Negative and Positive Results about Cut-elimination for Cyclic Proofs (DRAFT)

S. Berardi, M. Tatsuta

January 13, 2023

Abstract. In this paper we give four examples of cyclic proofs having no cut-free form, for different reasons. We prove that cut-free cyclic proofs define algorithms requiring polynomial time and constant space, and therefore only exist for simple theorems. We found a common syntactical pattern to most failures of cut-elimination: the cuts include what we call *local* cuts. On the positive side, we prove cut-elimination for cyclic proofs having only non-local cuts.

1 Introduction

We consider LKID, Martin-Löf theory of inductive definitions plus classical logic ([3]), and an alternative proof system for the same language, cyclic proofs ([5]), with no explicit induction rule.

In this paper, we prove that cut-elimination for a formula A in a cyclic proof may fail for many reasons: if A includes quantifiers; if A includes some inductive predicate p whose productions discard some free variable in the conclusion; if our goal is proving the existence of an individual whose size is exponential in the parameters of the problem; and if our goal requires an algorithm running in non-constant space. This is the case of proving that two definitions of transitive closure for a binary relation are equivalent.

In all cases (except perhaps the first one) the cuts we could not eliminate are what we call *local* cuts. We give an example of a local cut in the case of the inductive predicate N, "being a natural number". Assume there is some cut between $\Gamma \vdash \Delta, N(Su)$ and $N(Su), \Gamma \vdash \Delta$. Assume we proved the first $N(Su)$ from $N(u)$ and the second $N(Su)$ from $Su = Sx, N(x)$ for some eigenvariable x of the proof. If $x \in \mathtt{FV}(u)$ we call the cut a local cut. Here "local" means that the value u assigned by the cut to the eigenvariable x depends from x itself. If this is never the case we call the cut a global cut.

Local and global cuts may be generalized to cuts on any inductive predicate, on quantifier-free formulas, and to sets of cuts. Our positive result will be: if the set of all cuts of a proof is global then we may remove all cuts.

We explain informally why often we cannot eliminate a local cut. A local cut may destroy regularity, the fact that a cyclic proof has only finitely many subproofs and formulas. Indeed, the normalization process applies infinitely many times the substitution $[u/x]$, and if $x \in \mathtt{FV}(u)$ then the substitutions $[u/x]$, $[u/x][u/x]$, $[u/x][u/x][u/x]$, ... produce different formulas, hence infinitely many formulas, hence a non-cyclic proof.

Global cuts are is simple, yet are not trivial. For instance, for any polynomial P there is a canonical proof that $\mathtt{N}$ is closed under P. The set of cuts of this proof is global, hence all these cuts may be removed. For comparison, we prove that there is a cyclic proof that $\mathtt{N}$ is closed under 2^x, but there is no cut-free cyclic proof of the same result.

2 Cut-elimination fails for cyclic proofs and quantified formulas

In this section we prove that cut-elimination fails for cyclic proofs if the cut include at least one quantifier. This result has the advantage of having a short proof, but it leaves open the possibility of cut-elimination for quantifier-free formulas. In the next sections, using a fine analysis of the properties of cut-free proofs, we will show that even for quantifier-free formulas we have cut-elimination only in particular cases.

We first introduce some notations. We call $\mathtt{CLKID}^\omega$ the set of cyclic theorems. $\mathtt{CLKID}^\omega$ is a non-conservative extensions of $\mathtt{LKID}$ ([3]). If we add some injectivity axioms for constructors to both theories they become equal ([7], [4]). From now on, let I-Σ^0_n, I-Π^0_n be the fragments of arithmetic with Σ^0_n-induction and C-Σ^0_n, C-Π^0_n be the fragments of cyclic proofs whose formulas are all Σ^0_n, Π^0_n. The sub-formula property for a theory is: all formulas occurring in a proof are subformula of the conclusion or of some assumption.

This paper is about cut-elimination and the sub-formula property. Arithmetical proofs have cut-elimination, yet a cut-free arithmetical proof has no sub-formula property when an induction axiom is applied to an open term. Indeed, let $\mathtt{Cons}_n$ be the consistency statement for I-Σ^0_n, expressed as a Δ^0_0-open statement. Then $\mathtt{Cons}_n$ is provable in arithmetic, yet it has no proof with the subformula property, otherwise this would be a proof in I-$\Sigma^0_0 \subseteq I$-Σ^0_n, contradicting Gödel's Incompleteness Theorem.

Cut-free cyclic Σ^0_n-proof have a weak form of sub-formula property. Indeed, since we have a left-rule for elimination of equality, whenever we have formulas $A[a, b]$ and $a = b$ in the proof we may also have $A[b, a]$. Due to the case rule, if we have a formula $\mathtt{N}t$ in the proof, then we may have $t = Sx$ in the same proof. Due to this weak sub-formula property, the argument against cut-elimination for arithmetical proofs may be adapted to show that cyclic proofs with quantifiers and whose only inductive predicate is $\mathtt{N}$ have no cut-elimination in general. For cyclic proofs, the proof of this result is more involved than for arithmetical proofs.

Theorem 2.1 *Cut-elimination fails for C-Σ^0_1 (for cyclic proofs with sequents made of Σ^0_1-formulas).*

Proof We use the following result ([1]): for all $n \in \mathtt{N}$ the theories I-Σ^0_{n+1} and C-Σ^0_n prove the same Π^0_{n+1}-theorems. Let $F = \mathtt{Cons}_1 \in \Delta^0_1$ be the consistency statement for I-Σ^0_1, expressed as an open formula. $\mathtt{Cons}_1$ is provable in I-Π^0_2. Indeed, truth for a Σ^0_1-open formula is a Π^0_2-statement. Thus, we may prove by Π^0_2-induction that all proofs using only Σ^0_1-sequents are true. Then we use free-cut elimination, which reduces all formulas to Σ^0_1-formula, in order to prove that all I-Σ^0_1-proofs with a Σ^0_2-conclusion are true, hence are not a proof of false. From I-$\Pi^0_2 \vdash F$ we obtain I-$\Sigma^0_2 \vdash F$ by [6]. By [1] for $n = 1$ and $F \in \Delta^0_1$ we have C-$\Sigma^0_1 \vdash F$, with a proof Π possibly using cuts. We prove that Π has no cut-free form. For contradiction, take any cut-free proof of C-$\Sigma^0_1 \vdash G$. By the subformula property and $F \in \Delta^0_1$ this proof is quantifier-free, hence it is a proof in C-$\Sigma^0_0 \vdash F$. By [1] for $n = 0$ and $F \in \Pi^0_1$ we have I-$\Sigma^0_1 \vdash F$. By Gödel's Incompleteness Theorem we conclude I-$\Sigma^0_1 \not\vdash F$, which is the required contradiction. $\Box$

As we said, cut-elimination for quantifiers is ruled out by the previous theorem. If we have all inductive definitions then inductive predicates are exactly the Σ^0_1-predicates (see next section), and quantifier-free formulas are a subset of Δ^0_2-formulas. Thus, cut-elimination restricted to quantifier-free formulas is not trivial, and in general it fails. However, we could define a set of quantifier-free cuts which we called *global cuts* and which may be eliminated.

3 Failure of cut-elimination for quantifier-free proofs

In this section we prove that cut-elimination fails for atomic cuts and variable-discarding inductive definitions.

An inductive definition is variable-discarding if it has some production having some free variable in the assumption not occurring in the conclusion of the production. An example is the inductive predicate p with the production: if $q(x, y)$ then $p(x)$. A variable-discarding inductive definition hydes an existential quantifier inside the inductive predicate: in the previous example, $p(x)$ is equivalent to $\exists y.q(x, y)$.

If we use a variable-discarding inductive definitions then cut-elimination fails even in the simplest cases. We formulate in a variable-discarding way totality the “twice” map $f(x) = 2x$, a very weak arithmetical result. We prove that this statement has no cut-free proof. For comparison, we show that if we add cut to cyclic proofs we may prove the totality of $f(x) = 2x$, and even the totality of the Ackermann function. This latter is a strong arithmetical result with no proof in $I\text{-}\Sigma^0_1$, yet it has a cyclic proof with no propositional connectives nor quantifiers.

3.1 The map $f(x) = 2x$

In this sub-section we define totality for the map in $f(x) = 2x$ using a variable-discarding inductive definition. If we state totality of f in this way, we prove that totality of $f(x)$ has a cyclic proof with local cuts, but no cut-free total proof.

We consider the language $L = \{0, S\}$. We first define the graph $a(x, y)$ of the map $f(x) = 2x$ by: $a(0, 0)$, and if $a(x, y)$ then $a(Sx, SSy)$. The totality of the map $f(x) = 2x$ may be expressed by the predicate $\mathtt{T}(x)$ and the inductive rule: if $a(x, y)$ then $\mathtt{T}(x)$. This inductive definition discards the variable y: y occurs in $a(x, y)$ bu does not occur in $\mathtt{T}(x)$. The interpreation of $\mathtt{T}(x)$ is $\exists y.a(x.y)$: local inductive definition allow to express $\exists$ inside an inductive predicate.

There is a connective-free cyclic proof with cuts on $\mathtt{T}(y)$ of $\mathtt{N}x \vdash \mathtt{T}(x)$ in the language $0, S$, and no cut-free cyclic proof in $\mathtt{CLKID}^\omega$ of the same result.

Lemma 3.1 (The twice map is total) *Let t, u be any terms of the language $0, S$. There is a a connective-free cyclic proof with* local *cuts on* $\mathtt{T}(x)$ *of* $\mathtt{N}t \vdash \mathtt{T}(t)$ *in the same language.*

Proof 1. We first define a finite proof Π_0 of $\mathtt{N}t \vdash \mathtt{T}(t)$ from the open assumption $(1)\mathtt{N}x \vdash \mathtt{T}(x)$ for any $x \notin \mathtt{FV}(t)$. This is not yet the regular proof of $\mathtt{N}t \vdash \mathtt{T}(t)$.

We prove $\mathtt{N}t \vdash \mathtt{T}(t)$ by $\mathtt{N}L$ on $\mathtt{N}t$, from two premises: $t = 0 \vdash \mathtt{T}(t)$ and $\mathtt{N}x, t = Sx, \mathtt{N}x \vdash \mathtt{T}(t)$. For each premise we provide a proof.

(a) We prove $t = 0 \vdash \mathtt{T}(t)$ by $=\!L$ from $\vdash \mathtt{T}(0)$, then by $\mathtt{T}R$-rule from: $\vdash a(0,0)$, which is an aR-axiom.

(b) Proof of $\mathtt{N}x, t = Sx, \mathtt{N}x \vdash \mathtt{T}(t)$. We use $=L$ with premise $\mathtt{N}x \vdash \mathtt{T}(Sx)$. Then we use a cut with $\mathtt{N}x \vdash \mathtt{T}(x)$ and $\mathtt{T}(x) \vdash \mathtt{T}(Sx)$. $\mathtt{N}x \vdash \mathtt{T}(x)$ is an open assumption. We prove $\mathtt{T}(x) \vdash \mathtt{T}(Sx)$ by $\mathtt{T}L$-rule and $x = x', a(x', y') \vdash \mathtt{T}(Sx)$ (for x', y' fresh), then by $=\!L$-rule and $a(x, y') \vdash \mathtt{T}(Sx)$. We use $\mathtt{T}R$-rule with premise $a(x, y') \vdash a(Sx, SSy')$, then aR-rule with premise $a(x, y') \vdash a(x, y')$, and eventually `id`.

