EXPLICIT INDUCTION IS NOT EQUIVALENT TO CYCLIC PROOFS FOR CLASSICAL LOGIC WITH INDUCTIVE DEFINITIONS

(Article begins on next page)

14 December 2021

EXPLICIT INDUCTION IS NOT EQUIVALENT TO CYCLIC PROOFS FOR CLASSICAL LOGIC WITH INDUCTIVE DEFINITIONS

STEFANO BERARDI [a] AND MAKOTO TATSUTA [b]

[a] Università di Torino

[b] National Institute of Informatics / Sokendai, Tokyo

ABSTRACT. A cyclic proof system, called CLKID-omega, gives us another way of representing inductive definitions and efficient proof search. The 2005 paper by Brotherston showed that the provability of CLKID-omega includes the provability of LKID, first order classical logic with inductive definitions in Martin-Löf's style, and conjectured the equivalence. The equivalence has been left an open question since 2011. This paper shows that 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 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 on sets. 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 rules determine 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), or we found anywhere else in the proof-tree, 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 that in any infinite path of the proof-tree there is some infinitely decreasing inductive definition. In general, for proof search, a cyclic proof system can find an induction formula in a more efficient way than induction rules in Martin-Löf's style, since a cyclic

proof system does not have to choose a fixed induction formula in advance. A cyclic proof system enables efficient implementation of theorem provers with inductive definitions [2, 4]. In particular, it works well for theorem provers of Separation Logic [5, 7].

Brotherston and Simpson [6] investigated the system LKID of inductive definitions in classical logic for the first-order language, and the cyclic proof system CLKID^ω for the same language, showed the provability of CLKID^ω includes that of LKID, and conjectured the equivalence. Since then, the equivalence has been left an open question. In 2017, Simpson [11] proved a particular case of the conjecture, for the theory of Peano Arithmetic.

This paper (which is the journal version of [1]) shows CLKID^ω and LKID are indeed not equivalent. To this aim, we will consider the first-order language L (with equality) 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 Kirby and Paris [9]: the proviso "2" means that we only have two "heads". We show that the 2-Hydra statement is provable in CLKID^ω with language L, but the statement is not provable in LKID with language L. 2-Hydra is similar to the candidate for a counter-example proposed by Stratulat [12].

The unprovability is shown by constructing some Henkin model $\mathcal{M}$ of LKID where 2-Hydra is false. 2-Hydra is true in all standard models of LKID, but $\mathcal{M}$ is a non-standard model, in which both the universe of $\mathcal{M}$ and the interpretation of the predicate N are $\mathbb{N} + \mathbb{Z}$, where $\mathbb{N}$ is the set of natural numbers and $\mathbb{Z}$ is the set of integers. Predicates of $\mathcal{M}$ are the equality relation and one "partial bijection", i.e., a one-to-one correspondence between subsets of the universe of $\mathcal{M}$. The proof that $\mathcal{M}$ is a Henkin model of LKID immediately follows from a quantifier elimination result, which holds for all sets of partial bijections which are closed under composition and inverse.

Our quantifier elimination result is new, to our best knowledge, and it may be of some independent interest. However, our interest is not the quantifier elimination result *per se*, but rather the identification of this result as a way of proving the unprovability of 2-Hydra in LKID.

The model $\mathcal{M}$ also shows a side result, 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.

This is the plan of the paper. Section 2 describes inductive definitions, standard and Henkin models. Section 3 defines the first order system LKID for inductive definitions, the 2-Hydra statement, and proves 2-Hydra under two additional assumptions: the 0-axiom and the existence of an ordering $\leq$. Section 4 defines the system CLKID^ω for cyclic proofs, gives a cyclic proof for the 2-Hydra statement and describes the Brotherston-Simpson conjecture. Section 5 defines the structure $\mathcal{M}$ and the proof outline that $\mathcal{M}$ is a counter model. Section 6 introduces a set of partial bijections in $\mathcal{M}$. Section 7 proves a quantifier elimination theorem for any set of partial bijections closed under composition and inverse. Section 8 disproves the Brotherston-Simpson conjecture, by proving that the 2-Hydra statement is not provable in LKID. As a corollary, we have non-conservativity of LKID with additional inductive predicates. We conclude in Section 9.

2. Inductive Definitions, Standard Models and Henkin Models

In this section quickly recall the notion of first order inductive definition, standard model and Henkin model, taken from [6]. This introduction is only a sketch and we refer to [6] for motivations and examples. We fix a first order language Σ with equality that includes inductive predicate symbols $P_1, \ldots, P_n$ of arities $k_1, \ldots, k_n$.

Definition 2.1 (Productions of Σ)**.** An inductive definition set Φ for Σ is a finite set of productions. A production is a rule

$$\frac{Q_1(\vec{u_1}) \ \ldots \ Q_h(\vec{u_h}) \ P_{j_1}(\vec{t_1}) \ \ldots \ P_{j_m}(\vec{t_m})}{P_i(\vec{t})}$$

whose premises are a finite sequence of atomic formulas, where $Q_1, \ldots, Q_h$ are ordinary predicate symbols, $j_1, \ldots, j_m, i \in \{1, \ldots, n\}$, $P_1, \ldots, P_n$ are inductive predicate symbols, and all vector of terms have the appropriate length to match the arities of the predicate symbols.

An example. Let $\Sigma = \{0, s\}$ be the language with 0 and the successor. Then a set of productions Φ_N describing the inductive predicate N for "being a natural number" is:

$$\frac{}{N(0)} \qquad \frac{N(x)}{N(sx)}$$

We call the pair (Σ, Φ) an inductive definition system. The language for (Σ, Φ) is the first order language consisting of all constants, functions and predicates of Σ. The standard interpretation for (Σ, Φ) is obtained by considering the smallest prefixed point of a monotone operator ϕ_Φ defined below. From now on, we denote the powerset of a set X by $\mathcal{P}(X)$. In the next definition we suppose that ρ is a valuation from finitely many variables to the universe, and that ρ is applied componentwise on a vector of terms.

Definition 2.2 (Monotone Operator ϕ_Φ)**.** Let $\mathcal{M}$ with domain $|\mathcal{M}|$ be a first-order structure for Σ, and for each $i \in \{1, \ldots, n\}$, let k_i be the arity of the inductive predicate symbol P_i.
1. $\Phi_i = \{\phi \in \Phi \mid$ the conclusion of ϕ is $P_i\}$.
2. Assume Φ_i has the form $\{\Phi_{i,r} \mid 1 \le r \le |\Phi_i|\}$. For each rule $\Phi_{i,r}$ of the form shown in 2.1, we define $\Phi_{i,r} : \mathcal{P}(|\mathcal{M}|^{k_{j_1}}) \times \ldots \times \mathcal{P}(|\mathcal{M}|^{k_{j_n}}) \to \mathcal{P}(|\mathcal{M}|^{k_i})$ by:

$$\Phi_{i,r}(X_1 \ldots, X_n) = \{\rho(\vec{t}) \mid \rho \text{ a valuation}, \ \rho(\vec{t_1}) \in X_{j_1}, \ \ldots, \ \rho(\vec{t_m}) \in X_{j_m},$$
$$Q_1^{\mathcal{M}}(\rho(\vec{u_1})), \ \ldots, \ Q_h^{\mathcal{M}}(\rho(\vec{u_h}))\}.$$

3. We define Φ_i for each $i \in \{1, \ldots, n\}$ with the same domain and codomain, by:

$$\Phi_i(X_1, \ldots, X_n) = \bigcup_{1 \le r \le |\Phi_i|} \Phi_{i,r}(X_1, \ldots, X_n).$$

4. We define ϕ_Φ, with domain and codomain $\mathcal{P}(|\mathcal{M}|^{k_1}) \times \ldots \times \mathcal{P}(|\mathcal{M}|^{k_n})$, by: $\phi_\Phi(X_1, \ldots, X_n) = (\Phi_1(X_1, \ldots, X_n), \ldots, \Phi_n(X_1, \ldots, X_n))$.

We extend union and subset inclusion to the corresponding pointwise operations on n-tuples of sets: in this way $\mathtt{dom}(\phi_\Phi)$ becomes a complete lattice. A prefixed point of ϕ_Φ is $\vec{X} \in \mathtt{dom}(\phi_\Phi)$ such that $\vec{X} \subseteq \phi_\Phi(\vec{X})$. The map ϕ_Φ is monotone on a complete lattice. Thus, ϕ_Φ has a unique smallest prefixed point by the Tarski Fixed Point Theorem. We define the standard model for (Σ, Φ) from such a prefixed point.

Definition 2.3 (Standard model). A first-order structure $\mathcal{M}$ with universe $|\mathcal{M}|$ is said to be a standard model for (Σ, Φ) if the vector $(P_1^{\mathcal{M}}, \ldots, P_n^{\mathcal{M}})$ of interpretations of $P_1, \ldots, P_n$ in $\mathcal{M}$ is the smallest prefixed point of ϕ_Φ.

The Henkin class for $\mathcal{M}$ is a family of subsets $\mathcal{H}_k \subseteq |\mathcal{M}|^k$, indexed on $k \in \mathbb{N}$, including all graphs of predicates of $\mathcal{M}$ and closed w.r.t. all first order connectives, as we make precise below.

Definition 2.4 (Henkin class for a first order structure $\mathcal{M}$). Le $\mathcal{M}$ with domain $|\mathcal{M}|$ be a structure for Σ. Assume $k, h \in \mathbb{N}$, $\vec{x} = x_1, \ldots, x_k$ are variables, $t_1, \ldots, t_h$ are terms and $\vec{d} = d_1, \ldots, d_k \in |\mathcal{M}|$. A Henkin class for $\mathcal{M}$ is a family of sets $\mathcal{H} = \{\mathcal{H}_k \mid k \in \mathbb{N}\}$ such that, for each $k \in \mathbb{N}$: $\mathcal{H}_k \subseteq \mathcal{P}(|\mathcal{M}|^k)$;

(H_1) $\{(d, d) \mid d \in |\mathcal{M}|\} \in \mathcal{H}_2$;

(H_2) if $Q \in \Sigma$ is any predicate symbol of arity k then $Q_{\mathcal{M}} \in \mathcal{H}_k$;

(H_3) if $R \in \mathcal{H}_{k+1}$ and $d \in |\mathcal{M}|$ then $\{(\vec{d}) \mid (\vec{d}, d) \in R\} \in \mathcal{H}_k$;

(H_4) if $R \in \mathcal{H}_h$ and $t_1[\vec{x}], \ldots, t_h[\vec{x}]$ are terms then $\{(\vec{d}) \mid (t_1^{\mathcal{M}}[\vec{d}], \ldots, t_h^{\mathcal{M}}[\vec{d}]) \in R\} \in H_k$;

(H_5) if $R \in \mathcal{H}_k$ then $(|\mathcal{M}|^k \setminus R) \in \mathcal{H}_k$;

(H_6) if $R_1, R_2 \in \mathcal{H}_k$ then $R_1 \cap R_2 \in \mathcal{H}_k$;

(H_7) if $R \in \mathcal{H}_{k+1}$ then $\{(\vec{d}) \mid \exists d \in |\mathcal{M}|.(\vec{d}, d) \in R\} \in \mathcal{H}_k$.

The smallest Henkin family $\mathcal{H}_{\mathcal{M}}$ for a structure $\mathcal{M}$, and the only Henkin family we will consider later, is the set of definable sets in $\mathcal{M}$.

Definition 2.5 (The Henkin family $\mathcal{H}_{\mathcal{M}}$). Assume $\mathcal{M}$ is a structure of language Σ. Let $k \in \mathbb{N}$. We write $\vec{u}, \vec{v}$ for two vectors of elements in $|\mathcal{M}|$ of the same length as the vectors of variables $\vec{x}, \vec{y}$. Then the family of sets $\mathcal{H}_{\mathcal{M}} = \{\mathcal{H}_k \mid k \in \mathbb{N}\}$ is defined by:

$$\mathcal{H}_k = \{ \ \{\vec{u} \in |\mathcal{M}|^k \mid \mathcal{M} \models F[\vec{u}, \vec{v}/\vec{x}, \vec{y}]\} \ \mid \ (F \in L(\Sigma)) \ \wedge \ (\text{FV}(F) \subseteq \vec{x}, \vec{y}) \ \wedge \ (\vec{v} \in |\mathcal{M}|)\}$$

In a Henkin Model for Σ, instead of requiring that $(P_1^{\mathcal{M}}, \ldots, P_n^{\mathcal{M}})$ is the smallest prefixed points of ϕ_Φ w.r.t. all subsets of $|\mathcal{M}|$, we require that it is the smallest prefixed points w.r.t. all sets in some Henkin class $\mathcal{H}_k$ for $\mathcal{M}$.

