow B$. From $A \Rightarrow B$ we and x_n not in B we deduce $\exists x_n.A \Rightarrow B$. We prove the opposite implication. Assume B and fix any $k \in [n]_{\mathcal{P}}$, $k \neq n$. Since $B \Rightarrow x_k \in D_k$, there is a (unique) x such that $R_{k,n}(x_k, x)$ is true. For any $j \in [n]_{\mathcal{P}}, j \neq n$ we have $R_{j,n} = R_{k,n} \circ R_{j,k}$, therefore $R_{j,n}(\{x_j\}) = R_{k,n}(R_{j,k}(\{x_k\}) =$ (by $B \Rightarrow R_{j,k}(x_j, x_k)$) $R_{k,n}(\{x_k\}) = \{x\}$.

We conclude that $B \Rightarrow R_{j,n}(x_j, x)$ for all $j \in [n]_{\mathcal{P}}$, $j \neq n$. We deduce $B \Rightarrow A[x/x_n]$, then $B \Rightarrow \exists x_n.A$.

4. By the disjunctive normal form theorem, A is equivalent to $A_1 \vee \ldots \vee A_k$, for some $A_1, \ldots, A_k$ which are conjunctions of positive and negative $(\mathcal{R}, n)$-atoms. Thus, $\exists x_n.A$ is equivalent to $\exists x_n.A_1 \vee \ldots \vee \exists x_n.A_k$. By point 3 above, each $\exists x_n.A_i$ is equivalent to some $B_i \in \mathcal{A}_{n-1}$. Thus, A is equivalent to some $B_1 \vee \ldots \vee B_k \in \mathcal{A}_{n-1}$.

Proof (Theorem 2 (Quantifier Elimination for Partial Equivalences)).

1. Every quantifier-free formula of $U \cup \mathcal{R}$ is equivalent to some formula in some $\mathcal{A}_n$. Indeed, we may replace the predicate $=$ by $\mathtt{id}_{\mathcal{M}}$, then any $R(c, d)$ by the boolean formulas true or false, and any formula $R(x, d)$, $S(c, y)$ by either true or false or some $(\mathcal{R}, n)$-atoms of the form: $x \in \{c'\}$, $y \in \{d'\}$. Assume A is any formula of the language $U \cup \mathcal{R}$ with free variables $x_1, \ldots, x_n$. By induction on A, using the previous remark and Lemma 10.4 for an existential, we prove that A is equivalent to some $B \in \mathcal{A}_n$.
2. Assume $R(x_1, x_1)$ is any positive $(\mathcal{R}, 1)$-atom. Then $R \cap \mathtt{id}_{\mathcal{M}} \in \mathcal{R}$ by $\mathtt{id}_{\mathcal{M}} \in \mathcal{R}$ and closure under intersection, therefore $\{m \in \mathcal{U} | R(m, m)\} = \mathtt{dom}(R \cap \Delta) \in \mathcal{D}$. By point 1, any formula A in the language $U \cup \mathcal{R}$ with at most x_1 free is some boolean combination of positive $(\mathcal{R}, 1)$-atoms, therefore it is in $\mathcal{D}$ by closure of $\mathcal{D}$ under intersection and complement.

Proof (Theorem 3).

Let $\mathcal{U} = (M, \mathcal{R})$. We start proving the *Claim*: all atomic formulas of $\mathcal{M}$ are equivalent to some atomic formula of $\mathcal{U}$. *Proof of the Claim* The atomic formulas of $\mathcal{M}$ have predicate symbol $=$ or q. Those with symbol $=$ have the forms: *(i)* $x + n = y + m$ or *(ii)* $x + n = x + m$ or *(iii)* $x + n = b$ or *(iv)* $a = y + m$ or *(v)* $a = b$, for some $n, m \in \mathtt{Nat}$ and some $a, b \in \mathcal{M}$. They may be expressed with: *(i)* $y = \phi(x)$, with $\phi(x) = 2^0 * x + (n - m)$, *(ii)* with $x = x$ if $n = m$ and with `false` if $n \neq m$, *(iii)* with some $x = b'$ or some $a' = y$, or `false`. Those with symbol p have the form $p(x + n, y + m)$ or $p(x + n, b)$ or $p(a, y + m)$ or $p(a, b)$ for some $n, m \in \mathtt{Nat}$ and some $a, b \in \mathcal{M}$. They may be expressed with the odd bijection q, negated and composed with $\phi(x) = x + (n - m)$, or with $x = b'$ or $a' = y$, or with `false`.