2. We define a regular infinite proof Π from Π_0 by repeating cyclically from $\mathtt{N}x \vdash \mathtt{T}(x)$. Next time we use as eigenvariable some $y \not\equiv x$, then x again and so forth. Thus, we may define a regular proof Π by unfolding Π_0.

3. We check that $\mathtt{N}x \vdash \mathtt{T}(x)$ and $\mathtt{T}(x) \vdash \mathtt{T}(Sx)$ is a local cut in Π. Among the ancestors of $T(x)$ (right-hand side) we have an occurrence of $T(Sx)$, hence of $a(Sx, SSy')$. Among the ancestors of $T(x)$ (left-hand side) we have an occurrence of $a(x', y')$, which is the conclusion of a rule with eigenvariable y'.

4. We prove the global trace condition for Π. Take any infinite path π of the proof Π: then this path passes infinitely many times through $\mathtt{N}x \vdash \mathtt{T}(x)$ and $\mathtt{N}y \vdash \mathtt{T}(y)$, progressing each time.

$\square$

We may now prove that there is no cut-free proof of $\mathtt{N}x \vdash \mathtt{T}x$. We prove that if there is some cut-free proof then for some $k \in \mathtt{N}$ and all $x \in \mathtt{N}$ we would have $2x \leq x + k$, that is, $x \leq k$, which is impossible for $x = k + 1$.

Given any cut-free Π of $\Gamma \vdash \Delta$ we define some canonical operations on Π, which we use to extract information from Π. We assume that all formulas in Γ are atomic or quantified equations, and all formulas in Δ are atomic.

For any node $\nu \in \Pi$ we denote with $\Gamma_\nu \vdash \Delta_\nu$ the sequent decorating $\nu \in \Pi$. We define $\mu \leq \nu$ the ordering of Π having the root as bottom element. We call induction on ν the induction on the distance of ν from the root. By induction on $\nu \in \Pi$ we may prove that all formulas in Γ_ν are atomic or quantified equations, and all formulas in Δ_ν are atomic and the rule with conclusion ν in Π is $\mathtt{id}, =L, =R, \mathtt{Weak}, \forall L$ or is pL, pR for some inductive predicate p or is a substitution.

We define the eigenvariables of a rule pL are all the fresh variables of the rule. The eigenvariables of a substitution rule are all free variables in the assumption of the rule. By a renaming we may assume that no eigenvariable of a rule with conclusion ν occurs in any $\mu \leq \nu$.

Assume we fixed a model $\mathcal{M}$ of the language L. Assume we have an assignment $\sigma : \mathcal{M} \to \mathtt{FV}(\Gamma_\nu \vdash \Delta_\nu)$, such that $\mathcal{M}, \sigma \models \Gamma$ in the sense of Tarski. We call a production proof of an inductive predicate in $\mathcal{M}, \sigma$ a proof Θ. made of productions for the predicate and starting from atomic logical predicates true in $\mathcal{M}, \sigma$. We suppose that there is at least one value $\mathtt{dummy} \in \mathtt{range}(\sigma)$ and that for any inductive predicate $p_1(\vec{t_1}), p_k(\vec{t_k}) \in \Gamma$ we have some production proofs $\Theta_1, \ldots, \Theta_k$ for them in $\mathcal{M}, \sigma$.

We define a canonical extension $\sigma_\nu : \bigcup\{\mathtt{FV}(\Gamma_\nu \vdash \Delta_\mu) | \mu \leq \nu\} \to \mathcal{M}$ of σ, for each inductive predicate $p(\vec{t}) \in \Gamma_\nu$ a production proof for $p(\vec{t})$ in $\mathcal{M}, \sigma_\nu$. We define a pruning Π_1 of Π such that for all $\nu \in \Pi_1$ we have $\mathcal{M}, \sigma_\nu \models \Gamma_\nu$.

If $\nu =$ the root of Π then $\sigma_\nu = \sigma$ and production proofs for $p(\vec{t}) \in \Gamma_\nu$ are already given. Assume ν is the conclusion of a rule r whose premise number i is ν_i. If $r = \mathtt{id}$ we are adone. Assume $r = pL$. Then r has main formula some inductive predicate $p(\vec{t}) \in \Gamma_\nu$. We choose in Π_1 the premise $\mu = \nu_i$ corresponding to the production in the conclusion of Θ, and we assign the eigenvariables of r in such a way that the auxiliary formulas in ν_i are equal to the assumption of the production. For each auxiliary formula which is inductive we have an assumption Θ' of Θ proving it (hence the formula is true in $\mathcal{M}, \sigma_\mu$). For each auxiliary formula $R(\vec{u})$ which is logical we have $\mathcal{M}, \sigma \models R(\vec{u})$ by assumption of Θ. All auxiliary formulas which are equations are true in $\mathcal{M}, \sigma_{\nu_i}$ by definition of ν_i. If r is a substitution θ then we set $\sigma_\mu = \sigma_\nu \cup \sigma_\nu\theta$. Assume $r \neq pL$ and r is not a substitution. Then we for all premises μ of ν we set $\mu \in \Pi_1$, and we assign any fresh variable in $\mathtt{FV}(\Gamma_\mu \vdash \Delta_\mu)$ to $\mathtt{dummy} \in \mathtt{range}(\sigma)$.

We defined a pruning $\Pi_1 \subseteq \Pi$. By induction on $\nu \in \Pi_1$ we may prove that $\mathcal{M}, \sigma_\nu \models \Gamma_\nu$. We already checked the case $r = \mathtt{id}, {=}R, pL$. If r is a substitution θ then we set $\sigma_\mu = \sigma_\nu \cup \sigma_\nu\theta$. The thesis follows. If $r = \forall L$ then $\Gamma_\mu = \Gamma_\nu, a[\vec{t}/\vec{x}] = b[\vec{t}/\vec{x}]$ for some $\forall\vec{x}.a = b \in \Gamma_\nu$, and $\sigma_\mu = \sigma_\nu$, hence $\mathcal{M}, \sigma_\mu \models \Gamma_\mu$. If $r = \mathtt{Weak}, pR$ then $\Gamma_\mu \subseteq \Gamma_\nu$ and $\sigma_\mu = \sigma_\nu$, hence $\mathcal{M}, \sigma_\mu \models \Gamma_\mu$. If $r = {=}L$ then each formula in Γ_ν is replaced by a formula with equal arguments and $\sigma_\mu = \sigma_\nu$, hence $\mathcal{M}, \sigma_\mu \models \Gamma_\mu$.

Every infinite path in Π_1 would have an infinite progressing trace, which cannot be because all inductive predicates in the left-hand side are true, therefore no predicate may progress forever. Thus, all paths of Π_1 are finite and Π_1 is finite.

Assume $\nu \in \Pi_1$ and $A \in \Delta_\nu$. We say that A has a production proof in Π if there is a trace τ of A in Π_1 ending in the main formula of $\mathtt{id}$ or ${=}R$, such that all B in τ which are main formulas have all auxiliary formulas with a production proof in Π.

By induction on the height of $\nu \in \Pi_1$ (existing because Π_1 is finite) we may prove that all $A \in \Delta_\nu$ with a production proof in Π_1 are true in $\mathcal{M}, \nu$.

By induction on the height of $\nu \in \Pi_1$ we may prove that some $A \in \Delta_\nu$ has a production proof in Π_1.

We apply these results to any cut-free ∞-proof Π of $\mathtt{N}x \vdash \mathtt{T}x$ and we prove that Π is not regular. If Π were regular, we would have some maximum k such that $S^k(y)$ or $S^k(0)$ occurs in Π. We choose $\mathcal{M} = \mathtt{N}$, $\sigma(x) = k+1$ and $\Theta =$ the unique production proof of $\mathtt{N}n$. By induction on ν we prove that $\mathtt{range}(\sigma_\nu) \subseteq [0, k+1]$. We deduce that there is a production proof of $\mathtt{T}x$. There is no $\mathtt{T}t$ occurring in any Γ_ν, therefore some ancestor $\mathtt{T}t \in \sigma_\nu$ of $\mathtt{T}x$ in Π_1 is proved from some $a(t,u)$. By induction on ν we may prove that $\sigma_n u(t) = \sigma(x) = k+1$. By definition of k we have $u \equiv S^h(y)$ or $u \equiv S^h(0)$, hence $\sigma(u) \leq \sigma_\nu(y) + h \leq (k+1)+k < 2(k+1)$. Instead, from $\mathcal{M}, \sigma_\nu \models a(t,u)$ we deduce $\sigma_\nu(t) = 2\sigma_\nu(u) = 2(k+1)$. This is a contradiction, therefore Π is not regular.

This rules out the possibility of proving $2n$ total. The same argument holds for any other map $f(\vec{n})$ which is definitively $\geq 2\max(\vec{n})$, with the following proviso. We have to define the graph a of f inductively, then the totality $\mathtt{T}(\vec{x})$ of f in x by: $a(\vec{x}, y)$ implies $\mathtt{T}(\vec{x})$. In the next subsection we provide an example for f: the Ackermann function.

3.2 The Ackermann function

The Ackermann–Peter version of the Ackermann function is a map $\mathtt{A} : \mathtt{N}^2 \to \mathtt{N}$ defined by the following rewriting rules: for all $x, y \in \mathtt{N}$, $\mathtt{A}(0,y) \rightsquigarrow Sy$ an d $\mathtt{A}(Sx, 0) \rightsquigarrow \mathtt{A}(x, 1)$ and $\mathtt{A}(Sx, Sy) \rightsquigarrow \mathtt{A}(x, \mathtt{A}(x{+}1, y))$. We write $\rightsquigarrow_z$ for reduction z times. By Π^0_2-induction on $x \in \mathtt{N}$ we may prove totality of $\mathtt{A} : \mathtt{N}^2 \to \mathtt{N}$: we prove $\forall y.(y \in \mathtt{N}) \to \exists z, t.(z, t \in \mathtt{N}) \wedge (\mathtt{A}(x,y) \rightsquigarrow_z t)$.

We cannot insert an inductive definition for the map $\mathtt{A}$ in $\mathtt{LKID}$, but we define the statement $\mathtt{A}(x,y) = z$ as an inductive predicate $\mathtt{A}(x,y,z)$. We define $\mathtt{T}(x,y)$ as the correctness statement $\exists z.\mathtt{A}(x,y) = z$.

The $\mathtt{A}R$-rules for the inductive definition of $\mathtt{A}$ in $\mathtt{LKID}$ are: $\mathtt{A}(0, y, Sy)$ and from $\mathtt{A}(x, 1, z)$ deduce $\mathtt{A}(Sx, 0, z)$ and from $\mathtt{A}(Sx, y, z), \mathtt{A}(x, z, t)$ deduce $\mathtt{A}(Sx, Sy, t)$. The only $\mathtt{T}R$-rule is: from $\mathtt{A}(x,y,z)$ deduce $\mathtt{T}(x,y)$. The $\mathtt{A}L$, $\mathtt{T}L$-rules are defined in $\mathtt{LKID}$ as a consequence.

In $\mathtt{CLKID}^\omega$ we may bypass Π^0_2-induction and we provide a connective-free (hence quantifier-free) proof of the totality of $\mathtt{A}$. We prove first that all $\mathtt{A}(t)$ are a *partial* map $: \mathtt{N} \to \mathtt{N}$: that is, if $\mathtt{A}(t, u, v)$ and $\mathtt{N}u$ then $\mathtt{N}v$.