Definition 2.6 (Henkin model). Let $\mathcal{M}$ be a first-order structure for (Σ, Φ) and $\mathcal{H}$ be a Henkin class for $\mathcal{M}$. Then $(\mathcal{M}, \mathcal{H})$ is a Henkin model for (Σ, Φ) if $(P_1^{\mathcal{M}}, \ldots, P_n^{\mathcal{M}})$ is the least prefixed point of $\phi_\Phi \lceil \mathcal{H}$, where $\phi_\Phi \lceil \mathcal{H}$ is ϕ_Φ with each argument in $\mathcal{P}(|\mathcal{M}|^k)$ being restricted to $\mathcal{H}_k$. We say $\mathcal{M}$ is a Henkin model when $(\mathcal{M}, \mathcal{H}_{\mathcal{M}})$ is a Henkin model.

In a Henkin model the interpretation of $P_1, \ldots, P_n$ may be larger than the smallest prefixed points of ϕ_Φ. Some Henkin models are not standard models, and this paper will discuss a Henkin model which is not a standard model.

3. THE SYSTEM LKID FOR INDUCTIVE DEFINITIONS AND THE 2-HYDRA STATEMENT

In this section we quickly introduce some definitions and results of [6], in order to make the paper self-contained. We describe LKID(Σ, Φ), formalizing the notion of inductive proof for a first order language Σ with equality, and for the the set of productions Φ (see section 2). We state that LKID is sound and complete with respect to Henkin models (again, see [6]). Then we formalize the 2-Hydra statement, which is our work. In later sections we will prove

that 2-Hydra is false in some Henkin model, and we use 2-Hydra to distinguish between provability in LKID and cyclic proofs.

We write sequents of the form $\Gamma \vdash \Delta$ where Γ, Δ are finite sets of formulas. We write $\Gamma[\theta]$ for the application of substitution θ to all formulas in Γ. For first-order logic with equality, we use the (standard) sequent calculus rules, with contraction implicitly given. LKID(Σ, Φ) has a rule for substitution, and rules for equality. There are logical rules and rules for inductive predicates.

Structural and logical rules of LKID are the following.

Structural rules:

$$\frac{}{\Gamma \vdash \Delta} \; \Gamma \cap \Delta \neq \emptyset (\text{Axiom}) \qquad \frac{\Gamma \vdash \Delta}{\Gamma' \vdash \Delta'} \; \Gamma \subseteq \Gamma' \quad \Delta \subseteq \Delta' \quad (\text{Wk})$$

$$\frac{\Gamma \vdash \Delta, F \quad F, \Gamma \vdash \Delta}{\Gamma \vdash \Delta} \; (\text{Cut}) \qquad\qquad \frac{\Gamma \vdash \Delta}{\Gamma[\theta] \vdash \Delta[\theta]} \; (\text{Subst})$$

Logical rules:

$$\frac{\Gamma \vdash F, \Delta}{\Gamma, \neg F \vdash \Delta} \; (\neg L) \qquad\qquad \frac{\Gamma, F \vdash \Delta}{\Gamma \vdash \neg F, \Delta} \; (\neg R)$$

$$\frac{\Gamma, F \vdash \Delta \quad \Gamma, G \vdash \Delta}{\Gamma, F \vee G \vdash \Delta} \; (\vee L) \qquad\qquad \frac{\Gamma \vdash F, G, \Delta}{\Gamma \vdash F \vee G, \Delta} \; (\vee R)$$

$$\frac{\Gamma, F, G \vdash \Delta}{\Gamma, F \wedge G \vdash \Delta} \; (\wedge L) \qquad\qquad \frac{\Gamma \vdash F, \Delta \quad \Gamma \vdash G, \Delta}{\Gamma \vdash F \wedge G, \Delta} \; (\wedge R)$$

$$\frac{\Gamma \vdash F, \Delta \quad \Gamma, G \vdash \Delta}{\Gamma, F \rightarrow G \vdash \Delta} \; (\rightarrow L) \qquad\qquad \frac{\Gamma, F \vdash G, \Delta}{\Gamma \vdash F \rightarrow G, \Delta} \; (\rightarrow R)$$

$$\frac{\Gamma, F \vdash \Delta}{\Gamma, \exists x.F \vdash \Delta} \; (x \notin \text{FV}(\Gamma, \Delta) \quad (\exists L) \qquad\qquad \frac{\Gamma \vdash F[t/x], \Delta}{\Gamma \vdash \exists x.F, \Delta} \; (\exists R)$$

$$\frac{\Gamma, F[t/x] \vdash \Delta}{\Gamma, \forall x.F \vdash \Delta} \; (\forall L) \qquad\qquad \frac{\Gamma \vdash F, \Delta}{\Gamma \vdash \forall x.F, \Delta} \; (x \notin \text{FV}(\Gamma, \Delta) \quad (\forall R)$$

$$\frac{\Gamma[u/x, t/y] \vdash \Delta[u/x, t/y]}{\Gamma[t/x, u/y], t = u \vdash \Delta[t/x, u/y]} \; (=L) \qquad\qquad \frac{}{\Gamma \vdash t = t, \Delta} \; (=R)$$

We define left- and right-introduction rules for induction. For each production in Φ of the form:

$$\frac{Q_1(\vec{u_1}[\vec{x}])\ldots Q_h(\vec{u_h}[\vec{x}])P_{j_1}(\vec{t_1}[\vec{x}])\ldots P_{j_m}(\vec{t_m}[\vec{x}])}{P_i(\vec{t}[\vec{x}])}$$

we include the following right-introduction rule for P_i in $\mathtt{LKID}(\Sigma,\Phi)$:

$$\frac{\Gamma\vdash\Delta,Q_1(\vec{u_1}[\vec{u}])\ldots\Gamma\vdash\Delta,Q_h(\vec{u_h}[\vec{u}])\quad\Gamma\vdash\Delta,P_{j_1}(\vec{t_1}[\vec{u}])\ldots\Gamma\vdash\Delta,P_{j_m}(\vec{t_m}[\vec{u}])}{\Gamma\vdash\Delta,P_i(\vec{t}[\vec{u}])}$$

We assume that $\vec{u}$ is a vector of terms of the same length as $\vec{x}$.

We express left-introduction rules for inductive predicates in the form of induction rules for mutually depending predicates. We define mutual dependency first.

Definition 3.1 (Mutual dependency [6]). Let P_i, P_j be inductive predicate symbols of Σ.

1. P_j is a premise of P_i if P_i occurs in the conclusion of some production in Φ, and P_j occurs among the premises of that production.
2. P_i and P_j are mutually dependent if there is a chain for the *"premise relation"* from P_i to P_j, and conversely.

In order to define the left-introduction rule for any inductive predicate P_j, we first associate with every inductive predicate P_i a tuple $\vec{z}_i$ of k_i distinct variables (called induction variables), where k_i is the arity of P_i, and a formula (called an induction hypothesis) F_i, possibly containing (some of) the induction variables $\vec{z}_i$. We define a formula G_i for each $i \in \{1, \ldots, n\}$ by: $G_i = F_i$ if P_i and P_j are mutually dependent and $G_i = P_i(\vec{z}_i)$ otherwise. We write $G_i\vec{t}$ for $G_i[\vec{t}/\vec{z}_i]$, and the same for F_i. Then the induction rule for P_j has the following form:

$$\frac{\text{minor premises}\quad \Gamma, F_j\vec{u}\vdash\Delta}{\Gamma, P_j\vec{u}\vdash\Delta}$$

The premise $\Gamma, F_j\vec{u}\vdash\Delta$ is called the major premise of the rule, and for each production of Φ having in its conclusion a predicate P_i that is mutually dependent with P_j, say:

$$\frac{Q_1(\vec{u_1}[\vec{x}])\ \ldots Q_h(\vec{u_h}[\vec{x}])\ P_{j_1}(\vec{t_1}[\vec{x}])\ \ldots\ P_{j_m}(\vec{t_m}[\vec{x}])}{P_i(\vec{t}[\vec{x}])}$$

there is a corresponding minor premise:

$$\Gamma, Q_1\vec{u_1}[\vec{y}],\ldots,Q_h\vec{u_h}[\vec{y}], G_{j_1}t_1[\vec{y}],\ldots,G_{j_m}\vec{t_m}[\vec{y}]\vdash F_i\vec{t}[\vec{y}],\Delta$$

where $\vec{y}$ is a vector of the same length as $\vec{x}$ for fresh variables.

An alternative formalization of induction is the *induction schema*.

Definition 3.2 (Induction schema). The induction schema is the following set of axioms:

$$\text{(universal closures of minor premises)}\ \rightarrow\forall\vec{y}.(P_i\vec{t}(\vec{y})\rightarrow F_i\vec{t}(\vec{y})),\quad\text{for }i\in\{1,\ldots,n\}$$

$\mathcal{M}$ is defined to *satisfy the induction schema* if and only if all formulas of the induction schema are true in $\mathcal{M}$.

The axioms in the induction schema derive all instances of the induction rule and conversely. By definition unfolding we have the following. If a structure $\mathcal{M}$ has $0, s, N$ and the inductive predicate symbol is only N, then $(\mathcal{M}, \mathcal{H}_\mathcal{M})$ is a Henkin model if and only if: if $F[0/x]$ is true, and for all closed terms t if $F[t/x]$ is true then $F[st/x]$ is true, then we have

$F[u/x]$ true, for all closed terms u. Thus, such a structure $\mathcal{M}$ is a Henkin model if and only if $\mathcal{M}$ satisfies the induction schema. The same remark applies to all inductive predicates.

We write $A_1, \ldots, A_n \rightarrow B$ for $A_1 \wedge \ldots \wedge A_n \rightarrow C$ and $\forall x_1, \ldots, x_n \in N$. A for $\forall x_1. \ldots . \forall x_n.(N(x_1) \wedge \ldots \wedge N(x_n) \rightarrow A)$. We abbreviate 1 and 2 for $s0$ and $ss0$ respectively.

The case of the predicate N. The induction rule for the 'natural number' predicate N (section 2) is:

$$\frac{\Gamma \vdash F0, \Delta \quad \Gamma, Fx \vdash Fsx, \Delta \quad \Gamma, Ft \vdash \Delta}{\Gamma, Nt \vdash \Delta} \ (\text{Ind } N)$$

where x is fresh and F is the induction formula associated with the predicate N. The induction schema for N is the set of axioms

$$F0, (\forall x.Fx \rightarrow Fsx) \ \rightarrow \forall x.(Nx \rightarrow Fx)$$

for any formula F. $\mathcal{M}$ *satisfies the induction schema* for N if and only if $\mathcal{M} \models F0, (\forall x.Fx \rightarrow Fsx) \ \rightarrow \forall x.(Nx \rightarrow Fx)$.

Definition 3.3 (Validity and Henkin Validity). A sequent $\Gamma \vdash \Delta$ is said to be *valid* if it is true in all standard models. Let $(\mathcal{M}, \mathcal{H})$ be a Henkin model for $\text{LKID}(\Sigma, \Phi)$. A sequent $\Gamma \vdash \Delta$ is said to be *true* in $(\mathcal{M}, \mathcal{H})$ if, for all valuations ρ for $\mathcal{M}$, whenever $\mathcal{M} \models_\rho J$ for all $J \in \Gamma$ then $\mathcal{M} \models_\rho K$ for some $K \in \Delta$. A sequent is said to be *Henkin valid* if it is true in all Henkin models.

A derivation tree is a tree of sequents in which each sequent is obtained as the conclusion of an inference rule with its children as premises. A proof in LKID is a finite derivation tree all of whose branches end in an axiom. The basic result about provability is:

Theorem 3.4 (Henkin soundness and completeness of LKID [6]). $\Gamma \vdash \Delta$ *is a sequent provable in* LKID *if and only if* $\Gamma \vdash \Delta$ *is Henkin valid.*

We refer to [6] for a proof. Completeness does not hold for (standard) validity: there are valid sequents with no proof in LKID. One example is the sequent $\vdash H$, where H is the 2-Hydra statement, defined below.

3.1. **The 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 from growing again. In the mathematical problem of Hydra, we ask whether it is possible to destroy an Hydra just by cutting heads.

Kirby and 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. It is a miniature version of the Kirby-Paris statement. 2-Hydra will give a counterexample to the Brotherston-Simpson conjecture.

3.2. **The 2-Hydra Statement.** In this subsection we give the 2-Hydra statement, which is a formula saying that any 2-Hydra eventually loses its two heads.

Let Σ_N be the signature $\{0, s, p, N\}$, which are zero, the successor, an ordinary binary predicate symbol p, and an inductive predicate N for natural numbers. The logical system $\texttt{LKID}(\Sigma_N, \Phi_N)$ is defined as the system $\texttt{LKID}$ with the signature Σ_N and the production rules Φ_N for N (see section 2). We define the $(0, s)$-axioms in this language as the axioms "0 is not successor" or $\forall x \in N.\ sx \neq 0$, and "successor is injective", or $\forall x, y \in N.\ sx = sy \rightarrow x = y$.

We consider a formal statement H for 2-Hydra. H says that the number of heads is always 2, and we can win a game having the following rules:

1. When both heads have positive length, we cut them off completely. Then the first head shrinks to become 1 unit shorter than the previous head and the second head shrinks to become 2 units shorter than the previous head, if these shorter lengths exist. Otherwise we win.