We have to prove that any prefixed point in $\mathcal{H}_1$ of the definition of N includes the interpretation of N: this is to say, any set in $\mathcal{H}_1$ closed under 0 and s is equal to $\mathcal{M}$. By induction on the predicate we may prove that all first order predicates of $\mathcal{M}$ are definable in $\mathcal{U}$: in the case of an atomic predicate we use the Claim, otherwise the induction hypothesis. By Theorem 2.2 all definable sets of $\mathcal{M}$ are in $\mathcal{D}$, therefore $\mathcal{H}_1 \subseteq \mathcal{D}$. By Lemma 3.4, all sets in $\mathcal{D}$ have a dyadic measure, and by Lemma 2 if they are closed under 0 and s they are equal to $\mathcal{M}$. Thus, all definable sets of $\mathcal{M}$ closed under 0 and s are equal to $\mathcal{M}$, and by Def. 2.10 of [6], $\mathcal{M}$ is an Henkin model of $\mathtt{LKID}(\Sigma_N, \Phi_N)$. $\mathcal{M}$ satisfies the $(0, S)$-axioms by construction. $\mathcal{M}$ falsifies H by Lemma 1.

Proof (Lemma 11). The proof is by induction on the definition of $x \leq y$. If x is y then $x = 0 \to x = 0$, if y is $S(z)$ and the property holds for x, z then we trivially have $S(z) = 0 \to x = 0$ by 0-axiom.

Proof (Theorem 1 (H Has a Cyclic Proof)). The global trace condition holds for any infinite path π in the cyclic proof of §3.3. We may explicitly describe an infinite trace in π, as follows. We have three possible choices for constructing the infinite path π in the proof: taking a bud of the left, middle, or right. For a given bud and $z_1, z_2 \in \{x, y\}$, we write $z_1 \rightsquigarrow z_2$ for a progressing trace from Nz_1 in the companion to Nz_2 in the bud. We write $z_1 \rightsquigarrow z_2, z_3$ for $z_1 \rightsquigarrow z_2$ and $z_1 \rightsquigarrow z_3$. For the left bud, there are $x \rightsquigarrow x, y$. For the middle bud, there are $y \rightsquigarrow x, y$. For the left bud, there are $x \rightsquigarrow x$ and $y \rightsquigarrow y$. If the left bud does not appear in a path, there is a progressing trace $y \rightsquigarrow y \rightsquigarrow y \rightsquigarrow \ldots$. If the middle bud does not appear in a path, there is a progressing trace $x \rightsquigarrow x \rightsquigarrow x \rightsquigarrow \ldots$.

Assume both of the left and middle buds appear infinitely in a path. Start from the first left or middle bud and repeat infinitely one of following operations, according to the current bud. Take $x \rightsquigarrow x$ for the left buds except the last bud before the middle bud comes. Take $x \rightsquigarrow y$ for the last bud. Take $y \rightsquigarrow y$ for the middle buds except the last bud before the left bud comes. Take $y \rightsquigarrow x$ for the last bud.

In all cases, take $x \rightsquigarrow x$ or $y \rightsquigarrow y$ for the right bud depending the previous trace.

Given an infinite path, there is some tail of the path that satisfies one of these three cases. Hence the global trace condition holds.

Proof (Proof of Theorem 4). We will prove the equivalent sequent $\hat{H}, Nx, Ny \vdash p(x, y)$. We will show $\forall n.\ (n \geq x \wedge n \geq y \to p(x, y))$ by induction on n. The proof in §A.

For simplicity, we write (1),(2),(3), and (4) for 2-Hydra axioms H_a, H_b, H_c, H_d respectively. Case 1: $n = 0$. Then $x = y = 0$ by Lemma 11, hence $p(x, y)$ by (1).

Case 2: $n = sn'$.

Sub-case 2.1: $y = 0$. Sub-sub-case 2.1.1. $x = 0$ or $x = s0$. By (1). Sub-sub-case 2.1.2. $x = ssx''$. Then $p(S(x''), x'')$ by induction hypothesis, hence $p(x, 0)$ by (3).

Sub-case 2.2. $y = s0$. By (2).

Sub-case 2.3. $y = ssy''$. Sub-sub-case 2.3.1. $x = 0$. Then $p(S(y''), y'')$ by IH, hence $p(0, y)$ by (4). Sub-sub-case 2.3.2. $x = sx'$. Then $p(x', y'')$ by IH, hence $p(x, y)$ by (2).

By principal induction on x and secondary induction on y we may prove that $\exists n.(n \geq x) \wedge (n \geq y)$. From this statement and the previous one we conclude our thesis.