Lemma 3.2 (Ackermann is a partial function) *Let t, u be any terms of the language $0, S$. There is a connective-free cyclic proof with cuts of* $\mathtt{N}u, \mathtt{A}(t,u,v) \vdash$

$\mathtt{N}v$ *in the same language.*

Proof Let x, y, z, w be pairwise distinct variables $\notin \mathtt{FV}(t, u, v)$. We define a connective-free cyclic proof Π_0 of $\mathtt{N}u, \mathtt{A}(t, u, v) \vdash \mathtt{N}v$ using $\mathtt{A}L$ in the root, with open assumptions: (1)$\mathtt{N}1, \mathtt{A}(x, 1, z) \vdash \mathtt{N}z$ and (2)$\mathtt{N}y, \mathtt{A}(Sx, y, z) \vdash \mathtt{N}z$ and (3)$\mathtt{N}z, \mathtt{A}(x, z, w) \vdash \mathtt{N}w$. We define the 3 premises of the rule $\mathtt{A}L$.

1. *Premise* 1 is $\mathtt{N}u, t = 0, u = y, v = Sy \vdash \mathtt{N}v$. It is proved by $=L$ and $\mathtt{N}y \vdash \mathtt{N}Sy$, then by $\mathtt{N}R$ and $\mathtt{N}y \vdash \mathtt{N}y$, eventually by $\mathtt{id}$.

2. *Premise* 2 is $\mathtt{N}u, t = x, u = 1, v = z, \mathtt{A}(x, 1, z) \vdash \mathtt{N}v$. It is proved by $=L$ and $\mathtt{N}1, \mathtt{A}(x, 1, z) \vdash \mathtt{N}z$. This is *open assumption* 1.

3. *Premise* 3 is $\mathtt{N}u, t = Sx, u = y, v = w, \mathtt{A}(Sx, y, z), \mathtt{A}(x, z, w) \vdash \mathtt{N}v$. It is proved by $=L$ and $\mathtt{N}y, \mathtt{A}(Sx, y, z), \mathtt{A}(x, z, w) \vdash \mathtt{N}w$. This latter is proved by a cut between $\mathtt{N}y, \mathtt{A}(Sx, y, z) \vdash \mathtt{N}z$ and $\mathtt{N}z, \mathtt{A}(x, z, w) \vdash \mathtt{N}w$. These are *open assumptions* 2 *and* 3

We define a regular infinitary proof tree Π out of Π_0. Π_0 has 3 open assumptions: $\mathtt{N}1, \mathtt{A}(x, 1, z) \vdash \mathtt{N}z$ and $\mathtt{N}y, \mathtt{A}(Sx, y, z) \vdash \mathtt{N}z$ and $\mathtt{N}z, \mathtt{A}(x, z, w) \vdash \mathtt{N}w$, for $x, y, z, w \notin \mathtt{FV}(t, u, v)$. We unfold a second time and we provide 3 open assumptions $\mathtt{N}1, \mathtt{A}(x', 1, z') \vdash \mathtt{N}z$ and $\mathtt{N}y', \mathtt{A}(Sx', y', z') \vdash \mathtt{N}z'$ and $\mathtt{N}z', \mathtt{A}(x', z', w') \vdash \mathtt{N}w'$, for some $x', y', z', w' \notin \mathtt{FV}(t, u, v)$. We unfold a third time and we provide 3 open assumptions: $\mathtt{N}1, \mathtt{A}(x, 1, z) \vdash \mathtt{N}z$ and $\mathtt{N}y, \mathtt{A}(Sx, y, z) \vdash \mathtt{N}z$ and $\mathtt{N}z, \mathtt{A}(x, z, w) \vdash \mathtt{N}w$, for $x, y, z, w \notin \mathtt{FV}(t, u, v, x', y', z')$. We continue cyclically and we obtain a regular tree Π.

We prove the global trace condition for Π. In Π whenever we prove $\mathtt{N}u, \mathtt{A}(t, u, v) \vdash \mathtt{N}v$ we derive it from 3 sequents of the form $\mathtt{N}u', \mathtt{A}(t', u', v') \vdash \mathtt{N}v'$, and in each case there is a progressing trace from $\mathtt{A}(t, u, v)$ to $\mathtt{A}(t', u', v')$. Every infinite path of Π has to pass cyclically from $\mathtt{N}u, \mathtt{A}(t, u, v) \vdash \mathtt{N}v$ to $\mathtt{N}u', \mathtt{A}(t', u', v') \vdash \mathtt{N}v'$, therefore it includes an infinitely progressing trace from the unique atom $\mathtt{A}(t, u, v)$ in the root. $\square$

From the fact that $\mathtt{A}$ is the graph of a partial map on $\mathtt{N}$ we derive that $\mathtt{A}$ is the graph of a total map on $\mathtt{N}$, using cuts but no logical connective.

Lemma 3.3 (Ackermann is a total function) *Let* t, u *be any terms of the language* $0, S$. *There is a a connective-free cyclic proof with cuts of* $\mathtt{N}t, \mathtt{N}u \vdash \mathtt{T}(t, u)$ *in the same language.*

Proof We define a finite proof Π_0 of $\mathtt{N}t, \mathtt{N}u \vdash \mathtt{T}(t, u)$ from 3 open assumptions: (1)$\mathtt{N}x, \mathtt{N}1 \vdash \mathtt{T}(x, 1)$ and (2)$\mathtt{N}t, \mathtt{N}y \vdash \mathtt{T}(t, y)$ and (3)$\mathtt{N}x, \mathtt{N}z \vdash \mathtt{T}(x, z)$ for any $x, y, z \notin \mathtt{FV}(t, u)$.

We prove $\mathtt{N}t, \mathtt{N}u \vdash \mathtt{T}(t, u)$ by $\mathtt{N}L$ on $\mathtt{N}u$, from two premises: $\mathtt{N}t, u = 0 \vdash \mathtt{T}(t, u)$ and $\mathtt{N}t, u = Sy, \mathtt{N}y \vdash \mathtt{T}(t, u)$. For each premise we provide a proof.

1. We prove $\mathtt{N}t, u = 0 \vdash \mathtt{T}(t, u)$ by $=L$ from $\mathtt{N}t \vdash \mathtt{T}(t, 0)$, then by $\mathtt{N}L$-rule from: $t = 0 \vdash \mathtt{T}(t, 0)$ and $t = Sx, \mathtt{N}x \vdash \mathtt{T}(t, 0)$.

   (a) Proof of $t = 0 \vdash \mathtt{T}(t, 0)$. We use $=L$ and $\vdash \mathtt{T}(0, 0)$, then $\mathtt{T}R$-rule and $\mathtt{A}(0, 0, 1)$, which is an $\mathtt{A}R$-axiom.

   (b) We prove $t = Sx, \mathtt{N}x \vdash \mathtt{T}(t, 0)$ by $=L$-rule from $\mathtt{N}x \vdash \mathtt{T}(Sx, 0)$, and this latter by a cut between $\mathtt{N}x \vdash \mathtt{T}(x, 1)$ and $\mathtt{T}(x, 1) \vdash \mathtt{T}(Sx, 0)$. $\mathtt{N}x \vdash \mathtt{T}(x, 1)$ is proved by a cut between $\mathtt{N}1$ and $\mathtt{N}x, \mathtt{N}1 \vdash \mathtt{T}(x, 1)$: this is *(o.a.1)*. $\mathtt{T}(x, 1) \vdash \mathtt{T}(Sx, 0)$ is proved by $\mathtt{T}L$-rule from $x' = x, y' = 1, \mathtt{A}(x', y', z) \vdash \mathtt{T}(Sx, 0)$, then by $=L$ from $\mathtt{A}(x, 1, z) \vdash \mathtt{T}(Sx, 0)$, by $\mathtt{T}R$-rule from $\mathtt{A}(x, 1, z) \vdash \mathtt{A}(Sx, 0, z)$, by $\mathtt{A}R$-rule from $\mathtt{A}(x, 1, z) \vdash \mathtt{A}(x, 1, z)$, eventually by $\mathtt{id}$.

2. Proof of $\mathtt{N}t, u = Sy, \mathtt{N}y \vdash \mathtt{T}(t, u)$. We use $=L$ and $\mathtt{N}t, \mathtt{N}y \vdash \mathtt{T}(t, Sy)$. Then we use a cut with $\mathtt{N}t, \mathtt{N}y \vdash \mathtt{T}(t, y)$ and $\mathtt{N}t, \mathtt{N}y, \mathtt{T}(t, y) \vdash \mathtt{T}(t, Sy)$. $\mathtt{N}t, \mathtt{N}y \vdash \mathtt{T}(t, y)$ is *(o.a.2)*. We prove $\mathtt{N}t, \mathtt{N}y, \mathtt{T}(t, y) \vdash \mathtt{T}(t, Sy)$ by $\mathtt{N}L$-rule and $t = 0, \mathtt{N}y, \mathtt{T}(t, y) \vdash \mathtt{T}(t, Sy)$ and $t = Sx, \mathtt{N}x, \mathtt{N}y, \mathtt{T}(t, y) \vdash \mathtt{T}(t, Sy)$.

   (a) We prove $t = 0, \mathtt{N}y, \mathtt{T}(t, y) \vdash \mathtt{T}(t, Sy)$ by $=L$ and WL from $\vdash \mathtt{T}(0, Sy)$. By $\mathtt{T}R$-rule it is enough to prove $\vdash \mathtt{A}(0, Sy, SSy)$, which is some $\mathtt{A}R$-axiom.

   (b) We prove $t = Sx, \mathtt{N}x, \mathtt{N}y, \mathtt{T}(t, y) \vdash \mathtt{T}(t, Sy)$, by $=L$ and WL from $\mathtt{N}x, \mathtt{T}(Sx, y) \vdash \mathtt{T}(Sx, Sy)$. By $\mathtt{T}L$-rule we have to prove $\mathtt{N}x, Sx = x', y = y', \mathtt{A}(x', y', z) \vdash \mathtt{T}(Sx, Sy)$, by $=L$ we have to prove $\mathtt{N}x, \mathtt{A}(Sx, y, z) \vdash \mathtt{T}(Sx, Sy)$. We use a cut between $\mathtt{N}x, \mathtt{A}(Sx, y, z) \vdash \mathtt{N}z$ (provable by Lemma 3.2) and $\mathtt{N}x, \mathtt{N}z, \mathtt{A}(Sx, y, z) \vdash \mathtt{T}(Sx, Sy)$, then a cut between $\mathtt{N}x, \mathtt{N}z \vdash \mathtt{T}(x, z)$ and $\mathtt{A}(Sx, y, z), \mathtt{T}(x, z) \vdash \mathtt{T}(Sx, Sy)$. $\mathtt{N}x, \mathtt{N}z \vdash \mathtt{T}(x, z)$ is *(o.a.3)*. We prove $\mathtt{A}(Sx, y, z), \mathtt{T}(x, z) \vdash \mathtt{T}(Sx, Sy)$ by $\mathtt{T}L$-rule and $\mathtt{A}(Sx, y, z), x = x', z = z', \mathtt{A}(x', z', w) \vdash \mathtt{T}(Sx, Sy)$. By $=L$ we have to prove $\mathtt{A}(Sx, y, z), \mathtt{A}(x, z, w) \vdash \mathtt{T}(Sx, Sy)$. By $\mathtt{T}R$ it is enough to prove that $\mathtt{A}(Sx, y, z), \mathtt{A}(x, z, w) \vdash \mathtt{A}(Sx, Sy, w)$, by $\mathtt{A}R$ that $\mathtt{A}(Sx, y, z), \mathtt{A}(x, z, w) \vdash \mathtt{A}(Sx, y, z)$ and that $\mathtt{A}(Sx, y, z), \mathtt{A}(x, z, w) \vdash \mathtt{A}(x, z, w)$. These sequents are both $\mathtt{id}$-rules.