2. When there is a unique head of positive length, we cut it off completely. Then the first head shrinks to become 1 unit shorter than the original head of positive length and the second head shrinks to become 2 units shorter than the original head of positive length, if these shorter lengths exist. Otherwise we win.

We express H by saying that some set of transformations eventually reaches a winning condition. The winning condition is the union of the winning conditions for the points 1 and 2 above. Let $n, m \in \mathbb{N}$. The the winning conditions and the transformations are:

1. we win if we reach the cases: $(0, 0)$, $(1, 0)$ and $(x, 1)$ for any $x \in \mathbb{N}$.
2. if $n \geq 1$ and $m \geq 2$ then $(n, m) \mapsto (n - 1, m - 2)$;
3. if $m \geq 2$ then $(0, m) \mapsto (m - 1, m - 2)$;
4. if $n \geq 2$ then $(n, 0) \mapsto (n - 1, n - 2)$;

The four cases listed above are pairwise disjoint and cover all $(n, m) \in \mathbb{N}^2$. For instance, case 4 is disjoint from cases $1, 2, 3$. When we win, no transformation applies. Indeed, no transformation applies from $(0, 0)$ and $(1, 0)$, because if $m = 0$ we require $n \geq 2$. No transformation applies when $m = 1$, because transformations 1 and 2 require $m \geq 2$, and transformation 3 requires $m = 0$. We define H by a formula in the language Σ_N.

Definition 3.5 (2-Hydra Statement H). We define $H = (H_a, H_b, H_c, H_d \rightarrow \forall x, y \in N.\ p(x, y))$, where H_a, H_b, H_c, H_d are:

(H_a) $\forall x \in N.\ p(0, 0) \wedge p(1, 0) \wedge p(x, 1)$,
(H_b) $\forall x, y \in N.\ p(x, y) \rightarrow p(sx, ssy)$,
(H_c) $\forall y \in N.\ p(sy, y) \rightarrow p(0, ssy)$,
(H_d) $\forall x \in N.\ p(sx, x) \rightarrow p(ssx, 0)$.

For a closed term of $\{0, s\}$, its length is defined as the number of symbols s in it. Assume n, m are closed terms of $\{0, s\}$. Then $p(n, m)$ means that we win for the 2-Hydra game beginning with the first head being of length n and the second head being of length m. For all closed terms n, m of $\{0, s\}$, there is a formula among H_a, H_b, H_c, H_d having some instance inferring $p(n, m)$. The formula is unique if we assume the standard $(0, s)$-axioms. H_a says that $p(0, 0)$, $p(1, 0)$ and $p(n, 1)$ for any closed term n are true, and expresses the winning condition of the game. Each instance of H_b, H_c, H_d is some implication $p(n', m') \rightarrow p(n, m)$ such that the maximum length of n', m' is smaller than the maximum length of n, m. Thus, for all closed terms n, m of $\{0, s\}$, $p(n, m)$ is true in all standard models of $\texttt{LKID}(\Sigma_N, \Phi_N)$:

it is shown by induction on the maximum length of n, m. An example: we derive $p(1, 4)$ by H_b and $p(0, 2)$, the latter by H_c and $p(1, 0)$, the latter by H_a. In a standard model, the interpretation of N is the set of interpretations of closed terms of $\{0, s\}$: as a consequence, 2-Hydra is is true in all standard models of (Σ_N, Φ_N).

However, we will prove that $\mathtt{LKID}(\Sigma_N, \Phi_N) + (0, s)$-axioms does not prove 2-Hydra. Remark that the $(0, s)$-axioms define a proper extension of $\mathtt{LKID}(\Sigma_N, \Phi_N)$. These axioms cannot be proved in $\mathtt{LKID}(\Sigma_N, \Phi_N)$, because each of them fails in the following models.

1. the model with domain $|\mathcal{M}| = N_{\mathcal{M}} = \{0\}$, $s0 = 0$;
2. the model with domain $|\mathcal{M}| = N_{\mathcal{M}} = \{0, s0\}$, $0 \neq s0$ and $ss0 = s0$.

Compared with Peano Arithmetic $\mathtt{PA}$, in $\mathtt{LKID}(\Sigma_N, \Phi_N) + (0, s)$-axioms we do not have a sum or a product on N, and we do not have inductive predicate symbols for addition, multiplication, or order.

3.3. 2-Hydra is provable under additional assumptions.
As an example of a formal proof in $\mathtt{LKID}$, we prove 2-Hydra under two additional assumptions: the inductive predicate $\leq$ and the 0-axiom, which will be defined.

The inductive predicate $\leq$ is defined from the following production rules:

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

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

Lemma 3.6. $0\text{-}axiom, Nx, Ny, x \leq y \vdash y = 0 \to x = 0$

Proof. The proof is by induction on the definition of $x \leq y$. If y is x 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. $\qquad \square$

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

Theorem 3.7. $0\text{-}axiom \vdash H$ is provable in $\mathtt{LKID}(\Sigma_N + \{\leq\}, \Phi_N + \Phi_{\leq})$.

Proof. Let $\hat{H} = H_a, H_b, H_c, H_d$ be the list of 2-Hydra axioms in Def. 3.5. We will prove the equivalent sequent $\hat{H}, Nx, Ny \vdash p(x, y)$. We will first show $\forall n.\ (n \geq x \land n \geq y \to p(x, y))$ by induction on n.

- Case 1: $n = 0$. Then $x = y = 0$ by Lemma 3.6, therefore $p(x, y)$ by H_a.
- Case 2: $n = sn'$.
  - Sub-case 2.1: $y = 0$.
    * Sub-sub-case 2.1.1. $x = 0$ or $x = s0$. By H_a.
    * Sub-sub-case 2.1.2. $x = ssx''$. Then $p(sx'', x'')$ by induction hypothesis, hence $p(x, 0)$ by H_d.
  - Sub-case 2.2. $y = s0$. By H_a.
  - Sub-case 2.3. $y = ssy''$.
    * Sub-sub-case 2.3.1. $x = 0$. Then $p(sy'', y'')$ by I.H., hence $p(0, y)$ by H_c.
    * Sub-sub-case 2.3.2. $x = sx'$. Then $p(x', y'')$ by I.H., therefore $p(x, y)$ by H_b.

By principal induction on x and secondary induction on y we prove that $\exists n.(n \geq x) \land (n \geq y)$. From this statement and the previous one we conclude our claim. $\qquad \square$

4. The system CLKID$^\omega$ and the Brotherston-Simpson conjecture

In this section we introduce more definitions and results of [6], again in order to make the paper self-contained. We define an infinitary version of LKID called LKID$^\omega$, then a subsystem CLKID$^\omega$ of the latter called the system of cyclic proofs in [6]. We give a cyclic proof of 2-Hydra, which is ours, and eventually we state the Brotherston-Simpson conjecture.

The proof rules of the infinitary system LKID$^\omega$ are the rules of LKID, except the induction rules for each inductive predicate. The induction rule (Ind P_i) of LKID is replaced by the case-split rule:

$$\frac{\text{case distinctions}}{\Gamma, P_i \vec{u} \vdash \Delta} \ (\text{Case } P_i)$$

with case distinctions defined as follows. For each production having predicate P_i in its conclusion:

$$\frac{Q_1 \vec{u}_1[\vec{x}] \ \ldots \ Q_h \vec{u}_h[\vec{x}] P_{j_1} \vec{t}_1[\vec{x}] \ \ldots \ P_{j_m} \vec{t}_m[\vec{x}]}{P_i \vec{t}[\vec{x}]}$$

there is a case distinction

$$\Gamma, \vec{u} = \vec{t}[\vec{y}], Q_1 \vec{u}_1[\vec{y}], \ldots, Q_h \vec{u}_h[\vec{y}], P_{j_1} \vec{t}_1[\vec{y}], \ldots, P_{j_m} \vec{t}_m[\vec{y}] \vdash \Delta$$

where $\vec{y}$ is a vector of distinct variables of the same length as $\vec{x}$, and $\vec{y} \cap V = \emptyset$ for $V = FV(\Gamma \cup \Delta \cup \{P_i \vec{u} \mid i = 1, \ldots, n\})$.

The formulas $P_{j_1} \vec{t}_1[\vec{y}], \ldots, P_{j_m} \vec{t}_m[\vec{y}]$ occurring in a case distinction are said to be case-descendants of the principal formula $P_i \vec{u}$.

The case-split rule for N is

$$\frac{\Gamma, t = 0 \vdash \Delta \quad \Gamma, t = sx, Nx \vdash \Delta}{\Gamma, Nt \vdash \Delta} \ x \notin \text{FV}(\Gamma \cup \Delta \cup \{Nt\}) \ (\text{Case } N)$$

The formula Nx occurring in the right hand premise is the only case-descendant of the formula Nt occurring in the conclusion.

The system LKID$^\omega$ is based upon infinite derivation trees. We distinguish between 'leaves' and 'buds' in derivation trees. By a leaf we mean an axiom, i.e. the conclusion of a 0-premise inference rule. By a bud we mean a sequent occurrence in the tree that is not the conclusion of a proof rule.

Definition 4.1 (LKID$^\omega$ Pre-proof). An LKID$^\omega$ pre-proof of a sequent $\Gamma \vdash \Delta$ is a (possibly infinite) derivation tree Π, constructed according to the proof rules of LKID$^\omega$, such that $\Gamma \vdash \Delta$ is the root of Π and Π has no buds.

LKID$^\omega$ pre-proofs are not sound in general: there are pre-proofs of any invalid sequent. The global trace condition is a condition on pre-proofs which ensures their soundness.

A (finite or infinite) path π in a derivation tree Π is a sequence $\pi = (S_i)_{0 \leq i < \alpha}$, for some $\alpha \in N \cup \{\infty\}$, of sequent occurrences in the tree such that S_{i+1} is a child of S_i for all $i + 1 < \alpha$.

Definition 4.2 (Trace). Let Π be an LKID$^\omega$ pre-proof and let $\pi = (\Gamma_i \vdash \Delta_i)_{i \geq 0}$ be an infinite path in Π. A trace following π is a sequence $\tau = (\tau_i)_{i \in \mathbb{N}}$ such that, for all $i \in \mathbb{N}$:

1. $\tau_i = P_{j_i} \vec{t}_i \in \Gamma_i$, where $j_i \in \{1, \ldots, n\}$;
2. if $\Gamma_i \vdash \Delta_i$ is the conclusion of (Subst) then $\tau_i = \tau_{i+1}[\theta]$, where θ is the substitution associated with the instance of (Subst);

3. if $\Gamma_i \vdash \Delta_i$ is the conclusion of ($=$L) with principal formula $t = u$ then there is a formula F and variables x, y such that $\tau_i = F[t/x, u/y]$ and $\tau_{i+1} = F[u/x, t/y]$;

4. if $\Gamma_i \vdash \Delta_i$ is the conclusion of a case-split rule then either *(a)* $\tau_{i+1} = \tau_i$ or *(b)* τ_i is the principal formula of the rule instance and τ_{i+1} is a case-descendant of τ_i. In the latter case, i is said to be a progress point of the trace;

5. if $\Gamma_i \vdash \Delta_i$ is the conclusion of any other rule then $\tau_{i+1} = \tau_i$.

An infinitely progressing trace is a trace having infinitely many progress points.

Definition 4.3 (LKID$^\omega$ proof). An LKID$^\omega$ pre-proof Π is defined to be an LKID$^\omega$ proof if it satisfies the following global trace condition: for every infinite path $\pi = (\Gamma_i \vdash \Delta_i)_{i \geq 0}$ in Π, there is an infinitely progressing trace following some tail of the path, $\pi' = (\Gamma_i \vdash \Delta_i)_{i \geq k}$, for some $k \geq 0$.

Cyclic proofs are a subsystem CLKID$^\omega$ of LKID$^\omega$, defined by restricting LKID$^\omega$ to proofs given by regular trees, i.e. those (possibly infinite) trees with only finitely many distinct subtrees.

Proofs of CLKID$^\omega$ are called cyclic proofs and are represented as finite graphs.

Definition 4.4 (Companion). Let B be a bud of a finite derivation tree Π. A node C in Π which is conclusion of some rule is said to be a companion for B if C and B are the same sequent.

Definition 4.5 (Cyclic pre-proof). A CLKID$^\omega$ pre-proof Π of $\Gamma \vdash \Delta$ is a pair (Π, R), where Π is a finite derivation tree constructed according to the rules of LKID$^\omega$ and whose root is $\Gamma \vdash \Delta$, and R is a function assigning a companion to every bud node in Π.

By unfolding a cyclic pre-proof to its associated (possibly infinite) tree, cyclic pre-proofs generate exactly the class of LKID$^\omega$ pre-proofs given by the regular derivation trees.

Definition 4.6 (Cyclic proof). A CLKID$^\omega$ proof is defined as a CLKID$^\omega$ pre-proof such that its unfolding satisfies the global trace condition.

4.1. **Proof of 2-Hydra Statement in Cyclic-Proof System.** The logical systems LKID(Σ_N, Φ_N) and CLKID$^\omega$(Σ_N, Φ_N) are the systems LKID and CLKID$^\omega$ with the signature Σ_N and the set of production rules Φ_N. In this subsection we give an example of a cyclic proof: a cyclic proof of the 2-Hydra statement in CLKID$^\omega$(Σ_N, Φ_N).

Theorem 4.7. *The 2-Hydra statement H is provable in* CLKID$^\omega$(Σ_N, Φ_N).

Proof. Let the 2-Hydra axioms $\hat{H}$ be H_a, H_b, H_c, H_d as in Definition 3.5.

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

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

Rule ($=$L) is left-introduction of equality: from $\Gamma[a, b] \vdash \Delta[a, b]$ prove $a = b, \Gamma[b, a] \vdash \Delta[b, a]$. We will write a combination of (Case) and ($=$L) as one rule in the following example.

$$\frac{\hat{H}, N0 \vdash p00 \quad \hat{H}, Nx' \vdash psx'0}{\hat{H}, Nx \vdash px0} \; Nx$$

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

We define a cyclic proof Π of $Nx, Ny \vdash pxy$, where the mark *(a)* denotes the bud-companion relation (there are three buds, the only companion is the root). Π is:

$$\frac{\dfrac{\ldots\ \mathbf{(a)}\ldots}{\Pi_1}}{\dfrac{Nx \vdash px0}{}} \quad \frac{\dfrac{\ldots\ \mathbf{(a)}\ldots\ \mathbf{(a)}\ldots}{\Pi_2}}{Nx, Ny' \vdash pxsy'}\ Ny$$
$$\overline{\mathbf{(a)}Nx, Ny \vdash pxy}$$

where the left sub-proof Π_1 is:

$$\frac{\overline{N0 \vdash p00}\quad \dfrac{\overline{N0 \vdash p10}\quad \dfrac{\dfrac{\mathbf{(a)}Nx, Ny \vdash pxy}{Nsx'', Nx'' \vdash psx''x''}}{\dfrac{Nsx'', Nx'' \vdash pssx''0}{Nx' \vdash psx'0}\ Nx'}}{\dfrac{}{}}\ Nx}{Nx \vdash px0}$$

and the right sub-proof Π_2 is:

$$\frac{\overline{N0, Nx \vdash px1}\quad \dfrac{\dfrac{\dfrac{\mathbf{(a)}Nx, Ny \vdash pxy}{Nsy'', Ny'' \vdash psy''y''}}{Nsy'', Ny'' \vdash p0ssy''}\quad \dfrac{\dfrac{\mathbf{(a)}Nx, Ny \vdash pxy}{Nx', Ny'' \vdash px'y''}}{Nsy'', Nx', Ny'' \vdash psx'ssy''}\ Nx}{\dfrac{Nsy'', Nx, Ny'' \vdash pxssy''}{}}\ Nx}{Nx, Ny' \vdash pxsy'}$$

Π *is a cyclic proof.* We only have to check: the global trace condition holds for any infinite path π in the cyclic proof Π above. We can explicitly describe an infinite trace in π, as follows. We have three possible choices for constructing the infinite path π in the proof: taking the bud in the left, middle, or right of the proof. 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 right bud, there are both $x \rightsquigarrow x$ and $y \rightsquigarrow y$. We argue by cases.

1. Assume that from some point on the left bud does not appear in a path. Then from this point there is an infinitely progressing trace $y \rightsquigarrow y \rightsquigarrow y \rightsquigarrow \ldots$.
2. Assume that the middle bud from some point on does not appear in a path. Then from this point there is an infinitely progressing trace $x \rightsquigarrow x \rightsquigarrow x \rightsquigarrow \ldots$.
3. Assume that the left and middle buds appear infinitely many times in a path. Start from x and the left bud if the left bud comes first, and from y and the middle bud if the middle bud comes first, then repeat infinitely one of following operations, according to the current bud. Take $x \rightsquigarrow x$ for all left buds, except for the last left bud before the middle bud comes. Take $x \rightsquigarrow y$ for this bud. Take $y \rightsquigarrow y$ for all middle buds, except for the last middle bud before the left bud comes. Take $y \rightsquigarrow x$ for this bud.

   In both cases, take $x \rightsquigarrow x$ or $y \rightsquigarrow y$ for the right bud, depending if the previous trace was ending in x or in y. Also in this case we defined an infinitely progressing trace starting from some tail of the path, passing infinitely many times though x and though y.

Hence the global trace condition holds. $\square$

4.2. **The Brotherston-Simpson Conjecture.** LKID has been often used for formalizing inductive definitions, while CLKID^ω is another way for formalizing the same inductive definitions, and moreover CLKID^ω 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. The Brotherston-Simpson conjecture (the conjecture 7.7 in [6]) says that the provability LKID includes that of CLKID^ω. Simpson [11] proved the conjecture in the case of Peano Arithmetic. The goal of this paper is to prove that the conjecture is false in general, by showing that there is no proof of 2-Hydra in $\text{LKID}(\Sigma_N, \Phi_N)$.

5. The Structure $\mathcal{M}$ for the Language Σ_N

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 (definition 3.2). $\mathcal{M}$ is not a standard model of LKID (in any standard model 2-Hydra would be true). In the next sections we will prove that $(\mathcal{M}, \mathcal{H}_\mathcal{M})$ is a Henkin model of LKID, where $\mathcal{H}_\mathcal{M}$ was defined as the set of definable sets in $\mathcal{M}$ (definition 2.5).

5.1. **Outline for Proof of Non-Provability.** In this section we define a counter model $\mathcal{M}$, whose predicates are the equality relation and a partial bijection relation (a one-to-one correspondence between some subsets of the universe for $\mathcal{M}$). We prove that $(\mathcal{M}, \mathcal{H}_\mathcal{M})$ is a Henkin model of $\text{LKID}(\Sigma_N, \Phi_N)$ if we take $\mathcal{H}_\mathcal{M}$ as the set of definable sets of the theory of $\mathcal{M}$ (definition 2.5). In fact, we will prove that $\mathcal{M}$ satisfies the induction schema for N (definition 3.2).

On one hand, we prove that in our structure $\mathcal{M}$ all definable sets of $\mathcal{M}$ (that is, all unary definable predicates of $\mathcal{M}$) are all sets we obtain by adding/removing finitely many elements to: the set $|\mathcal{M}|$, the set of even numbers in $|\mathcal{M}|$, the set of multiples of four in $|\mathcal{M}|$, and so forth, together with their translations and their finite unions. All these sets have measure of a dyadic rational, which is a rational of the form $z/2^m$ for some $z \in \mathbb{Z}$, $m \in \mathbb{N}$. This claim about the measure of definable sets of $\mathcal{M}$ is derived as a particular case of a quantifier-elimination result (section 7), in which we characterize the sets which are first order definable from a set of partial bijections closed under composition and inverse (section 6). This result is new, as far as we know. For an introduction to quantifier-elimination we refer to [8, section 3.1, section 3.2].

On the other hand, section 5.3 shows that a definable set of $\mathcal{M}$ with dyadic measure satisfies the induction schema for N (definition 3.2). Combining them, finally we will show that $\mathcal{M}$ satisfies the induction schema for N and therefore $(\mathcal{M}, \mathcal{H}_\mathcal{M})$ is a Henkin model of $\text{LKID}(\Sigma_N, \Phi_N)$.

5.2. **Definition of the Structure $\mathcal{M}$.** Let $\mathbb{Z}$ be the set of integers. We first define the structure $\mathcal{M}$ for $0, S, p$ and N. Later we will define the interpretation of the predicate p in $\mathcal{M}$. We denote the universe of $\mathcal{M}$ by $|\mathcal{M}|$ and we set:

Definition 5.1 (The sets $|\mathcal{M}|$ and $N_{\mathcal{M}}$)**.**

1. $|\mathcal{M}| = \mathbb{N} + \mathbb{Z} = \{(1, x) \mid x \in \mathbb{N}\} \cup \{(2, x) \mid x \in \mathbb{Z}\}$ (the disjoint union of $\mathbb{N}$ and $\mathbb{Z}$).
2. $0_{\mathcal{M}} = (1, 0)$ and $s_{\mathcal{M}}(x, y) = (x, y + 1)$.
3. $N_{\mathcal{M}} = |\mathcal{M}|$.

For all $n \in \mathbb{N}$ we set: $(x, y) + n = (x, y + n)$, and $0_{\mathbb{Z}} = (2, 0)$ (the element 0 in the component $\mathbb{Z}$), and $0_{\mathbb{Z}} - n = (2, -n)$ (the relative integer $-n$ in the component $\mathbb{Z}$). We define the following subsets of $|\mathcal{M}|$: $\mathbb{N} = \{0_{\mathcal{M}} + n \mid n \in \mathbb{N}\}$ and $\mathbb{Z}^- = \{0_{\mathbb{Z}} - (n + 1) \mid n \in \mathbb{N}\}$ and $\mathbb{Z}_0^+ = \{0_{\mathbb{Z}} + n \mid n \in \mathbb{N}\}$. The sets $\mathbb{N}, \mathbb{Z}^-, \mathbb{Z}_0^+$ are a partition of $|\mathcal{M}|$.

By construction $\mathcal{M}$ satisfies the closedness of N under 0 and s, and the $(0, s)$-axioms. $\mathcal{M}$ is not a standard model of LKID because the intersection of all subsets of $|\mathcal{M}|$ closed under under 0 and s is $\mathbb{N} \subset |\mathcal{M}|$, while $N_{\mathcal{M}} = |\mathcal{M}|$.

Even if $\mathcal{M}$ is not a standard model of LKID, one can extend $\mathcal{M}$ to a Henkin model $(\mathcal{M}, \mathcal{H})$ of $\mathrm{LKID}(\Sigma_N, \Phi_N)$, provided that one can identify a suitable Henkin class $\mathcal{H}$ of sets in $\mathcal{P}(|\mathcal{M}|)$ that meets the Henkin closure conditions, and show that $N_{\mathcal{M}}$ is the least prefixed point of ϕ_{Φ_N} within this class. We do it by adding to $\mathcal{M}$ the interpretation $p_{\mathcal{M}}$ of the binary predicate p, and taking $\mathcal{H}$ to be $\mathcal{H}_{\mathcal{M}}$, the set of all sets first order definable from $0, s, =, N, p$ (definition 2.5). We first define a (non-empty) set of points in which the instances of 2-Hydra will be false in $\mathcal{M}$. Let $r = \{(n, 2n) \mid n \in \mathbb{N}\}$. r is the set of points of the straight line $y = 2x$ which are in $\mathbb{N} \times \mathbb{N}$. We imagine r starting from the infinity, moving at each step from some (sa, ssb) to (a, b), and ending at $(0, 0)$. Given $(m_1, m_2) \in |\mathcal{M}| \times |\mathcal{M}|$ we define $(m_1, m_2) + r = \{(m_1 + a, m_2 + b) \mid (a, b) \in r\}$ and $(m_1, m_2) - r = \{(m_1 - a, m_2 - b) \mid (a, b) \in r\}$. We define three paths in $|\mathcal{M}| \times |\mathcal{M}|$ by $\pi_1 = (0_{\mathcal{M}}, 0_{\mathbb{Z}}) + r$ and $\pi_2 = (0_{\mathbb{Z}}, 0_{\mathcal{M}}) + r$ and $\pi_3 = (0_{\mathbb{Z}} - 1, 0_{\mathbb{Z}} - 2) - r$. Then $\pi_1 \cup \pi_2 \cup \pi_3$ is the set of points in which 2-Hydra will be false in the model.