We define a regular infinite proof Π from Π_0. In Π_0 proved $\mathtt{N}t, \mathtt{N}u \vdash \mathtt{T}(t, u)$ from 3 open assumptions: $\mathtt{N}x, \mathtt{N}1 \vdash \mathtt{T}(x, 1)$ and $\mathtt{N}t, \mathtt{N}y \vdash \mathtt{T}(t, y)$ and $\mathtt{N}x, \mathtt{N}z \vdash \mathtt{T}(x, z)$ for any $x, y, z \notin \mathtt{FV}(t, u)$. We may prove these latter from $\mathtt{N}x', \mathtt{N}1 \vdash \mathtt{T}(x, 1)$ and $\mathtt{N}t, \mathtt{N}y' \vdash \mathtt{T}(t, y')$ and $\mathtt{N}x', \mathtt{N}z' \vdash \mathtt{T}(x', z')$ for any $x', y', z' \notin \mathtt{FV}(t, u, x, y, z)$. We may prove these latter from $\mathtt{N}x, \mathtt{N}1 \vdash \mathtt{T}(x, 1)$ and $\mathtt{N}t, \mathtt{N}y \vdash \mathtt{T}(t, y)$ and $\mathtt{N}x, \mathtt{N}z \vdash \mathtt{T}(x, z)$ because $x, y, z \notin \mathtt{FV}(t, u, x', y', z')$. Thus, we may define a regular proof Π by unfolding Π_0.

We prove the global trace condition for Π. Each $\mathtt{N}t, \mathtt{N}u \vdash \mathtt{T}(t, u)$ is proved cyclically by: (1)$\mathtt{N}x, \mathtt{N}1 \vdash \mathtt{T}(x, 1)$ or (2)$\mathtt{N}t, \mathtt{N}y \vdash \mathtt{T}(t, y)$ or (3)$\mathtt{N}x, \mathtt{N}z \vdash \mathtt{T}(x, z)$. In cases (1) and (3) is a progressing trace from $\mathtt{N}t$ to $\mathtt{N}x$. In case (2) there is a trace from $\mathtt{N}t$ to $\mathtt{N}t$ and a progressing trace from $\mathtt{N}u$ to $\mathtt{N}y$. Take any infinite path π of the proof Π, in order to prove that there is some infinitely progressing trace. π passes infinitely many times through (1) or (2) or (3). Assume π passes infinitely many times through (1) or (3) (and any number of times through (2)). Then there is an infinite trace τ from $\mathtt{N}t$ in the root, τ is infinitely progressing (whenever τ passes through (1) or (3)) and we are done. Assume π passes finitely many times through (1) or (3). Then from some node ξ on, π passes cyclically through (2), progressing from $\mathtt{N}u$ to $\mathtt{N}x$. From ξ on, the trace υ from the occurrence of $\mathtt{N}u$ in ξ progresses in *every* step. Also in this case there is some infinitely progressing trace in π. $\Box$

We may now prove that there is some connective-free cyclic proof whose cuts cannot be eliminated.

Theorem 3.4 *There a connective-free cyclic proof of* $\mathtt{N}x, \mathtt{N}y \vdash \mathtt{T}(x, y)$ *with cuts in the language* $0, S$. *There is no cut-free proof cyclic proof of* $\mathtt{N}x, \mathtt{N}y \vdash \mathtt{T}(x, y)$ *in the same language.*

Proof As for the map $f(x) = 2x$. $\Box$

4 Upper and lower bound for the fragment of cyclic proofs with cut-elimination

In §3 we proved that normalization fails for atomic formulas if we allow variable discarding productions in inductive definition. In this section we consider a single inductive definition, N (the simplest relevant example), discarding no variables. We prove that if we consider only cuts over formulas $\mathtt{N}t$ then normalization succeeds for totality of polynomials and fails for totality of exponential.

Fix any production for an inductive definition in LKID. We recall that a production discards a variable if the variable occurs in the assumption and not in the conclusion. The definition of N discards no variables. The definition of the graph $a(x, y)$ of the map $f(x) = 2x$ discards no variables. The inductive definition $\mathtt{T}(x)$ of totality of f is: "if $a(x, y)$ then $\mathtt{T}(x)$" discards the variable y. Assume A is quantifier-free. A cut occurrence between twos formulas A is local if some ancestor of one A is the main formula of a pL rule with eigenvariable x, and some ancestors of the other A has the same x free.

In this section we provide some cuts between two occurrences of $\mathtt{N}(t)$ with some $x \in \mathtt{FV}(t)$ which is an eigenvariable for the other occurrence. We show that some of these cuts cannot be eliminated.

The cyclic proofs we consider are again totality proofs for maps, but instead of using a local inductive definition $T(x)$ of totality as in §3 we express totality of f in the form: $E_f, \mathtt{N}x \vdash \mathtt{N}f(x)$, with E_f the equational axioms of f. We prove that all polynomials with coefficients in $\mathtt{N}$ have cut-free proofs of totality, while the map 2^x has some totality proof whose cuts are all of the form $\mathtt{N}(2^y)$, but no totality proof which is cut-free. Our first steps are proving cut-free that sum and product are total.

Let $E_+ = \forall x.x + 0 = x, \forall x, y.x + Sy = S(x + y)$. We claim that there is a cut-free proof of the totality of $+$.

Lemma 4.1 *Assume $E_+ \subseteq \Gamma$ and t is any term.*

1. *There is a cut-free cyclic proof of $\Gamma, \mathtt{N}u \vdash \mathtt{N}(t + u)$ with free assumption $\Gamma \vdash \mathtt{N}t$.*

2. *There is a cut-free cyclic proof of $E_+, \mathtt{N}t, \mathtt{N}u \vdash \mathtt{N}(t + u)$.*

3. *There is a cut-free cyclic proof of $E_+, \mathtt{N}t \vdash \mathtt{N}(t + t)$.*

Proof 1. We prove $\Gamma, \mathtt{N}u \vdash \mathtt{N}(t+u)$ by $\mathtt{N}L$-rule for $\mathtt{N}u$. We have to prove: *(1)* $\Gamma, u = 0 \vdash \mathtt{N}(t + u)$ and *(2)* $\Gamma, \mathtt{N}z, u = Sz \vdash \mathtt{N}(t + u)$ for $z \notin \mathtt{FV}(\Gamma, t, u)$.

(a) Proof of $\Gamma, u = 0 \vdash \mathtt{N}(t + u)$. We use $=L$ and $\Gamma \vdash \mathtt{N}(t + 0)$, then $\forall L$ for $\forall x.(x + 0) = x \in \Gamma$ and $\Gamma, (t + 0) = t \vdash \mathtt{N}(t + 0)$, then $=L$ and $\Gamma \vdash \mathtt{N}t$. This latter is a free assumption.

(b) Proof of $\Gamma, \mathtt{N}z, u = Sz \vdash \mathtt{N}(t+u)$. We use $=L$ and $\Gamma, \mathtt{N}z \vdash \mathtt{N}(t+Sz)$, then $\forall L$ for $\forall x.(x + Sy) = S(x + y) \in \Gamma$ and $\Gamma, (t + Sz) = S(t + z), \mathtt{N}z \vdash \mathtt{N}(t + Sz)$, then $=L$ and $\Gamma, \mathtt{N}z \vdash \mathtt{N}S(t + z)$, eventually $\mathtt{N}R$ and $\Gamma, \mathtt{N}z \vdash \mathtt{N}(t + z)$. Here we repeat cyclically: next time we choose $z' \notin \mathtt{FV}(\Gamma, t, u, z)$ as eigenvariable, next time we choose z again. In this way we have a regular proof.

In order to have a cyclic proof we have to check the global trace condition. The trace of $\mathtt{N}u$ progresses whenever we pass a $\mathtt{N}L$-rule, otherwise it is stationary. Every infinite path has infinitely many $\mathtt{N}L$-rule, therefore the trace of $\mathtt{N}u$ is infinitely progressing.

2. By point 1 above there is a cut-free cyclic proof of $E_+, \mathtt{N}t, \mathtt{N}u \vdash \mathtt{N}(t+u)$ with free assumption $E_+, \mathtt{N}t, \mathtt{N}u \vdash \mathtt{N}t$. We prove the free assumption with $\mathtt{id}$. Regularity is preserved because we add no sub-proofs, and every infinite path in the new proof is in the old proof, therefore is includes some infinitely progressing trace. Thus, we defined a cut-free cyclic proof (without assumptions).

3. By point 2 above if we choose $t \equiv u$.
□

Let $E_* = E_+, \forall x.x * 0 = 0, \forall x, y.x * Sy = x * y + x$. We claim that there is a cut-free proof of the totality of $*$.

Lemma 4.2 *There is a cut-free proof of* $E_*, \mathtt{N}x, \mathtt{N}y \vdash \mathtt{N}(x * y)$.

Proof We prove $E_*, \mathtt{N}x, \mathtt{N}y \vdash \mathtt{N}(x * y)$ by $\mathtt{N}L$-rule for $\mathtt{N}*$. We have to prove *(1)* $E_*, \mathtt{N}x, y = 0 \vdash \mathtt{N}(x * y)$ and *(2)* $E_*, \mathtt{N}x, \mathtt{N}z, y = Sz \vdash \mathtt{N}(x * y)$.

1. Proof of $E_*, \mathtt{N}x, y = 0 \vdash \mathtt{N}(x + y)$. We use $=L$ and $E_*, \mathtt{N}x \vdash \mathtt{N}(x * 0)$, then $\forall L$ and $E_*, (x * 0) = 0, \mathtt{N}x \vdash \mathtt{N}(x * 0)$, then $=L$ and $E_*, \mathtt{N}x \vdash \mathtt{N}0$, eventually $\mathtt{N}R$.

2. Proof of $E_*, \mathtt{N}x, \mathtt{N}z, y = Sz \vdash \mathtt{N}(x * y)$. We use $=L$ and $E_*, \mathtt{N}x, \mathtt{N}z \vdash \mathtt{N}(x * Sz)$, then $\forall L$ and $E_*, (x * Sz) = x * z + x, \mathtt{N}x, \mathtt{N}z \vdash \mathtt{N}(x * Sz)$, then $=L$ and $E_*, \mathtt{N}x, \mathtt{N}z \vdash \mathtt{N}x * z + x$. By Lemma 4.1 there is a cut-free cyclic proof Π of $E_*, \mathtt{N}x, \mathtt{N}z \vdash \mathtt{N}x{*}z{+}x$ with free assumption $E_*, \mathtt{N}x, \mathtt{N}z \vdash \mathtt{N}x{*}z$. Here we repeat cyclically, next time we choose y as eigenvariable, in order to obtain a regular proof.