Informally, the reason is that we can move forever along $\pi_1 \cup \pi_2 \cup \pi_3$ while "cutting heads", and we never reach a winning condition. Here is an example, where we write $\mapsto$ for a single move of the game, and we use the clause H_c for a head duplication. The infinite sequence of moves is:

$\ldots \mapsto (0_{\mathcal{M}} + 2, 0_{\mathbb{Z}} + 4) \mapsto (0_{\mathcal{M}} + 1, 0_{\mathbb{Z}} + 2) \mapsto (0_{\mathcal{M}}, 0_{\mathbb{Z}}) \mapsto$ *(head duplication, by the clause H_c)* $(0_{\mathbb{Z}} - 1, 0_{\mathbb{Z}} - 2) \mapsto (0_{\mathbb{Z}} - 2, 0_{\mathbb{Z}} - 4) \mapsto \ldots$. In the next figure we represent $\pi_1 \cup \pi_2 \cup \pi_3$ in $|\mathcal{M}| \times |\mathcal{M}|$:
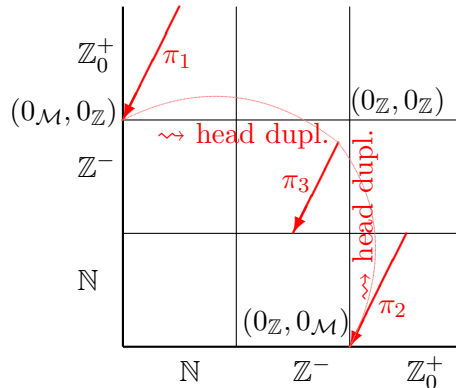
Eventually, we set
$$p_{\mathcal{M}} = |\mathcal{M}|^2 \setminus (\pi_1 \cup \pi_2 \cup \pi_3)$$
We already defined the set $N_{\mathcal{M}}$ as $|\mathcal{M}|$ (definition 5.1). We complete the definition of $\mathcal{M}$ by:

Definition 5.2 (The structure $\mathcal{M}$). $\mathcal{M} = \langle |\mathcal{M}|, 0_{\mathcal{M}}, s_{\mathcal{M}}, N_{\mathcal{M}}, p_{\mathcal{M}} \rangle$

In the following sections we will check that $N_{\mathcal{M}}$ is the least prefixed point of ϕ_{Φ_N} restricted to the Henkin family $\mathcal{H}_{\mathcal{M}}$ (definition 2.5), and therefore that $(\mathcal{M}, \mathcal{H}_{\mathcal{M}})$ is a Henkin model. In this section we check that H is false in $\mathcal{M}$.

Lemma 5.3 (The 2-Hydra Lemma). $\mathcal{M} \not\models H$

Proof. By Def. 3.5, $H = (H_a, H_b, H_c, H_d \to \forall x, y \in N.\ p(x,y))$. We have $\mathcal{M} \not\models \forall x, y \in N.\ p(x,y)$ because $N_{\mathcal{M}} = |\mathcal{M}|$ while $p_{\mathcal{M}} \subset |\mathcal{M}|^2$. In order to prove $\mathcal{M} \not\models H$, we have to prove that $\mathcal{M} \models H_a, H_b, H_c, H_d$.

1. $\mathcal{M} \models H_a$. We have to prove that for all $x \in |\mathcal{M}|$ we have: $(0_{\mathcal{M}}, 0_{\mathcal{M}}), (0_{\mathcal{M}}+1, 0_{\mathcal{M}}), (x, 0_{\mathcal{M}}+1) \in p_{\mathcal{M}}$, that is: $(0_{\mathcal{M}}, 0_{\mathcal{M}}), (0_{\mathcal{M}}+1, 0_{\mathcal{M}}), (x, 0_{\mathcal{M}}+1) \notin \pi_1 \cup \pi_2 \cup \pi_3$. For all $n, m \in \mathbb{N}$, the sets $\pi_2 \cup \pi_3$ include no point of the form $(0_{\mathcal{M}}+n, 0_{\mathcal{M}}+m)$: this proves $(0_{\mathcal{M}}, 0_{\mathcal{M}}), (0_{\mathcal{M}}+1, 0_{\mathcal{M}}) \notin \pi_1 \cup \pi_2 \cup \pi_3$. We have $(x, 0_{\mathcal{M}}+1) \notin \pi_1 \cup \pi_3$ because all points in π_1, π_3 have the second coordinate of the form $0_{\mathbb{Z}}+z$ for some $z \in \mathbb{Z}$. We have $(x, 0_{\mathcal{M}}+1) \notin \pi_2$ because all points in π_2 have the second coordinate of the form $0_{\mathcal{M}}+2n$ for some $n \in \mathbb{N}$.

2. $\mathcal{M} \models H_b$. We have to prove that for all $a, b \in |\mathcal{M}|$ if $\mathcal{M} \models p_{\mathcal{M}}(a,b)$ then $p_{\mathcal{M}}(s_{\mathcal{M}}(a), s_{\mathcal{M}}s_{\mathcal{M}}(b))$, that is: $(a,b) \notin \pi_1 \cup \pi_2 \cup \pi_3$ implies $(s_{\mathcal{M}}(a), s_{\mathcal{M}}s_{\mathcal{M}}(b)) \notin \pi_1 \cup \pi_2 \cup \pi_3$. By taking the contrapositive, this is equivalent to show: $(s_{\mathcal{M}}(a), s_{\mathcal{M}}s_{\mathcal{M}}(b)) \in \pi_1 \cup \pi_2 \cup \pi_3$ implies $(a,b) \in \pi_1 \cup \pi_2 \cup \pi_3$. We argue by cases. Assume $(s_{\mathcal{M}}(a), s_{\mathcal{M}}s_{\mathcal{M}}(b)) \in \pi_1$. Then $(s_{\mathcal{M}}(a), s_{\mathcal{M}}s_{\mathcal{M}}(b)) = (0_{\mathcal{M}}+n+1, 0_{\mathbb{Z}}+2n+2)$ for some $n \in \mathbb{N}$, hence $(a,b) = (0_{\mathcal{M}}+n, 0_{\mathbb{Z}}+2n) \in \pi_1$. Assume $(s_{\mathcal{M}}(a), s_{\mathcal{M}}s_{\mathcal{M}}(b)) \in \pi_2$. Then $(s_{\mathcal{M}}(a), s_{\mathcal{M}}s_{\mathcal{M}}(b)) = (0_{\mathbb{Z}}-1-n, 0_{\mathbb{Z}}-2-2n)$ for some $n \in \mathbb{N}$, hence $(a,b) = (0_{\mathbb{Z}}-1-1-n, 0_{\mathbb{Z}}-2-2-n) \in \pi_2$. Assume $(s_{\mathcal{M}}(a), s_{\mathcal{M}}s_{\mathcal{M}}(b)) \in \pi_3$. Then $(s_{\mathcal{M}}(a), s_{\mathcal{M}}s_{\mathcal{M}}(b)) = (0_{\mathbb{Z}}+n+1, 0_{\mathcal{M}}+2n+2)$ for some $n \in \mathbb{N}$, hence $(a,b) = (0_{\mathbb{Z}}+n, 0_{\mathcal{M}}+2n) \in \pi_3$.

3. $\mathcal{M} \models H_c$. We have to prove that for all $b \in |\mathcal{M}|$ if $\mathcal{M} \models p_{\mathcal{M}}(s_{\mathcal{M}}(b), b)$ then $p_{\mathcal{M}}(0_{\mathcal{M}}, s_{\mathcal{M}}s_{\mathcal{M}}(b))$, that is: $(s_{\mathcal{M}}b, b) \notin \pi_1 \cup \pi_2 \cup \pi_3$ implies $(0_{\mathcal{M}}, s_{\mathcal{M}}s_{\mathcal{M}}(b)) \notin \pi_1 \cup \pi_2 \cup \pi_3$. By taking the contrapositive, this is equivalent to show: $(0_{\mathcal{M}}, s_{\mathcal{M}}s_{\mathcal{M}}(b)) \in \pi_1 \cup \pi_2 \cup \pi_3$ implies $(s_{\mathcal{M}}(b), b) \in \pi_1 \cup \pi_2 \cup \pi_3$. We argue by cases. Assume $(0_{\mathcal{M}}, s_{\mathcal{M}}s_{\mathcal{M}}(b)) \in \pi_1$. Then $(0_{\mathcal{M}}, s_{\mathcal{M}}s_{\mathcal{M}}(b)) = (0_{\mathcal{M}}, 0_{\mathbb{Z}})$, hence $(s_{\mathcal{M}}(b), b) = (0_{\mathbb{Z}}-1, 0_{\mathbb{Z}}-2) \in \pi_2$. Assume $(0_{\mathcal{M}}, s_{\mathcal{M}}s_{\mathcal{M}}(b)) \in \pi_2 \cup \pi_3$. This cannot be, because all points in π_2, π_3 have the first coordinate of the form $0_{\mathbb{Z}}+z$ for some $z \in \mathbb{Z}$.

4. $\mathcal{M} \models H_d$. It is similarly proved to the previous case. □

$\mathcal{H}_{\mathcal{M}}$ was defined as the set of definable sets in $\mathcal{M}$ (definition 2.5). We prove that $(\mathcal{M}, \mathcal{H}_{\mathcal{M}})$ is a Henkin model of LKID. We have to prove that $N_{\mathcal{M}}$ is the smallest pre-fixed point in $\mathcal{H}_1$ for ϕ_{Φ_N} (definition 2.2). An equivalent condition is to prove the induction schema for N: $A[0/x], (\forall x.Nx, A \to A[x+1/x]) \to \forall x.(Nx \to A)$ for any $A \in L(\mathcal{M})$. Since the interpretation of N is $|\mathcal{M}|$ itself, we have in fact to prove that all $X \in \mathcal{H}_1$ which are closed under 0 and s are equal to $|\mathcal{M}|$.

5.3. **The Measure for the Subsets of $\mathcal{M}$ Closed Under 0 and s.** In this subsection we define a sufficient condition for a subset of $\mathcal{M}$ to satisfy the induction schema for N, by using a finitely additive measure $\mu(X)$, defined on subsets $X \subseteq |\mathcal{M}|$. We will prove that all definable subsets for $\mathcal{M}$ satisfy this condition.

Definition 5.4 (Measure for Subset of $\mathcal{M}$). For $X \subseteq |\mathcal{M}|$ we set:

$$\mu(X) = \lim_{x \to \infty} \frac{|\ \{0_{\mathcal{M}} + n, 0_{\mathbb{Z}} - n, 0_{\mathbb{Z}} + n \in |\mathcal{M}| \mid n \in [0, x] \cap N\} \cap X\ |}{3(x+1)}$$

whenever this limit exists.

For instance, $\mu(\mathbb{N}) = 1/3$ and if $E = \{0_{\mathcal{M}}, 0_{\mathcal{M}} + 2, \ldots, 0_{\mathbb{Z}} - 2, 0_{\mathbb{Z}}, 0_{\mathbb{Z}} + 2, \ldots\}$, then $\mu(E) = 1/2$. A *dyadic rational* is any rational of the form $z/2^n$ for some $z \in \mathbb{Z}$, $n \in \mathbb{N}$. We prove that having a dyadic measure is a sufficient condition for a predicate $A[x]$ to satisfy the induction schema for N, namely: $A[0], \forall x.Nx, A[x] \to A[sx]) \to \forall x.(Nx \to A[x])$ (definition 3.2). Later, we will prove that all definable predicates of $\mathcal{M}$ have a dyadic measure, hence they satisfy the induction schema.

Lemma 5.5 (Measure Lemma). *If $\mu(P)$ is a dyadic rational, then P satisfies the induction schema for N.*

Proof. In order to show the contraposition, assume P does not satisfy the induction schema. Then P is closed under 0, s (hence $P \supseteq \mathbb{N}$) and there is some $a \in |\mathcal{M}| \setminus P$. From $P \supseteq \mathbb{N}$ we deduce that $a \notin \mathbb{N}$, hence $a = 0_{\mathbb{Z}} + z$ for some $z \in \mathbb{Z}$. 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, $|\mathcal{M}| \setminus P = \bigcup\{S_a \mid a \in |\mathcal{M}| \setminus P\}$. 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 $|\mathcal{M}| \setminus P = \mathbb{Z}^- \cup \mathbb{Z}_0^+$. 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 the induction schema for N then $\mu(P) = 1/3, 2/3$ and $\mu(P)$ is not a dyadic rational. $\square$

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

6. The 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 domains have some dyadic rational measure. In sections 7, 8 we will prove that all definable sets in $\mathcal{M}$ (definition 2.5) are domains of bijections in $\mathcal{R}$, therefore all these have dyadic rational measure, and by Lemma 5.5 they satisfy the induction schema for N (definition 3.2). We will conclude that $(\mathcal{M}, \mathcal{H}_{\mathcal{M}})$ is a Henkin model of $\mathtt{LKID}(\Sigma_N, \Phi_N)$.

For a set X and binary relations R, S we write: $\mathtt{id}_X = \{(x, x) \mid x \in X\}$, $\mathtt{dom}(R) = \{x \mid \exists y.(x, y) \in R\}$, $\mathtt{range}(R) = \{y \mid \exists x.(x, y) \in R\}$, $R^{-1} = \{(y, x) \mid (x, y) \in R\}$, $R \circ S = \{(x, z) \mid \exists y.((y, z) \in R) \wedge ((x, y) \in S)\}$ and $R \upharpoonright X = \{(x, y) \in R \mid x \in X\}$. Note that we write a relation composition $R \circ S$ in the same order as function composition.

6.1. **The set $\mathcal{D}$.** In this subsection we propose a candidate $\mathcal{D}$ for the definable subsets of $\mathcal{M}$ (definition 2.5). $\mathcal{D}$ will consist of $|\mathcal{M}|$, the set including every other elements of $|\mathcal{M}|$, the set including every other elements of the previous set, and so forth. $\mathcal{D}$ is closed under translations and finite unions and adding/removing finitely many elements. We first define the equivalence relation $\sim$, the subset $M(2^r, z)$ of $|\mathcal{M}|$, and a set $\mathcal{B}$ of subsets for $|\mathcal{M}|$, then we will define $\mathcal{D}$.