We check the global trace condition. Every infinite path π either passes infinitely many times through a $\mathtt{N}L$-rule inferring $\mathtt{N}y$, with the trace of $\mathtt{N}y$ progressing each time, or from some node on is inside some inserted proof Π of $E_*, \mathtt{N}x, \mathtt{N}z \vdash \mathtt{N}x * z + x$. In the first case the global trace condition for π is satisfied. In the second case, the suffix of π which is in Π includes from some node on some infinite progressing trace, the same holds for π and the global trace condition for π is satisfied. □

If global cuts are removable, then from t total and u total we deduce that $t[u/x]$ is total. If $x \notin \mathtt{FV}(t)$ this is immediate. Assume $x \in \mathtt{FV}(t)$. Let E_t be the union of the lists of axioms for function symbols in t, and E_u for function symbols in u. From $x \in \mathtt{FV}(t)$ we deduce that the function symbols in $[t[u/x]$ are those in t or in u, hence $E_t, E_u = E_{t[u/x]}$. Let $\vec{x} = \mathtt{FV}(t, u)$. From $E_t, \mathtt{N}\vec{x}, \mathtt{N}x \vdash \mathtt{N}t$ we deduce $\mathtt{N}\vec{x}, \mathtt{N}u \vdash \mathtt{N}t[u/x]$ by substitution. From $E_u, \mathtt{N}\vec{x} \vdash \mathtt{N}u$

and cut we conclude $E_t, E_u, \mathtt{N}\vec{x} \vdash \mathtt{N}t[u/x]$, that is, $E_{t[u/x]}, \mathtt{N}\vec{x} \vdash \mathtt{N}t[u/x]$. The cut is global because it is the unique cut in the proof, hence by renaming eigenvariables we may may prevent an eigenvariable in one side of the proof to occur in the other side of the proof. If we may remove global cuts, then we may obtain a cut-free proof of $E_{t[u/x]}, \mathtt{N}\vec{x} \vdash \mathtt{N}t[u/x]$.

By repeating this reasoning we obtain that all polynomials, being compositions of 0, S, $x + y$ and $x * y$ are provably total with a cut-free proof, provided global cuts are removable.

With the same reasoning, if global cuts are removable, and there is a cut-free proof of totality for 2^x, then there is a cut-free proof of totality for all poly-exponential maps, obtained composing 0, S, $x+y$, $x*y$ and 2^x. We will prove that this cannot be: at least one exponential map has no cut-free proof of totality.

Lemma 4.3 (Failure of cut-elimination for some exponential map) *There is some exponential map $f(x) = 2^{(x+3)^2} + x$ with no cut-free totality proof. If global cuts may be eliminated, then the same holds for 2^x.*

Proof Assume there is some cut-free proof Π of totality of $f(x)$. Let us consider the set of traces from some inductive predicate in the left-hand side of a node a to some inductive predicate in the left-hand side of a node b in the graph representation of the cyclic proof. Assume there is a path from a to b. Then set of traces i from a to b and the set of traces j from b to c may be composed by composing each trace with every compatible trace. The result ji is the set of traces from a to c. We add an empty trace 0 and we set $ji = 0$ if the last node of i is different from the first node of j. Assume π is any infinite path in the infinite unfolding of the cyclic proof. Then the nodes of π define a complete graph whose edges are colored on M, with coloring compatible with composition, and with all colors $\neq 0$.

Any homogeneous subset of π with at least 3 elements a, b, c has all edges colored with some idempotent $i \in M$, $i \not0$. Indeed, if i colors (a, b) and (b, c) and (a, c), then by compatibility with composition (a, c) has also color ii. Thus, $ii = i$.

By Ramsey Theorem there is some infinite homogeneous subset, a set with all edges in the same color i, with $i \neq 0$, i idempotent as we just proved. If it were $a \neq b$ then $ii = 0$, hence $i = 0$, contradiction. Thus, i connects a with itself. There is an infinite subsequence $a, a, a, \ldots$ of nodes of π, with each connection from one a to another one with color i.

By the global trace condition there is some infinitely progressing trace τ in π. τ passes infinitely many times through a, and a has finitely many inductive predicate in the left-hand side. Thus, τ passes infinitely many times through the same inductive formula $p(\vec{t})$. Take the first occurrence of $p(\vec{t})$ in τ, the first progress point of τ after it, then the first occurrence of $p(\vec{t})$ in τ after the progress point. We deduce that there are two nodes a such that $p(\vec{t})$ in the first a progresses in τ to $p(\vec{t})$ in the second a. The color between the two a's is i, therefore $p(\vec{t})$ progress to $p(\vec{t})$ in the color i. Thus, in any homogeneous set with $h+1$ elements the inductive predicate $p(\vec{t})$ progresses at least h times.

In Π, the formula $p(\vec{t})$ is some ancestor of the formula $\mathtt{N}x$ in the conclusion of Π, hence some ancestor of $\mathtt{N}x$ progresses at least h times in any homogeneous set with $h+1$ elements.

Let $R(m,\ldots,m)$ be the diagonal Ramsey number for m: is the minimum size of a complete graph with k colors having some homogeneous sets of cardinality m. A folk-lore result says that $R(m,\ldots,m) \leq k^{km}$. We claim that every poly-exponential map $f(n)$ with a cut-free proof of totality has upper bound $r(n) = R(n+3,\ldots,n+3)$ for all $n \in \mathtt{N}$.

In order to prove it, fix any assignment $\sigma(x) = n$ for x and we extend it to all sequents in Π. We call the canonical extension of σ the extension assigning $\max(0, p-1)$ to the eigenvariable of the case rule with main formula $\mathtt{N}u$ and $\sigma(u) = p$. There is exactly one path π of Π with all formulas in the left-hand side true with respect to the canonical extension of σ. π has length $< r(n)$, because a path with length $r(n)$ would include an homogeneous set of $n+3$ elements, hence $n+2$ progresses of $\mathtt{N}x$, and this is impossible because $\sigma(x) = n$. π includes $\geq f(n) - n$ rules $\mathtt{N}R$, then either the rule $\mathtt{id}$ or the rule $\mathtt{N}R$ with main formula $\mathtt{N}0$. $r(n)$ cannot be a bound for $f(n) - n$ for all poly-exponential maps f. For instance, we have $f(z) = 2^{(z+3)^2} + z > k^{k(z+3)} + z \geq r(z) + z \geq f(z) - z + z = f(z)$ for all $z > k\log_2(k) - 3$, because in this case we have $2^{(z+3)^2} > 2^{k\log_2(k)(z+3)} = (2^{\log_2(k)})^{k(z+3)} = k^{k(z+3)} = r(z)$.
$\square$

We prove that if global cuts are eliminable, then $E_{2^x}, \mathtt{N}x \vdash \mathtt{N}2^x$ has no cut-free cyclic proof. Instead, $E_{2^x}, \mathtt{N}x \vdash \mathtt{N}2^x$ has a cyclic proof of totality whose cuts are all local cuts. All cuts of this proof are local.

Lemma 4.4 (Totality proof with cuts for 2^x) *There is proof of $E_{2^x}, \mathtt{N}x \vdash \mathtt{N}2^x$ with all cuts local.*

Proof We already checked that there is no cut-free proof of $E_{2^x}, \mathtt{N}x \vdash \mathtt{N}2^x$: we provide a proof with cuts on $\mathtt{N}2^y$. We use $\mathtt{N}L$ with main formula $\mathtt{N}x$ and premises $E_{2^x}, x = 0 \vdash \mathtt{N}2^x$ and $E_{2^x}, \mathtt{N}y, x = Sy \vdash \mathtt{N}2^x$ for $y \not\equiv x$.

1. Proof of $E_{2^x}, x = 0 \vdash \mathtt{N}2^x$. We use $=\!L$ and $E_{2^x} \vdash \mathtt{N}2^0$. Then we use $=\!L$ on $2^0 = 1 \in E_{2^x}$ with premise $E_{2^x} \vdash \mathtt{N}1$, where $1 \equiv S0$. We prove $E_{2^x} \vdash \mathtt{N}S0$ from $\mathtt{N}R$ for S and $E_{2^x} \vdash \mathtt{N}0$, then by $\mathtt{N}R$ for 0.

2. Proof of $E_{2^x}, \mathtt{N}y, x = Sy \vdash \mathtt{N}2^x$. We use $=L$ and $E_{2^x}, \mathtt{N}y \vdash \mathtt{N}2^{Sy}$. Then we use $\forall L$ on $\forall x.2^{Sx} = 2^x + 2^x$ and $E_{2^x}, 2^{Sy} = 2^y + 2^y, \mathtt{N}y \vdash \mathtt{N}2^{Sy}$, then $=L$ and $E_{2^x}, \mathtt{N}y \vdash \mathtt{N}2^y + 2^y$. We derive this latter by a cut between $E_{2^x}, \mathtt{N}y \vdash \mathtt{N}2^y$ and $E_{2^x}, \mathtt{N}2^y \vdash \mathtt{N}2^y + 2^y$. In the first premise we repeat cyclically the proof, in the second one we apply Lemma 4.1. The second time we choose x as eigenvariable, in order to have a regular proof.

We check the global trace condition. Any infinite path in the proof either passes infinitely many times through $E_{2^x}, \mathtt{N}x \vdash \mathtt{N}2^x$ and $E_{2^x}, \mathtt{N}y \vdash \mathtt{N}2^y$, with the trace of $\mathtt{N}x$ progressing each time, or from some node on is in some proof of $E_{2^x}, \mathtt{N}2^y \vdash \mathtt{N}2^y + 2^y$. In this case there is a trace infinitely progressing from some point on.

We check that the cut on $\mathtt{N}2^y$ is local. The first premise of the cut on $\mathtt{N}2^y$ has ancestor $\mathtt{N}2^x$, therefore has ancestor $\mathtt{N}2^y + 2^y$. The ancestors of $\mathtt{N}2^y + 2^y$ include the eigenvariable z of the case rule of $E_{2^x}, \mathtt{N}2^y \vdash \mathtt{N}2^y + 2^y$. The second premise of the cut on $\mathtt{N}2^y$ is the main formula inferred by the case rule of $E_{2^x}, \mathtt{N}2^y \vdash \mathtt{N}2^y + 2^y$, therefore has ancestor $\mathtt{N}z$ with z eigenvariable of the case rule. Thus, the cut is local.

$\square$

5 A last example: the transitive closure

We prove that the equivalence of right-to-left and left-to-right definitions of the transitive closure has a cyclic proof but no cut-free cyclic proof.

A word before we start: this example is rather surprising. The equivalence just unfolds the definition of right-to-left transitive closure, generating a list, then reverses the list in square time, and eventually proves left-to-right transitive closure. Our interpretation of the lack of cut-elimination is: this algorithm requires non-constant space, having to remember the list unfolding the right-to-left transitive closure. For this reason, the proof requires left-hand sides of unbounded size and it is not regular. Apparently, cut-elimination is only possible when the proof uses a polynomial-time algorithm requiring constant space.

Equivalence of two transitive definitions is a simplified version of an example of a proof from Separation Logic. We consider a first order language $L = \{R\}$, with no constants and no function symbols, only one binary predicate $R(x, y)$ and variables. We extend L with two equivalent definitions of the transitive closure of R: $\mathtt{B}(x, y)$ and $\mathtt{F}(x, y)$.

1. $\mathtt{B}(x, y)$ means: "we recursively define an R-chain from x to y by listing

R-related elements right-to-left, from y to x". In this definition we first list $R(z', y)$, then $R(z'', z')$, ..., until we reach some $R(x, z)$.

2. $\mathtt{F}(x, y)$ means: "we recursively define an R-chain from x to y by listing R-related elements left-to-right, from x to y". In this definition we first list $R(x, z')$, then $R(z', z'')$, ..., until we reach some $R(z, y)$".

$\mathtt{B}(x, y)$ and $\mathtt{F}(x, y)$ are equivalent because we may recursively reverse the order with which we list the R-chain from x to y. We will inductively define $\mathtt{B}$ and $\mathtt{F}$, then prove that $\mathtt{B}(x, y) \vdash \mathtt{F}(x, y)$ has a cyclic-proof but no cut-free cyclic proof.

The productions of $\mathtt{B}$ are: if $R(x, y)$ then $\mathtt{B}(x, y)$; if $\mathtt{B}(x, y)$, $R(y, z)$ then $\mathtt{B}(x, z)$. The productions of $\mathtt{F}$ are: if $R(x, y)$ then $\mathtt{F}(x, y)$; if $R(x, y)$, $\mathtt{F}(y, z)$ then $\mathtt{F}(x, z)$. These productions define the rules: $\mathtt{B}L$, $\mathtt{B}R$, $\mathtt{F}L$ and $\mathtt{F}R$.

As a Lemma, we first prove (cut-free) the following statement: "if we take a left-to-right R-chain and we add one step to the right we obtain a left-to-right R-chain".

Lemma 5.1 $\mathtt{F}(x, z), R(z, y) \vdash \mathtt{F}(x, y)$ *has some cut-free cyclic proof* Π.

Proof
1. We first define a regular infinite proof Π. We choose any variable $t \not\equiv x, z, y$ and we infer the conclusion of Π by $\mathtt{F}L$-rule.
   (a) The base case is $x = x', z = z', R(x', z'), R(z, y) \vdash \mathtt{F}(x, y)$ for x', z' fresh. We use $=L$ with premise $R(x, z), R(z, y) \vdash \mathtt{F}(x, y)$. We prove it by $\mathtt{F}R$-rule with premises: $R(x, z), R(z, y) \vdash \mathtt{F}(x, z)$ and $R(x, z), R(z, y) \vdash R(z, y)$. The first premise is proved by $\mathtt{F}R$ with premise $R(x, z), R(z, y) \vdash R(x, z)$, then $\mathtt{id}$. The second premise is proved by $\mathtt{id}$.
   (b) The induction case is $x = x', z = z', R(x', t), \mathtt{F}(t, z'), R(z, y) \vdash \mathtt{F}(x, y)$ for x', z', t fresh. We use $=L$ twice and we have to prove $R(x, t), \mathtt{F}(t, z), R(z, y) \vdash \mathtt{F}(x, y)$. We use $\mathtt{F}R$ with two premises: $R(x, t), \mathtt{F}(t, z), R(z, y) \vdash R(x, t)$ and $R(x, t), \mathtt{F}(t, z), R(z, y) \vdash \mathtt{F}(t, y)$. The first premise is an $\mathtt{id}$-rule. We prove the second premise by $\mathtt{Weak}$ and $\mathtt{F}(t, z), R(z, y) \vdash \mathtt{F}(t, y)$. This latter is a renaming by a fresh variable t of the goal, hence we are done.
2. We check the global trace condition for Π. The unique infinite path is the rightmost path π. π moves from $\mathtt{F}(x, z), R(z, y) \vdash \mathtt{F}(x, y)$ to $\mathtt{F}(t, z), R(z, y) \vdash \mathtt{F}(t, y)$, and each time the unique assumption $\mathtt{F}(x, z)$ progresses. Thus, the trace connecting all ancestors of $\mathtt{F}(x, y)$ is infinitely progressing in π.

□

We prove $\mathtt{B}(x, y) \vdash \mathtt{F}(x, y)$ by a cut between the Lemma $\mathtt{F}(x, z), R(z, y) \vdash \mathtt{F}(x, y)$ and the very sequent $\mathtt{B}(x, y) \vdash \mathtt{F}(x, y)$ we are proving. This cut is of particular kind. It is a cut on a sequent decorating a descendant of the conclusion of the cut itself, and this is considered a restricted version of cut. We will also prove that this cut is a local cut in our terminology.

Lemma 5.2 $\mathtt{B}(x, y) \vdash \mathtt{F}(x, y)$ *has some cyclic proof* Π *having a local cut.*

Proof

1. We define a regular infinite proof Π. We infer the conclusion of Π by $\mathtt{B}L$-rule.
   (a) The base case of the $\mathtt{B}L$-rule is $x = x', y = y', R(x', y') \vdash \mathtt{F}(x, y)$ for x', y' fresh. We apply $=L$ twice and we have to prove $R(x, y) \vdash \mathtt{F}(x, y)$. This is provable by $\mathtt{F}R$-rule with premise $R(x, y) \vdash R(x, y)$, which is an $\mathtt{id}$-rule.
   (b) The inductive case of the $\mathtt{B}L$-rule is $x = x', y = y', \mathtt{B}(x', z), R(z, y') \vdash \mathtt{F}(x, y)$. We apply $=L$ twice and we have to prove $\mathtt{B}(x, z), R(z, y) \vdash \mathtt{F}(x, y)$. We prove it by a cut on $\mathtt{F}(x, z)$: the premise of the cut are $\mathtt{B}(x, z) \vdash \mathtt{F}(x, z)$ and $\mathtt{F}(x, z), R(z, y) \vdash \mathtt{F}(x, y)$. The first premise $\mathtt{B}(x, z) \vdash \mathtt{F}(x, z)$ of the cut is the original goal renamed with z fresh. The second premise of the cut is Lemma 5.1.
2. We check that the cut on $\mathtt{F}(x, z)$ is local in Π. *(i).* $\mathtt{F}(x, z)$ in the first premise has ancestor $\mathtt{F}(x, y)$ in the goal, which has ancestor $\mathtt{F}(x, y)$ in $\mathtt{F}(x, z), R(z, y) \vdash \mathtt{F}(x, y)$. This latter has ancestor $\mathtt{F}(t, y)$, which includes the eigenvariable t of a $\mathtt{F}L$-rule. *(ii).* $\mathtt{F}(x, z)$ in the second premise is inferred from a $\mathtt{F}L$-rule and $\mathtt{F}(t, z')$, with t eigenvariable of the rule. From *(i)* and *(ii)* we deduce that the same eigenvariable occurs in some ancestors of the left and right cut formula, hence the cut is local.
3. We check the global trace condition for Π. Consider any infinite path π in Π. If π eventually moves to $\mathtt{F}(x, z), R(z, y) \vdash \mathtt{F}(x, y)$, proved by Lemma 5.1, then π has an infinitely progressing trace from the unique assumption $\mathtt{F}(x, z)$. Otherwise π always moves from $\mathtt{B}(x, y) \vdash \mathtt{F}(x, y)$ to $\mathtt{B}(x, z) \vdash \mathtt{F}(x, z)$, and each time the unique inductive assumption $\mathtt{B}(x, y)$ progresses. In both cases, the global trace condition is satisfied.

□

An ∞-proof is an infinitary proof with the global trace condition, hence it is a sound proof. It may be not regular.

Lemma 5.3 *There is a cut-free non-regular ∞-proof of* $\mathtt{B}(x,y) \vdash \mathtt{F}(x,y)$

Proof For all $m \in \mathtt{N}$, there is a finite cut-free proof Φ_m of $R(x_0,x_1),\ldots,R(x_m,x_{m+1}) \vdash \mathtt{F}(x_0,x_{m+1})$, using only $\mathtt{F}R$-rule and $\mathtt{id}$. The definition is by induction on m. From this family of proofs we define a cut-free not regular ∞-proof Ψ_m of $\mathtt{B}(x_0,x_1), R(x_1,x_2),\ldots,R(x_m,x_{m+1}) \vdash \mathtt{F}(x_0,x_{m+1})$. We define Ψ_m by $\mathtt{B}L$ and $=L$ from $R(x_0,x_1), R(x_1,x_2),\ldots,R(x_m,x_{m+1}) \vdash \mathtt{F}(x_0,x_{m+1})$ and $\mathtt{B}(x_0,y), R(y,x_1), R(x_1,x_2),\ldots,R(x_m,x_{m+1}) \vdash \mathtt{F}(x_0,x_{m+1})$ for some fresh y. The first premise is Φ_m. Up to renaming, the second premise is Ψ_{m+1}. Now we set $\Psi = \Psi_0$: this is an infinitary proof of $\mathtt{B}(x_0,x_1) \vdash \mathtt{F}(x_0,x_1)$. There is a unique infinite path π in Ψ, and it is the rightmost. In π, the unique ancestor of the inductive formula $\mathtt{B}(x_0,x_1)$ progresses at each step. Thus, the global trace condition is satisfied in Ψ. For each m, Ψ includes the sequent $R(x_0,x_1),\ldots,R(x_m,x_{m+1}) \vdash \mathtt{F}(x_0,x_{m+1})$, hence Ψ includes infinitely many sequents of different size and it is not regular. $\square$

We will check now that any cut-free ∞-proof Π of $\mathtt{B}(x,y) \vdash \mathtt{F}(x,y)$ is similar to the proof defined in Lemma 5.3 above, and not regular. Indeed, we will show that Π for each $m \in \mathtt{N}$ first unfolds the inductive definition of $\mathtt{B}(x,y)$ to some $R(x,x_1),\ldots,R(x_m,y)$. Then Π proves $\mathtt{F}(x,y)$. This operation cannot be done in *constant memory space*: for any $m \in \mathtt{N}$, all atoms $R(x_1,x_2),\ldots,R(x_m,y)$ should be together in some left-hand side of some sequent of Π. The reason is: if, say, we forget the atom $R(x_1,x_2)$ and we unfold again $\mathtt{B}(x,y)$, there is no reason why we should get the same R-chain we got before. Instead of obtaining $R(x_1,x_2)$, we obtain some $R(x'_1,x'_2)$, which cannot be combined with $\mathtt{F}(x,x_1)$ to prove $\mathtt{F}(x,y)$.

Thus, Π has sequents of size $\geq m$ for all $m \in \mathtt{N}$ and Π is not regular. As a corollary, we will deduce that being cut-free and being regular are incompatible for any ∞-proof of $\mathtt{B}(x,y) \vdash \mathtt{F}(x,y)$.

The first step in our proof is the following one. For every $m \in \mathtt{N}$ we define a canonical model $\mathcal{M}_m$ of the language $L = \{R, \mathtt{F}, \mathtt{B}\}$. We set $\mathcal{M}_m = [0, m+1] \times \mathtt{N}$, and we define $R_{\mathcal{M}_m}((p,q),(p',q')) \Leftrightarrow (p+1 = p')$. The model $\mathcal{M}_m$ consists of $m+2$ vertical lines, two elements are R-related if they are in consecutive lines. The longest R-chain in $\mathcal{M}_m$ has $m+2$ elements and $m+1$ edges. Two elements in the same vertical line cannot be distinguished by $R_{\mathcal{M}_m}$. $\mathtt{F}_{\mathcal{M}_m}$ and $\mathtt{B}_{\mathcal{M}_m}$ are defined inductively from $R_{\mathcal{M}_m}$. As p consequence, we have $\mathtt{F}_{\mathcal{M}_m}((p,q),(p',q'))$ if and only if $p < p'$ if and only if $\mathtt{B}_{\mathcal{M}_m}((p,q),(p',q'))$.

We introduce some proof terminology. Whenever a proof Π is fixed, we write $\nu \in \Pi$ for: "ν is a node of Π". We write $\Gamma_\nu \vdash \Delta_\nu$ for the sequent decorating ν in Π and $\nu : \Gamma \vdash \Delta$ for $\Gamma = \Gamma_\nu$ and $\Delta = \Delta_\nu$. We call "induction on ν" the induction on the distance of ν from the root of Π. If $\mu \in \Pi$, we write $\nu \leq \mu, \nu < \mu$ for ν descendant of μ, proper descendant of μ respectively. The root of Π is the the lowest node.

Assume Π is a cut-free ∞-proof of $\mathtt{B}(x,y) \vdash \mathtt{F}(x,y)$. By possibly renaming Π, we may assume that all eigenvariables of any $\nu \in \Pi$ are different from all eigenvariables of any $\mu \in \Pi$ with $\mu < \nu$. By induction on ν we prove that if r is the rule of conclusion $\nu \in \Pi$, then $r = \mathtt{Weak}, =\!L, \mathtt{B}L, \mathtt{F}R$, or $r = \mathtt{id}$, with $\mathtt{id}$ inferring some $R(x,y) \in \Gamma_\nu \cap \Delta_\nu$, or $r =$ a substitution rule; and that Γ_ν consists of instances of $=, \mathtt{B}, R$, while Δ_ν consists of instances of $\mathtt{F}$, R.