For sets I, J we define $I \overset{\subseteq}{\sim} J$ as "$(I \setminus J)$ is finite": this means "$I \subseteq J$ up to finitely many elements". We define $I \sim J$ as $I \overset{\subseteq}{\sim} J \wedge J \overset{\subseteq}{\sim} I$: 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 $r \in \mathbb{N}$, $s \in \mathbb{Z}$ we define the following set of elements of $|\mathcal{M}|$:

$$M(2^r, s) \ = \ \{0_{\mathcal{M}} + (2^r * z + s) \mid 2^r * z + s \geq 0 \wedge z \in \mathbb{Z}\} \ \cup \ \{0_{\mathbb{Z}} + (2^r * z + s) \mid z \in \mathbb{Z}\}$$

If $r = 0, s = 0$ then $M(2^r, s) = |\mathcal{M}|$. We write $\mathcal{B}$ for the set of all sets $M(2^r, s)$, for some $r \in \mathbb{N}$, $s \in \mathbb{Z}$. Since $2^r > 0$, all sets $M(2^r, s)$ are infinite. We define $\mathcal{D}$ as the set of subsets which equal finite unions of sets in $\mathcal{B}$ up to finitely many elements.

Definition 6.1 (The set $\mathcal{D}$). $D \in \mathcal{D}$ if and only if $D \subseteq |\mathcal{M}|$ and $D \sim (B_1 \cup \ldots \cup B_n)$ for some $B_1, \ldots, B_n \in \mathcal{B}$.

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

Lemma 6.2 ($\mathcal{D}$-Lemma). *Let $a_0, a \in \mathbb{N}$ 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 any D there are some a and $0 \leq b_1 < \ldots < b_i < 2^a$ 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. *D satisfies the induction schema for N.*
6. *$\mathcal{D}$ is closed under $\sim$, complement and finite union.*

Proof. 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 can 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. Assume $D \sim (B_1 \cup \ldots \cup B_n)$. By the point 2 above there are $a_1, \ldots, a_n$ such that for all $a \geq a_1, \ldots, a_n$ and all $i = 1, \ldots, n$ there are $0 \leq b_{i,1} < \ldots < b_{i,n_i} < 2^a$ such that $B_i = (M(2^a, b_{i,1}) \cup \ldots \cup M(2^a, b_{i,n_i}))$. It follows our claim with $a = \max(a_1, \ldots, a_n)$.

4. From the point 3 above there are a and $0 \leq b_1 < \ldots < b_i < 2^a$ in $\mathbb{N}$ such that $D \sim (M(2^a, b_1) \cup \ldots \cup M(2^a, b_i))$. For any $M(2^a, b) \subseteq |\mathcal{M}|$ we have $\mu(M(2^a, b) \cap |\mathcal{M}|) = 1/2^a$. Since $0 \leq b_1 < \ldots < b_i < 2^a$, the sets $M(2^a, b_1), \ldots, M(2^a, b_i)$ are pairwise disjoint. From $\mu(D)$ finite additive, we deduce that $\mu(D) = i/2^a$.

5. By the point 4 above and Lemma 5.5, D satisfies the induction schema for N.

6. By construction, $\mathcal{D}$ is closed under $\sim$ and finite union. Thus, we have to prove that if $D \in \mathcal{D}$ then $(|\mathcal{M}| \setminus D) \in \mathcal{D}$. By the point 3 above there are a and $0 \leq b_1 < \ldots < b_i < 2^a$ in $\mathbb{N}$ 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 definition, we conclude that $(|\mathcal{M}| \setminus D) \in \mathcal{D}$. $\square$

6.2. **The Set $\mathcal{R}$ of Partial Bijections on $|\mathcal{M}|$.** In this subsection we define a set $\mathcal{R}$ of partial bijections on $|\mathcal{M}|$ whose domains are in $\mathcal{D}$.

From now on, for $n \in \mathbb{N}$ we call the relation R^n the n-th power of the relation R. R^n is defined by iterating composition n times: R^0 is the identity relation and R^{n+1} is $R^n \circ R$. We define a negative power of a relation by $R^{-n} = (R^{-1})^n$, where R^{-1} denotes the inverse of R. Let $R_0 = |\mathcal{M}|^2 \setminus p_{\mathcal{M}}$. Graphically, R_0 is the union of the three lines we see in the image in section 5.2. We will define $\mathcal{R}$ as the set of binary relations on $|\mathcal{M}|$ which include R_0^z for some $z \in \mathbb{Z}$, constant addition relation, plus all relations we obtain from those by restricting the domain to some $D \in \mathcal{D}$.

We first define some set $\mathcal{F}$ of straight lines. $\mathcal{F}$ is the set of maps $\phi : \mathbb{Q} \to \mathbb{Q}$, defined by $\phi(x) = 2^z x + r$ for some $z \in \mathbb{Z}$ and some $r \in \mathbb{Q}$. $\mathcal{F}$ 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 $\mathbb{Q} + \mathbb{Q} = \{(i, r) \mid i = 1, 2 \wedge r \in \mathbb{Q}\}$. We extend the notations $0_{\mathcal{M}} + n$ and $0_{\mathbb{Z}} + z$ for $n \in \mathbb{N}, z \in \mathbb{Z}$ to the notations $0_{\mathcal{M}} + r = (1, r) \in \mathbb{Q} + \mathbb{Q}$ and $0_{\mathbb{Z}} + r = (2, r) \in \mathbb{Q} + \mathbb{Q}$ for $r \in \mathbb{Q}$.

Let $\phi \in \mathcal{F}$, $\phi(x) = 2^z x + r$ with $z \in \mathbb{Z}$ and $r \in \mathbb{Q}$. We say that $\phi_{\mathcal{M}}$ is *even* if z even, and that ϕ is *odd* if z is odd. For any $\phi \in \mathcal{F}$ we define a map $\phi_{\mathcal{M}} : \mathtt{dom}(\phi) \to \mathbb{Q} + \mathbb{Q}$. We set $\phi_{\mathcal{M}}((i, r)) = (i, \phi(r))$ if ϕ is even, and if ϕ is odd: $\phi_{\mathcal{M}}((1, r)) = (2, \phi(r))$, $\phi_{\mathcal{M}}((2, r)) = (2, \phi(r))$ if $r < 0$, $\phi_{\mathcal{M}}((2, r)) = (1, \phi(r))$ if $r \geq 0$. We say that ϕ is sign-preserving at $0_{\mathcal{M}} + a \in |\mathcal{M}|$ if $a \geq 0$ implies $\phi(a) \geq 0$, it is sign-preserving at $0_{\mathbb{Z}} + b \in |\mathcal{M}|$ if $b \geq 0 \Leftrightarrow \phi(b) \geq 0$. ϕ is sign-preserving on $E \subseteq |\mathcal{M}|$ if ϕ is sign-preserving on all $e \in E$.

Assume $\phi(x)$ is sign-preserving on $E \subseteq |\mathcal{M}|$. We deduce: if ϕ is even, then $\phi_{\mathcal{M}}(\mathtt{N} \cap E) \subseteq \mathtt{N}$ and $\phi_{\mathcal{M}}(\mathtt{Z}^- \cap E) \subseteq \mathtt{Z}^-$ and $\phi_{\mathcal{M}}(\mathtt{Z}_0^+ \cap E) \subseteq \mathtt{Z}_0^+$; if ϕ is odd, then $\phi_{\mathcal{M}}(\mathtt{N} \cap E) \subseteq \mathtt{Z}_0^+$ and $\phi_{\mathcal{M}}(\mathtt{Z}^- \cap E) \subseteq \mathtt{Z}^-$ and $\phi_{\mathcal{M}}(\mathtt{Z}_0^+ \cap E) \subseteq \mathtt{N}$. As a consequence, if ϕ is sign-preserving on $E \subseteq |\mathcal{M}|$, and $\phi(E) \subseteq F$, and ψ is sign-preserving on F, then $(\psi \circ \phi)_{\mathcal{M}}$ and $\psi_{\mathcal{M}} \circ \phi_{\mathcal{M}}$ coincide when restricted to E.

A *partial bijection* on $|\mathcal{M}|$ is a one-to-one relation between two subsets of $|\mathcal{M}|$. A *partial identity* on $|\mathcal{M}|$ is the identity relation on some subset of $|\mathcal{M}|$. We now define a set $\mathcal{R}$ of partial bijections on $|\mathcal{M}|$ which are the restriction of $\phi_{\mathcal{M}}$ to some $D \in \mathcal{D}$, for some $\phi \in \mathcal{F}$, and have range some $E \in \mathcal{D}$. For instance, one bijection in $\mathcal{R}$ is defined by $\phi(x) = 2^2 x$, with domain $|\mathcal{M}|$ and codomain $M(2^2, 0)$, mapping $0_{\mathcal{M}} + n \mapsto 0_{\mathcal{M}} + 4n$ and $0_{\mathbb{Z}} + z \mapsto 0_{\mathbb{Z}} + 4z$.

We define "even" and "odd" bijections. They will be restrictions of an even or odd power of the relation $R_0 = |\mathcal{M}|^2 \setminus p_{\mathcal{M}}$.

We write M for $|\mathcal{M}|$.

Definition 6.3 (The set of partial bijections $\mathcal{R}$). Let $D, E \in \mathcal{D}$ and $\phi \in \mathcal{F}$, $\phi(x) = 2^z * x + r$.

1. R is a (D, E, ϕ)-bijection if R is in $\mathcal{R}$. and $\mathtt{dom}(R) = D, \mathtt{range}(R) = E$ and $\forall a \in D.\forall b \in |\mathcal{M}|.R(a, b) \Leftrightarrow b = \phi_{\mathcal{M}}(a)$ and ϕ is sign-preserving on E.
2. R is an even (odd) bijection if R is a (D, E, ϕ) bijection and ϕ is even (odd).
3. $\mathcal{R}$ is the set of all (D, E, ϕ)-bijections for $D, E \in \mathcal{D}$ and $\phi \in \mathcal{F}$.

R_0, the complement of $p_{\mathcal{M}}$, is an example of an odd bijection, shown as follows. R_0 is a partial bijection. For all $n \in \mathbb{N}$, R_0 maps $0_{\mathcal{M}} + n \mapsto 0_{\mathbb{Z}} + 2n$ and $0_{\mathbb{Z}} - (n+1) \mapsto 0_{\mathbb{Z}} - 2(n+1)$ and $0_{\mathbb{Z}} + n \mapsto 0_{\mathcal{M}} + 2n$. R_0 is the restriction of $\phi_{\mathcal{M}}$ to $|\mathcal{M}|$, where ϕ is the odd map $\phi(x) = 2^1 x$.

We will prove that the definable sets of $\mathcal{M}$ (definition 2.5) can be expressed by the propositional formulas whose predicates are equality and symbols for predicates in $\mathcal{R}$.

Lemma 6.4 (ϕ-Lemma). *Let $\phi(x) = 2^{z_1}x + r_1$, $z_1 \in \mathbb{Z}$, $r_1 \in \mathbb{Q}$.*

1. *Assume $r \in \mathbb{N}$, $z \in \mathbb{Z}$ and $B = M(2^r, z) \in \mathcal{B}$ and $B' = M(2^{r+z_1}, 2^{z_1}z + r_1)$. If $B' \in \mathcal{B}$ then $\phi_{\mathcal{M}}(B) \sim B'$.*

2. *If $B \in \mathcal{B}$ and $\phi_{\mathcal{M}}(B) \widetilde{\subseteq} |\mathcal{M}|$, then $\phi_{\mathcal{M}}(B) \sim B'$ for some $B' \in \mathcal{B}$*

3. *If $D \in \mathcal{D}$ and $\phi_{\mathcal{M}}(D) \subseteq |\mathcal{M}|$ then $\phi_{\mathcal{M}}(D) \in \mathcal{D}$*

Proof.

1. From $B, B' \in \mathcal{B}$ we deduce $B = (B \cap \mathbb{N}) \cup (B \cap \mathbb{Z}^-) \cup (B \cap \mathbb{Z}_0^+)$, and the same for B'. If ϕ is even we have $\phi_{\mathcal{M}}(B \cap \mathbb{N}) \sim B' \cap \mathbb{N}$ and $\phi_{\mathcal{M}}(B \cap \mathbb{Z}^-) \sim B' \cap \mathbb{Z}^-$ and $\phi_{\mathcal{M}}(B \cap \mathbb{Z}_0^+) \sim B' \cap \mathbb{Z}_0^+$. If ϕ is odd we have $\phi_{\mathcal{M}}(B \cap \mathbb{N}) \sim B' \cap \mathbb{Z}_0^+$ and $\phi_{\mathcal{M}}(B \cap \mathbb{Z}^-) \sim B' \cap \mathbb{Z}^-$ and $\phi_{\mathcal{M}}(B \cap \mathbb{Z}_0^+) \sim B' \cap \mathbb{N}$. In both cases we conclude that $\phi_{\mathcal{M}}(B) \sim B'$.

2. Assume $B = M(2^r, z)$ for some $r \in \mathbb{N}$, $z \in \mathbb{Z}$ and $\phi_{\mathcal{M}}(a) \in |\mathcal{M}|$ for all but finitely many $a \in B$. By definition, the set $\phi_{\mathcal{M}}(B)$ includes elements of $|\mathcal{M}|$ with second coordinate $r_w = (2^{r+z_1} * w + (2^{z_1}z + r_1)) \in \mathbb{Z}$, for all but finitely many $w \in \mathbb{Z}$. If we choose two consecutive values of w such that $r_w \in \mathbb{Z}$, we deduce that $2^{r+z_1} \in \mathbb{Z}$ and $2^{z_1}z + r_1 \in \mathbb{Z}$, hence that $r + z_1 \in \mathbb{N}$. Thus, $M(2^{r+z_1}, 2^{z_1}z + r_1)$ is a set of $\mathcal{B}$. By the point 1 above we have $\phi_{\mathcal{M}}(B) \sim M(2^{r+z_1}, 2^{z_1}z + r_1)$. We conclude that $\phi_{\mathcal{M}}(B) \sim B'$ for some $B' \in \mathcal{B}$.

3. If $D \in \mathcal{D}$ then by Lemma 6.2, point 3, we have $D \sim M(2^{a_1}, b_1) \cup \ldots \cup M(2^{a_i}, b_i)$ for some $a_1, \ldots, a_i \in \mathbb{N}$ and some $b_1, \ldots, b_i \in \mathbb{Z}$. From $\phi_{\mathcal{M}}(D) \subseteq |\mathcal{M}|$ we deduce $\phi_{\mathcal{M}}(a) \in |\mathcal{M}|$ for all but finitely many $a \in M(2^{a_1}, b_1) \cup \ldots \cup M(2^{a_i}, b_i)$. By the point 2 above we obtain $\phi_{\mathcal{M}}(M(2^{a_1}, b_1)) \sim B_1', \ldots, \phi_{\mathcal{M}}(M(2^{a_i}, b_i)) \sim B_n'$ for some $B_1', \ldots, B_n' \in \mathcal{B}$. Thus, $\phi_{\mathcal{M}}(D) \in \mathcal{D}$. $\square$

$\mathcal{R}$ and $\mathcal{D}$ satisfy the following closure properties.

Lemma 6.5 (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. $R^{-1} \in \mathcal{R}$

Proof.

1. $\mathtt{id}_D$ is an even $(D, D, \mathtt{id})$-bijection.

2. If R is a (A, B, ϕ)-bijection, then by $\phi_{\mathcal{M}}(A \cap D) = R(D) \subseteq B \subseteq |\mathcal{M}|$ we deduce $\phi_{\mathcal{M}}(A \cap D) \subseteq |\mathcal{M}|$. By Lemma 6.4, by $A \cap D \in \mathcal{D}$ and $\phi_{\mathcal{M}}(A \cap D) \subseteq |\mathcal{M}|$ we deduce $R(D) \in \mathcal{D}$.

3. S is some (A, B, ϕ)-bijection and R is some (C, D, ψ)-bijection. If R is an even bijection, then R maps $\mathbb{N}$ in $\mathbb{N}$, and $\mathbb{Z}_0^+$ in $\mathbb{Z}_0^+$, and $\mathbb{Z}^-$ in $\mathbb{Z}^-$. If R is an odd bijection, then R maps $\mathbb{N}$ in $\mathbb{Z}_0^+$, and $\mathbb{Z}_0^+$ in $\mathbb{N}$, and $\mathbb{Z}^-$ in $\mathbb{Z}^-$. 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 the other is even, and it is some $(\phi_{\mathcal{M}}^{-1}(B \cap C), \psi_{\mathcal{M}}(B \cap C), \psi \circ \phi)$-bijection. Here we use the fact that $B, C \in \mathcal{D}$ imply $B \cap C \in \mathcal{D}$ by closure of $\mathcal{D}$ under intersection, and that $\phi^{-1} \in \mathcal{F}$ and $\phi_{\mathcal{M}}^{-1}(B \cap C) \subseteq A \subseteq |\mathcal{M}|$ imply $\phi_{\mathcal{M}}^{-1}(B \cap C) \in \mathcal{D}$ by Lemma 6.4, point 2. In the same way we prove that $\psi_{\mathcal{M}}(B \cap C) \in \mathcal{D}$.

4. Assume that R is a (D, E, ϕ)-bijection. Then R^{-1} is even or odd according to what is R, and is a (E, D, ϕ^{-1})-bijection. $\square$

We write $L(\mathcal{R})$ for the first-order language generated from binary predicate symbols for relations in $\mathcal{R}$. Our goal is to prove that every first-order definable set in $\mathcal{M}$ is in $\mathcal{D}$. Since the sets definable in $L(\mathcal{R})$ include those definable in $\mathcal{M}$, it is enough to prove that any first-order definable set in $L(\mathcal{R})$ is in $\mathcal{D}$. To this aim, we need a quantifier-elimination result for a language including $L(\mathcal{R})$.

7. Quantifier Elimination Result for Partial Bijections

In this section we prove a quantifier elimination result for some set of partial bijections, which is an abstract counterpart of the set $\mathcal{R}$ introduced in section 6. The quantifier elimination result holds when $\mathcal{R}$ is closed under composition and inverse. It is a simple, self-contained result introducing a model-theoretical tool of some interest. The only part of this section which is used in the rest of the paper is the theorem 7.4, which will be used to characterize the sets which are first order definable from the set $\mathcal{R}$. We take the definition of quantifier elimination from [8], section 3.1, section 3.2.

Definition 7.1. A set $\mathcal{R}$ of bijections on U is called *closed under composition and inverse*, if $R, S \in \mathcal{R}$ implies $R^{-1}, R \circ S \in \mathcal{R}$.

Lemma 7.2. *Assume R_1, R_2 are in $\mathcal{R}$ that is closed under composition and inverse.*
(1) $\exists x_2 R_1(x_1, x_2) \leftrightarrow R_1^{-1} \circ R_1(x_1, x_1)$.
(2) $R_1(x_1, x_2) \wedge R_2(x_2, x_3) \leftrightarrow R_1(x_1, x_2) \wedge R_2 \circ R_1(x_1, x_3)$.

Proof.
(1) $\leftarrow$ trivially holds. Since R_1 is a partial bijection, $\rightarrow$ holds.
(2) $\rightarrow$ trivially holds. We will show $\leftarrow$. Assume $R_1(x_1, x_2) \wedge R_2 \circ R_1(x_1, x_3)$. Then $R_1^{-1}(x_2, x_1)$. Then $R_2 \circ R_1 \circ R_1^{-1}(x_2, x_3)$. By definition of composition, $R_2 \circ R_1 \circ R_1^{-1}(x_2, x_3) \rightarrow \exists x_1 x_2'(R_1^{-1}(x_2, x_1) \wedge R_1(x_1, x_2') \wedge R_2(x_2', x_3))$. Since R_1 is a partial bijection, $x_2 = x_2'$. Hence $R_2 \circ R_1 \circ R_1^{-1}(x_2, x_3) \rightarrow R_2(x_2, x_3)$. Hence we have the left-hand side. $\qquad\square$

For a set $\mathcal{R}$ of partial bijection on U we will consider the structure $(U, \mathcal{R})$ where U is the universe and each partial bijection in $\mathcal{R}$ is a binary relation. We will also consider the theory of the structure $(U, \mathcal{R})$ where each element u in U is denoted by the constant u itself and each partial bijection R in $\mathcal{R}$ is denoted by the predicate symbol R itself.

Theorem 7.3 (Quantifier Elimination). *If $\mathcal{R}$ is a set of partial bijection on U that is closed under composition and inverse, the theory of the structure $(U, \mathcal{R})$ admits quantifier elimination.*

Proof. Let $\mathcal{U}$ be the structure $(U, \mathcal{R})$.
(1) First we will show the following claim:

If $\mathcal{R}$ is a set of partial bijection on U that is closed under composition and inverse, the theory of the structure $(U, \mathcal{R})$ without $=$ admits quantifier elimination.

Assume a quantifier-free formula A of $L(\mathcal{U})$ is given. Let $FV(A) = \{x_1, \ldots, x_n\}$. We assume A is a disjunctive normal form. We will find a quantifier-free formula B of $L(\mathcal{U})$ that is equivalent to $\exists x_n A$ in $\mathcal{U}$. Since $\exists x_n$ can be distributed over disjuncts, we can assume A does not contain disjunction.

First we replace $R(x_i, x_j)$ by $R^{-1}(x_j, x_i)$ in A if $i > j$. Then we can assume $i \leq j$ for every $R(x_i, x_j)$ in A.

- Case 1. There is some positive $R_1(x_i, x_n)$ in A such that $i < n$.
  We replace every positive or negative $R_3(x_j, x_n)$, $R_4(x_n, x_j)$, and $R_5(x_n, x_n)$ for $j < n$ except the atom $R_1(x_i, x_n)$ by $R_1^{-1} \circ R_3(x_j, x_i)$, $R_4 \circ R_1(x_i, x_j)$, and $R_1^{-1} \circ R_5 \circ R_1(x_i, x_i)$ respectively. Then atoms that contain x_n is only the positive $R_1(x_i, x_n)$. Let the result be $C \wedge R_1(x_i, x_n)$. Then $\exists x_n A \leftrightarrow C \wedge \exists x_n R_1(x_i, x_n)$.
  Then $\exists x_n R_1(x_i, x_n) \leftrightarrow R_1^{-1} \circ R_1(x_i, x_i)$. Hence $\exists x_n A \leftrightarrow C \wedge R_1^{-1} \circ R_1(x_i, x_i)$. Take B to be it.
- Case 2. Positive atoms that contain x_n are only $R_1(x_n, x_n), \ldots, R_k(x_n, x_n)$.
  Let A be $A_1 \wedge R_1(x_n, x_n) \wedge \ldots \wedge R_k(x_n, x_n) \wedge \neg R_1'(x_n, x_n) \wedge \ldots \wedge \neg R_m'(x_n, x_n) \wedge A_2$ where $k, m \geq 0$, A_1 does not contain x_n and each atom in A_2 is negative and contains both x_n and x_i for some $i < n$.
  Let X be $\{x \in U \mid R_1(x, x), \ldots, R_k(x, x), \neg R_1'(x, x), \ldots, \neg R_m'(x, x)\}$.
- Case 2.1. X is finite.
  Let X be $\{u_1, \ldots, u_m\}$. Take B to be $\bigvee_{u \in X} A[x_n := u]$. Then $\exists x_n A \leftrightarrow B$.
- Case 2.2. X is infinite.
  By moving $\exists x_n$ inside, $\exists x_n A \leftrightarrow A_1 \wedge \exists x_n (R_1(x_n, x_n) \wedge \ldots \wedge R_k(x_n, x_n) \wedge \neg R_1'(x_n, x_n) \wedge \ldots \wedge \neg R_m'(x_n, x_n) \wedge A_2)$. Take B to be A_1. Then $\exists x_n A \leftrightarrow B$, since we can show $\exists x_n (R_1(x_n, x_n) \wedge \ldots \wedge R_k(x_n, x_n) \wedge \neg R_1'(x_n, x_n) \wedge \ldots \wedge \neg R_m'(x_n, x_n) \wedge A_2)$ as follows. Fix a negative atom $\neg R''(x_i, x_n)$ in A_2 where $i < n$. Given $x_1, \ldots, x_{n-1}$, we have $|\{x_n \in U \mid R''(x_i, x_n)\}| \leq 1$ since R'' is a partial bijection. Let Y be $\{x_n \in U \mid A_2\}$. Then Y is cofinite. Since X is infinite, $X \cap Y \neq \emptyset$. Hence $\exists x_n (R_1(x_n, x_n) \wedge \ldots \wedge R_k(x_n, x_n) \wedge \neg R_1'(x_n, x_n) \wedge \ldots \wedge \neg R_m'(x_n, x_n) \wedge A_2)$ is true.

We have shown the claim.

Next we will show the theorem by using (1).

Assume a formula A is given. Let $\mathcal{R}'$ be $\mathcal{R} \cup \{\mathrm{id}_U\}$. Then $\mathcal{R}'$ is also closed under composition and inverse. Let A' be the formula obtained from A by replacing $t_1 = t_2$ by $\mathrm{id}_U(t_1, t_2)$. Then A' is a formula in the theory of the structure $(U, \mathcal{R}')$ without $=$. By (1), we have a quantifier-free formula B' equivalent to A' in the theory of the structure $(U, \mathcal{R}')$. Let B be the formula obtained from B' by replacing $\mathrm{id}_U(t_1, t_2)$ by $t_1 = t_2$. Then B is a quantifier-free formula in the theory of $\mathcal{U}$ and $B \leftrightarrow A$. □

Theorem 7.4 (Quantifier and Constant Elimination). *If $\mathcal{R}$ is a set of partial bijection on U that is closed under composition and inverse, and $\mathrm{id}_{\{u\}} \in \mathcal{R}$ for every $u \in U$, then in the theory of the structure $(U, \mathcal{R})$, for any given formula, there is some quantifier-free constant-free formula that is equivalent to the formula.*

Proof. Assume a formula A is given. Choose any variable x. By the theorem 7.3, there is a quantifier-free formula B that is equivalent to A. In B, we replace $R(u_1, u_2)$ with constants u_1, u_2 by $x = x$ if $R(u_1, u_2)$ is true, and replace it by $\neg x = x$ if it is false.