For all $m \in \mathtt{N}$, $\nu \in \Pi$ we define by induction on ν the *canonical* $\mathcal{M}_m$-*assignment* $\sigma_\nu : \mathtt{FV}(\Gamma_\nu \vdash \Delta_\nu) \to \mathcal{M}_m$, with $\mathtt{dom}(\sigma_\nu)$ the set of all variables occurring in some node $\mu \leq \nu$. Informally, we set $\sigma_\nu(x) = (i,j)$ if the only values for x "relevant for the proof" are the elements in the vertical line number i of $\mathcal{M}_m$. When all values of x are "irrelevant for the proof", we arbitrarily choose some previously selected value as value for x. When x is an eigenvariable of Π, we use the index j (the position in the vertical line in $\mathcal{M}_m$) in order to distinguish x from all previous values in $\mathtt{range}(\sigma_\nu)$, whenever this is possible.

Definition 5.4 (Canonical assignment σ_ν) *Assume $\nu_0 \in \Pi$ is the root. We set $\sigma_{\nu_0}(x) = (0,0)$ and $\sigma_{\nu_0}(y) = (m+1,0)$. Assume $\nu \in \Pi$, $\nu : \Gamma_i \vdash \Delta_i$ and ν is the premise number i of some rule r of Π, with conclusion $\mu : \Gamma \vdash \Delta$. Let $x \in \mathtt{dom}(\sigma_\nu)$.*

1. *Assume x is an eigenvariable of r. If $r =$ some substitution rule θ, we set $\sigma_\nu(x) = \sigma_\mu(\theta(x))$. If $r = \mathtt{B}L$, then r infers $\mathtt{B}(a,b), \Gamma' \vdash \Delta'$ from $\mathtt{B}(a',c'), a = a', b = b', R(c',b'), \Gamma' \vdash \Delta'$, and from $R(a',b'), a = a', b = b', \Gamma' \vdash \Delta'$. The possible choices for x are a', b', c'. We set $\sigma_\nu(a') = \sigma_\mu(a)$ and $\sigma_\nu(b') = \sigma_\mu(b)$. If $\sigma_\mu(b) = (i,j)$ then:*

   (a) *in the case $i > 0$ we set $\sigma_\nu(c') = (i-1, j')$, where j' is the number of $\mathtt{B}L$-rules in the path between ν and the root.*

   (b) *in the case $i = 0$ we set $\sigma_\nu(c') =$ some value in $\mathtt{range}(\sigma_\mu)$ (say, $(0,0)$).*

2. *Assume x is not an eigenvariable of r. If $x \in \mathtt{FV}(\Gamma \vdash \Delta)$ we set $\sigma_\nu(x) = \sigma_\mu(x)$, otherwise we set $\sigma_\nu(x) =$ some value in $\mathtt{range}(\sigma_\mu)$ (say, $(0,0)$).*

By induction on ν, we may prove that the definition is correct and that $\mathtt{dom}(\sigma_\nu)$ equal to the set of all variables occurring in some $\mu \leq \nu$. In the case x is some eigenvariable, by our convention on eigenvariables, x does not occur in any node $\rho \leq \mu$, therefore $x \notin \mathtt{dom}(\sigma_\mu)$ and we are free to choose any value for $\sigma_\nu(x)$.

By case analysis, we have $\mathtt{range}(\sigma_\nu) = \mathtt{range}(\sigma_\mu)$, except in the case ν is the second premise of a $\mathtt{B}L$-rule, in which case we have $\mathtt{range}(\sigma_\nu) \setminus \mathtt{range}(\sigma_\mu) = \{\sigma_\nu(c')\}$.

As usual in Model Theory, we define $\sigma_\nu, \mathcal{M}_m \models R(a,b)$ as $R_{\mathcal{M}_m}(\sigma_\nu(a), \sigma_\nu(b))$. We define $\models$ in the same way for the formulas: $a = b, \mathtt{F}(a,b), \mathtt{B}(a,b)$. We define $\sigma_\nu, \mathcal{M}_m \models \Gamma$ as $\sigma_\nu, \mathcal{M}_m \models A$ for all $A \in \Gamma$. We define $\Pi_1 \subseteq \Pi$ as the "pruning of Π whose nodes have all assumptions true". Formally, we set $\nu \in \Pi_1$ if and only if $\mathcal{M}_m, \sigma_\mu \models \Gamma_\mu$ for every $\mu \leq \nu$. Π_1 is a subtree of the proof Π, but it is not a sound proof: some rules in Π_1 have missing premises.

Lemma 5.5 (Π_1-Lemma) *1.* Π_1 *includes:* (a) *the root of* Π*;* (b) *exactly one premise for each* $\mathtt{B}L$*-rule; and* (c) *all premises of all other rules.*

2. Π_1 *is finite.*

Proof 1. (a) Assume ν_0 is the root of Π. Then $\Gamma_{\nu_0} = \{\mathtt{B}(x,y)\}$ and $\mathcal{M}_m, \sigma_{\nu_0} \models \mathtt{B}(x,y)$, hence $\nu_0 \in \Pi_1$.

(b) Assume $\nu \in \Pi_1$ and r is a rule with conclusion ν. Assume $r = \mathtt{B}L$. Then $\nu : \mathtt{B}(a,b), \Gamma' \vdash \Delta'$. ν has first premise $\alpha : a = a', b = b', \mathtt{B}(a',c'), R(c',b'), \Gamma' \vdash \Delta'$ and second premise $\beta : a = a', b = b', R(a',b'), \Gamma' \vdash \Delta'$. For $\mu = \alpha, \beta$ we have $\sigma_\mu(a') = \sigma_\nu(a)$ and $\sigma_\mu(b') = \sigma_\nu(b)$. By the assumption $\nu \in \Pi_1$ we have $\sigma_\nu, \mathcal{M}_m \models \mathtt{B}(a,b)$: then $\sigma_\nu(a)$ and $\sigma_\nu(b)$ are connected by some R-chain of length $l \geq 1$, and the same holds for $\sigma_\nu(a')$ and $\sigma_\nu(b')$. If $l = 1$ then $\mathtt{B}(a',c'), R(c',b')$ are false in $\sigma_\alpha, \mathcal{M}_m$, independently from the value of $\sigma_\alpha(c')$, while $\sigma_\beta, \mathcal{M}_m \models R(a',b')$. Thus, $\alpha \notin \Pi_1$ and $\beta \in \Pi_1$. If $l > 1$, then $\mathtt{B}(a',c'), R(c,b')$ are true because $\sigma_\alpha(c')$ is defined as some R-predecessor of $\sigma_\alpha(b')$, while $R(a',b')$ is false in $\sigma_\beta, \mathcal{M}_m$. Thus, $\alpha \in \Pi_1$ and $\beta \notin \Pi_1$.

(c) Assume $r \neq \mathtt{B}L$, hence r is $=\!L, \mathtt{F}R, \mathtt{id}$ or is the substitution rule. By case analysis we deduce that for all premises $\mu : \Gamma_i \vdash \Delta_i$ we have $\sigma_\mu, \mathcal{M}_m \models \Gamma_i$.

2. Π_1 *is a finite tree.* Assume $\nu \in \Pi_1$ and $\mathtt{B}(a,b) \in \Gamma_\nu$ and $\sigma_\nu(b) = (i,h)$. Any ancestor $\mathtt{B}(a',b') \in \Gamma_\mu$ of $\mathtt{B}(a,b) \in \Gamma_\nu$ is true in $\mathcal{M}_m, \sigma_\mu$. Therefore in any progress of $\mathtt{B}(a,b) \in \Gamma_\nu$ the first component i of $\sigma_\nu(b)$ is reduced by 1. Since $i \in [0, m+1]$, this may happen at most $m+1$ times. Thus, no path in $\Pi_1 \subseteq \Pi$ has an infinite progressing trace: by the global trace condition for Π, all paths in Π_1 are finite. From Π_1 binary and König's Lemma we deduce that Π_1 is a finite tree.

□

By Lemma 5.5.1.(b), the only rule left with two premises in Π_1 is $\mathtt{F}R$.

We need some more proof terminology. If $\nu, \mu \in \Pi$, $\nu > \mu$, and an occurrence of A in $\Gamma_\nu \vdash \Delta_\nu$ is an ancestor of an occurrence B in $\Gamma_\mu \vdash \Delta_\mu$, we say that A, B have ancestor distance 0 if there is no rule between ν, μ whose main formula is some ancestor of B. A, B could still be syntactically different, because we may have $=L$-rules or substitution rules between ν, μ.

Ancestor of distance 0 in Π_1 have equal arguments in $\mathcal{M}_m$. Indeed, assume that $p = R, \mathtt{F}, \mathtt{B}$. If ν is an ancestor of μ in Π_1 and $p(a', b') \in \Gamma_\nu$ is an ancestor of $p(a, b) \in \Gamma_\mu$ (or $p(a', b') \in \Delta_\nu$ is an ancestor of $p(a, b) \in \Delta_\mu$) and $p(a', b'), p(a, b)$ have distance 0, then $\sigma_\nu(a') = \sigma_\mu(a)$ and $\sigma_\nu(b') = \sigma_\mu(b)$. The proof is by induction on $\nu \in \Pi_1$. We use the following fact. All $=L$-rules whose conclusion is some $\rho \in \Pi_1$ have main formula some $a = b \in \Gamma_\rho$. By definition of Π_1 we have $\sigma_\rho, \mathcal{M}_m \models a = b$. Thus, $=L$ replaces an argument of p by an equal argument in $\mathcal{M}_m$.

Another feature of Π_1 is that for any $\nu \in \Pi_1$, any $\mathtt{B}(a, b) \in \Gamma_\nu$ we have $\sigma_\nu(a) = (0, 0)$, and for any $\mathtt{F}(a, b) \in \Delta_\nu$ we have $\sigma_\nu(b) = (m + 1, 0)$. The proof is by induction on ν.

The main feature of Π_1 is that for all right-hand side Δ_ν of a sequent of Π_1 we may extract from Π_1 some proof of some $A \in \Delta_\nu$, starting from assumptions in Π_1, then using zero or more $\mathtt{F}$-productions. All steps of this proof are sound in $\mathcal{M}_m$. Formally, for any $\nu \in \Pi$ we define a notion of *production proof* for $A \in \Delta_\nu$.

We say that $R(a, b) \in \Delta_\nu$ has a production proof if some ancestor $R(a', b')$ of $R(a, b)$ is a main formula of some $\mathtt{id}$-rule.

We say that $\mathtt{F}(a, b) \in \Delta_\nu$ has a production proof if there is some trace of $\mathtt{F}(a, b)$ ending in some main formula of an $\mathtt{id}$, such that for all rules $r = \mathtt{F}R$ whose main formula is in the trace: the trace chooses the auxiliary formula $\mathtt{F}(c', b')$ of the r if any, and the auxiliary formula $R(a', c')$ of r has a production proof.