In B, we replace $R(u, x)$ with constants u by $\mathrm{id}_{\{u_1\}}(x, x)$ if $R(u, x)$ is equivalent to $x = u_1$, and replace it by $\neg x = x$ if it is false.

In B, we replace $R(x, u)$ with constants u in the same way as $R(u, x)$.

Let C be the result. Then $A \leftrightarrow C$ and C is a quantifier-free constant-free formula. □

Example 7.5 (Quantifier and constant elimination). Our proof of the quantifier elimination results give an effective way to transform any $A \in L(\mathcal{U})$ into some equivalent quantifier-free $B \in L(\mathcal{R})$. We explain how this method works by two examples. Assume $R_1, R_2, R_3 \in \mathcal{R}$.

We will eliminate quantifiers in $\exists x_4.A$ for a given quantifier-free formula A in the language $L(\mathcal{U})$, by producing some equivalent quantifier-free formula $B \in L(\mathcal{R})$.

- Example 1. $A = (R_1(x_1, x_4) \land R_2(x_2, x_4) \land \neg R_3(x_3, x_4))$. First we can use $R_1(x_1, x_4)$ to eliminate x_4 in the other atoms, since R_1 is a partial bijection. Then $\exists x_4 A$ is equivalent to

$$\exists x_4 (R_1(x_1, x_4) \land R_1^{-1} \circ R_2(x_2, x_1) \land \neg R_1^{-1} \circ R_3(x_3, x_1)).$$

  Next we move $\exists x_4$ inside and obtain an equivalent formula

$$\exists x_4 (R_1(x_1, x_4)) \land R_1^{-1} \circ R_2(x_2, x_1) \land \neg R_1^{-1} \circ R_3(x_3, x_1).$$

  Then we can replace $\exists x_4 (R_1(x_1, x_4))$ by $R_1^{-1} \circ R_1(x_1, x_1)$, since R_1 is a partial bijection, to obtain an equivalent formula

$$R_1^{-1} \circ R_1(x_1, x_1) \land R_1^{-1} \circ R_2(x_2, x_1) \land \neg R_1^{-1} \circ R_3(x_3, x_1),$$

  which we can take B to be.
- Example 2. $A = (R_1(x_1, x_3) \land R_2(x_4, x_4) \land \neg R_3(x_3, x_4))$. First we move $\exists x_4$ inside and obtain an equivalent formula

$$R_1(x_1, x_3) \land \exists x_4 (R_2(x_4, x_4) \land \neg R_3(x_3, x_4)).$$

  Let X be $\{x \in U \mid R_2(x, x)\}$. We have two cases according to whether X is finite or not.
  - Case 1. X is finite.
    For example, we assume X is $\{u_1, u_2\}$. By replacing existential quantification by disjunction we obtain an equivalent formula

$$R_1(x_1, x_3) \land (\neg R_3(x_3, u_1) \lor \neg R_3(x_3, u_2)).$$

    Since R_3 is a partial bijection, $R_3(x_3, u)$ is equivalent to false or $x_3 = u'$ for some $u' \in U$. For example, we assume $R_3(x_3, u_1)$ is equivalent to $x_3 = u_1'$ and $R_3(x_3, u_2)$ is equivalent to $x_3 = u_2'$. Since $x_3 = u_i'$ is equivalent to $\mathrm{id}_{u_i'}(x_3, x_3)$ for $i = 1, 2$, we can take B to an equivalent formula

$$R_1(x_1, x_3) \land (\neg \mathrm{id}_{u_1'}(x_3, x_3) \lor \neg \mathrm{id}_{u_2'}(x_3, x_3)).$$

  - Case 2. X is infinite.
    For a given $u_3 \in U$, $|\{x_4 \in U \mid \neg R_3(u_3, x_4)\}|$ is cofinite, since R_3 is a partial bijection. Since X is infinite, $\exists x_4 (R_2(x_4, x_4) \land \neg R_3(x_3, x_4))$ is true. Hence we can take B to be an equivalent formula

$$R_1(x_1, x_3).$$

8. Main Theorem

In this section we prove that the statement 2-Hydra is a counterexample to the Brotherston conjecture. Assume $\mathcal{M}$ is the structure for the language Σ_N with universe $|\mathcal{M}|$ defined in section 5. Recall that $L(\mathcal{R})$ denoted the language having a predicate symbol for each $R \in \mathcal{R}$, where we identify R and the symbol denoting R. We write $L(\mathcal{M})$ for the language generated from $\Sigma_N \cup |\mathcal{M}|$. We consider the equality predicate $=$ a part of any first order language.

We write $\mathcal{U}$ for the structure $(|\mathcal{M}|, 0_{\mathcal{M}}, s_{\mathcal{M}}, N_{\mathcal{M}}, p_{\mathcal{M}}, \mathcal{R})$. We write $L(\mathcal{U})$ for the first-order language generated from $|\mathcal{M}|, 0, s, N, p, \mathcal{R}$.

Lemma 8.1 (Translation from $L(\mathcal{U})$ to $L(\mathcal{R})$). *Let $\mathcal{R}$ be that introduced in section 6. Then all atomic formulas $A \in L(\mathcal{U})$ are equivalent to some formula $B \in L(\mathcal{R})$ in $\mathcal{U}$.*

Proof. Translation is defined to be homomorphic with logical connectives.

- $N(t)$ is translated into true.
- $x = y$ is translated into $\mathrm{id}_M(x, y)$.
- $x = s^n(0)$ is translated into $\mathrm{id}_{\{(1,n)\}}(x, x)$.
- $x = s^n((i, a))$ for $(i, a) \in M$ is translated into $\mathrm{id}_{\{(i,a+n)\}}(x, x)$.
- $x = s^n(y)$ is translated into $R(y, x)$ where $R = (|\mathcal{M}|, |\mathcal{M}| - \{0, 1, \ldots, n - 1\}, \phi)$ and $\phi(x) = x + n$.
- $t_1 = t_2$ is first translated into $\exists xy(x = t_1 \wedge y = t_2 \wedge x = y)$, then translated into some formula by using above translation.
- $p(t_1, t_2)$ is first translated into $\exists xy(x = t_1 \wedge y = t_2 \wedge p(x, y))$, then translated into some formula by using above translation.
- $R(t_1, t_2)$ is first translated into $\exists xy(x = t_1 \wedge y = t_2 \wedge R(x, y))$ for $R \in \mathcal{R}$. then translated into some formula by using above translation. $\square$

Lemma 8.2. *If $X = \{x \in M \mid R(x, x)\}$ for some $R \in \mathcal{R}$, then $X \in \mathcal{D}$.*

Proof. Let R be (A, B, ϕ) where $\phi(x) = 2^a x + b$. If $(a, b) = (0, 0)$, then $X = A$ and $X \in \mathcal{D}$. If $(a, b) \neq (0, 0)$, $|X| \leq 2$ since X is the intersection of the lines $\{(x, y) \in M^2 \mid y = \phi(x), x \in A\}$ and the line $\{(x, y) \in M^2 \mid x = y\}$. Hence $X \in \mathcal{D}$. $\square$

Theorem 8.3 (Counterexample to the Brotherston-Simpson Conjecture)**.** *Let H be the formula defined in Definition 3.5. 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 of H in $\mathtt{CLKID}^\omega$ is shown in Theorem 4.7. The non-provability of H in $\mathtt{LKID}(\Sigma_N, \Phi_N) + (0, s)$-axioms is shown as follows. Let $\mathcal{M}$ be the structure defined in section 5.2: $\mathcal{M}$ falsifies H by Lemma 5.3.

We defined $\mathcal{H}_\mathcal{M}$ as the Henkin family of definable sets in $\mathcal{M}$ (definition 2.5). What is left to be proved is: $(\mathcal{M}, \mathcal{H}_\mathcal{M})$ is a Henkin model of $\mathtt{LKID}(\Sigma_N, \Phi_N)$. By definition of Henkin model we have to prove that any prefixed point of the monotone operator ϕ_{Φ_N} with the restriction in $\mathcal{H}_\mathcal{M}$ includes the interpretation of N. As we already pointed out, since the interpretation of N is $\mathcal{M}$ itself, this is to say that *any set in $\mathcal{H}_1$ of $\mathcal{H}_\mathcal{M}$ which is closed under 0 and s is equal to $\mathcal{M}$.*

Let $\mathcal{R}, \mathcal{D}$ be the set of relations and domains defined in Def. 6.1, 6.3, and let $\mathcal{U} = (|\mathcal{M}|, \mathcal{R})$ be the partial bijection structure defined by $\mathcal{R}$. By induction on the formula we prove that all formulas $A \in L(\mathcal{M})$ are equivalent in $\mathcal{U}$ to some formula $B \in L(\mathcal{R})$: in the case A is an atomic formula we use Lemma 8.1, in the cases $A = \neg A_1, A_1 \vee A_2, \exists x.A_1$ the induction hypothesis on A_1, A_2.

$\mathcal{D}$ includes all singletons and it is closed under complement and finite union by Lemma 6.2. $\mathcal{R}$ is closed under composition and inverse by Lemma 6.5, points 3, 4, By Theorem 7.4, each $A \in L(\mathcal{U})$ having exactly one free variable x is equivalent in $\mathcal{U}$ to some quantifier-free $B \in L(\mathcal{R})$. By replacing by x each variable $y \neq x$ in B we obtain a formula B' equivalent to A, which is a boolean combination of atoms of the form $R(x, x)$ for some $R \in \mathcal{R}$, or the form $x = x$. Assume an atom of the form $R(x, x)$. Then $D = \{x \in |\mathcal{M}|^2 \mid R(x, x)\}$ is in $\mathcal{D}$ by Lemma 8.2. Assume an atom of the form $x = x$. Then $\{x \in U \mid x = x\}$ is $U \in \mathcal{D}$. Thus, each atom $R(x, x)$ in B' is equivalent to $x \in D$ for some $D \in \mathcal{D}$. By the closure properties for $\mathcal{D}$ we deduce that B' defines some set D' in $\mathcal{D}$. By Lemma 6.2, point 4, D' has a dyadic measure, and by Lemma 5.5 D' satisfies the induction schema. Hence $(\mathcal{M}, \mathcal{H}_\mathcal{M})$ is a Henkin model of $\mathtt{LKID}(\Sigma_N, \Phi_N)$, as we wished to show. $\square$

8.1. **Non-Conservativity of the Inductive Definition System** LKID. This subsection shows a side result: non-conservativity of LKID with respect to additional inductive predicates, by giving a counterexample.

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 the 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.

Theorem 8.4 (Non-Conservativity). *There are $\Sigma_1, \Phi_1, \Sigma_2, \Phi_2$ such that* LKID(Σ_2, Φ_2) *is an extension of* LKID(Σ_1, Φ_1) *and* LKID(Σ_2, Φ_2) *is not conservative over* LKID(Σ_1, Φ_1).

Proof. Take Σ_1 to be $0, s, N, p$ and Φ_1 to be Φ_N and Σ_2 to be $\Sigma_1 \cup \{\leq\}$ and Φ_2 to be Φ_1 with the production rules for $\leq$. Then the sequent 0-axiom $\vdash H$ is in the language of LKID(Σ_1, Φ_1) but it is not provable in LKID(Σ_1, Φ_1) by Theorems 8.3, while it is provable in LKID(Σ_2, Φ_2) by Theorem 3.7. $\qquad\square$

9. CONCLUSION

We have proved in Thm. 8.3 that CLKID$^\omega$, the formal system of cyclic proofs [6] proves strictly more than LKID, Martin-Löf's formal system of inductive definitions with classical logic. This settles an open question given in [6]. In Theorem 8.4, by the same counterexample we also shows that if we add more inductive predicates to LKID we may obtain a non-conservative extension of LKID.

REFERENCES

[1] Stefano Berardi, Makoto Tatsuta, The Classic Martin-Löf's System of Inductive Definitions is not Equivalent to Cyclic Proofs, FOSSACS 2017, 301–317.

[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. Hauptsatz for the intuitionistic theory of iterated inductive definitions. In Proceedings of the Second Scandinavian Logic Symposium, pp. 179–216. North-Holland, 1971.

[11] Alex Simpson. Cyclic Arithmetic is Equivalent to Peano Arithmetic. Proceedings of Fossacs 2017.

[12] Sorin Stratulat, Structural vs. cyclic induction: a report on some experiments with Coq, 2016, SYNASC 2016: Proceedings of the 18th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing, p. 27-34, IEEE Computer Society