Lemma 5.6 *Assume $\nu \in \Pi_1$.*

1. *Assume $R(a, b) \in \Delta_\nu$ has a production proof. Then: $R(a, b)$ has some ancestor $R(a', b') \in \Delta_\mu$, $\mu \geq \nu$ such that $R(a', b') \in \Gamma_\mu$, and: $\sigma_\nu, \mathcal{M}_m \models R(a, b)$.*

2. *If $A \in \Delta_\nu$ has a production proof then $\sigma_\nu, \mathcal{M}_m \models A$.*

3. *There is some $A \in \Delta_\nu$ with a production proof.*

Proof 1. Assume $A = R(a,b) \in \Delta_\nu$. Then some ancestor $R(a',b') \in \Delta_\mu$ of $R(a,b)$ in Π_1 is a main formula of an `id`-rule. Then $R(a',b') \in \Gamma_\mu$, hence $\sigma_\mu, \mathcal{M}_m \models R(a',b')$. $R(a',b')$ is a 0-ancestor of $R(a,b)$, because the only rule with main formula $R(a',b')$ is `id`, and there are no `id`-rules below μ because the `id`-rule has no premises. Thus, $\sigma_\nu, \mathcal{M}_m \models R(a,b)$.

2. By induction on $\nu \in \Pi_1$.

   (a) By point 1 above.

   (b) Assume $A = \mathtt{F}(a,b) \in \Delta_\nu$. There is some trace τ of $\mathtt{F}(a,b)$ ending in some main formula of an `id`, such that for all rules $r = \mathtt{F}R$ whose main formula is in τ: τ chooses the auxiliary formula $\mathtt{F}(c',b')$ of the r if any, and the auxiliary formula $R(a',c')$ of r has a production proof. The `id`-rule has main formula some $R(c,d)$, therefore τ includes some 0-ancestor $\mathtt{F}(a',b')$ of $\mathtt{F}(a,b)$, which is the main formula of some $\mathtt{F}R$-rule. By $\mathtt{F}(a',b')$ 0-ancestor of $\mathtt{F}(a,b)$ it is enough to prove $\sigma_\mu, \mathcal{M}_m\mathtt{F}(a,b)$.

   Assume $\mathtt{F}R$ has a unique premise μ, and auxiliary formula $R(a'',b'')$, with $a' = a''$, $b' = b''$ true in σ_μ. By induction on μ we have $\sigma_\mu, \mathcal{M}_m \models R(a'',b'')$, hence $\sigma_\mu, \mathcal{M}_m \models \mathtt{F}(a',b')$, as wished.

   Assume $\mathtt{F}R$ has two premises α, β, and auxiliary formulas $R(a'',c'')$ and $\mathtt{F}(c'',b'')$, with $a' = a''$, $b' = b''$ true in σ_α and σ_β. By induction on α, β we have $\sigma_\alpha, \mathcal{M}_m \models R(a'',c'')$ and $\sigma_\beta, \mathcal{M}_m \models \mathtt{F}(c'',b'')$, hence $\sigma_\mu, \mathcal{M}_m \models \mathtt{F}(a',b')$, as wished.

3. By induction on the height of a node $\nu \in \Pi_1$: the height exists because Π_1 is finite. We prove the thesis for all leaves of Π, then we assume the thesis for all premises of a rule of Π_1 and we prove it for the conclusion of the rule.

   (a) Assume ν is a leaf of Π_1. Then ν is an `id`-rule and we choose $A =$ the atom $R(a,b)$ inferred by the `id`-rule.

   (b) Assume ν is the conclusion of some $\mathtt{F}R$-rule in Π_1. Then $\nu : \Gamma \vdash \mathtt{F}(a,b), \Delta$ has premises $\alpha : \Gamma \vdash R(a,c), \Delta$ and $\beta : \Gamma \vdash \mathtt{F}(c,b), \Delta$. If there is some $A \in \Delta$ in α we a production proof we choose A. If not, and there is some $B \in \Delta$ in β with a production proof we choose B. If not, by induction hypothesis on the trees of root α and β, both $R(a,c)$ and $\mathtt{F}(c,b)$ have a production proof. Thus, $\mathtt{F}(a,b)$ has a production proof.

(c) Assume ν is the conclusion of some rule $\neq \mathtt{id}, \mathtt{F}R$ in Π_1. Then r has a single premise μ in Π_1. We apply induction hypothesis and we choose the descendant A' of the formula A we have for μ.

□

Let $\nu \in \Pi_1$ and $k \in \mathtt{N}$. The last ingredient we need for proving the non-regularity of Π is the notion of R-chain in the node. We say that $a_1, \ldots, a_{k+1} \in \mathcal{M}_m$ is an R-chain in the node ν if $a_1 \in \mathtt{range}(\sigma_\nu)$ and there are $R(x'_1, z'_1), \ldots, R(x'_k, z'_k) \in \Gamma_\nu$ such that $\sigma_\nu(x'_i) = a_i, \sigma_\nu(z'_i) = a_{i+1}$ for $i = 1, \ldots, k$. If $k = 0$ the definition of R-chain in ν becomes: $a_1 \in \mathtt{range}(\sigma_\nu)$.

If there is an R-chain of $k+1$ elements then $\mathcal{M}_m, \sigma_\nu \models R(x'_i, z'_i)$ by definition of Π_1, therefore $a_1 = (i, h_1), \ldots, a_{k+1} = (i+k, h_{k+1})$ are in consecutive vertical lines in $\mathcal{M}_m$, hence pairwise distinct. Thus, the k atoms $R(x'_i, z'_i)$ are pairwise distinct because they are distinguished by σ_ν. If we are able to prove that for all $m \in \mathtt{N}$ there is an R-chain of $m+1$ elements in some $\nu \in \Pi$ then Π is not regular.

Lemma 5.7 (Right-extension) *Assume that $\nu \in \Pi_1$ and for some $\mu \geq \nu$ there is some $R(a, b) \in \Gamma_\mu$ such that $(0, 0) \neq \sigma_\mu(a) \in \mathtt{range}(\sigma_\nu)$. Then $(0, 0) \neq \sigma_\mu(b) \in \mathtt{range}(\sigma_\nu)$ and there is some $R(a', b') \in \Gamma_\nu$ such that $\sigma_\nu(a') = \sigma_\mu(a)$ and $\sigma_\nu(b') = \sigma_\mu(b)$.*

Proof Either $R(a, b)$ is the 0-ancestor of some $R(a', b') \in \Gamma_\nu$ or $R(a, b)$ is the 0-ancestor of some $R(a', b')$ auxiliary formula of some premise $\mu \geq \rho > \nu$ of some $\mathtt{B}L$-rule.

Assume the first case. Then $\sigma_\nu(a') = \sigma_\mu(a)$ and $\sigma_\nu(b') = \sigma_\mu(b)$, hence $\sigma_\mu(b) \in \mathtt{range}(\sigma_\nu)$. From $\sigma_\mu, \mathcal{M}_m \models R(a, b)$ we deduce that $\sigma(b)$ cannot be in the first vertical line of $\mathcal{M}_m$, hence $(0, 0) \neq \sigma_\mu(b)$.

Assume the second case: we derive a contradiction. We argue by cases on ρ.

1. Assume ρ is the first premise $a = a', b = b', R(a', b'), \Gamma' \vdash \Delta'$ of $\mathtt{B}(a, b), \Gamma' \vdash \Delta'$. Then $\sigma_\mu(a') = \sigma_\rho(a') = \sigma_\rho(a) = (0, 0)$ (this is a property of Π_1), contradicting the hypothesis.

2. Assume ρ is the second premise $a = a', b = b', c = c', \mathtt{B}(a', c'), R(c', b'), \Gamma' \vdash \Delta'$ of $\mathtt{B}(a, b), \Gamma' \vdash \Delta'$. By definition of σ_ρ we should have $\sigma_\mu(c') = \sigma_\rho(c') \notin \mathtt{range}(\sigma_\nu)$, contradicting the hypothesis.

□

We prove that there is no cut-free cyclic proof Π for $\mathtt{B}(x, y) \vdash \mathtt{F}(x, y)$.

Theorem 5.8 *Assume* Π *is a cut-free* ∞*-proof of* $\mathtt{B}(x, y) \vdash \mathtt{F}(x, y)$*. For all* $m \in \mathtt{N}$*, there is some* $\nu \in \Pi$ *and some* m *atoms* $R(x'_1, z'_1), \ldots, R(x'_m, z'_m) \in \Gamma_\nu$ *pairwise distinct. In particular,* Π *is not regular.*

Proof $\mathtt{F}(x, y)$ is the unique formula in the right-hand side of the root of Π_1. Thus, by Lemma 5.6, $\mathtt{F}(x, y)$ has a production proof in Π. We unfold the definition of production proof. There are $m+1$ nodes $\nu_0 < \ldots < \nu_m$ in Π_1, all conclusions of $\mathtt{F}R$-rules. For all $0 \leq k < m$, the node $\nu_k : \Gamma_k \vdash \mathtt{F}(x_k, y_k), \Delta'_k$ has first premise $\alpha_k : \Gamma_k \vdash R(x_k, z_k), \Delta'_k$ and second premise $\beta_k : \Gamma_k \vdash \mathtt{F}(z_k, y_k), \Delta'_k$. $\mathtt{F}(x_0, y_0)$ is a distance 0 ancestor of $\mathtt{F}(x, y)$ and $\mathtt{F}(x_{k+1}, y_{k+1})$ is a distance 0 ancestor of $\mathtt{F}(x_k, y_k)$. The node $\nu_m : \Gamma_m \vdash \mathtt{F}(x_m, y_m)$ is the conclusion of a $\mathtt{F}L$-rule with a single premise $\rho = \alpha_m : \Gamma_m \vdash R(x_m, y_m), \Delta'_k$. For all $k < m$, the formulas $R(x_k, z_k)$ and $\mathtt{F}(x_k, y_k)$ have a production proof, hence they are true in σ_{ν_k} and $\mathcal{M}_m$. By the distance 0 ancestor relation we have $(0, 0) = \sigma_\rho(x) = \sigma_\rho(x_0)$ and $\sigma_\rho(z_k) = \sigma_\rho(x_{k+1})$ for all $k < m$ and $\sigma_\rho(y_k) = \sigma_\rho(y) = (m + 1, 0)$ for all $k \leq m$. Thus there are $a_0, \ldots, a_m \in \mathcal{M}_m$ which form an R-chain in $\mathcal{M}_m$. Thus, $a_k = (k, h_k)$ for all $k \leq m + 1$ and $\sigma_\rho(x_k) = a_k$, $\sigma_\rho(y_k) = a_{m+1}$ for all $k \leq m$.

We claim that there is an R-chain in ν_0. The proof is by induction on $k \in [0, m]$. Let $\tau = \sigma_{\nu_0}$ be the canonical assignment for the node $\nu_0 : \Gamma_0 \vdash \mathtt{F}(x_0, y_0), \Delta'_0$.

1. Let $k = 0$: then $a_1 = \tau(z_0) \in \mathtt{range}(\tau)$. We already checked that $a_1 = (1, h_1) \neq (0, 0)$.

2. Assume the thesis for $0 \leq k < m$, in order to prove it for $k + 1$. By inductive assumption $(0, 0) \neq a_1 \in \mathtt{range}(\tau)$ and and there are $R(x'_1, z'_1), \ldots, R(x'_k, z'_k) \in \Gamma_{\nu_0}$ such that $\sigma_{\nu_0}(x'_i) = a_i, \sigma_{\nu_0}(z'_i) = a_{i+1}$ for $i = 1, \ldots, k$. We already proved that there is some $R(x_{k+1}, z_{k+1}) \in \Gamma_\mu$ in some $\mu \geq \nu_0$ such that $\sigma_\mu(x_{k+1}) = a_{k+1}, \sigma_\mu(z_{k+1}) = a_{k+2}$. We apply the Right Extension Lemma 5.7and we deduce that there is some $R(x'_{k+1}, z'_{k+1}) \in \Gamma_{\nu_0}$ such that $\sigma_{\nu_0}(x'_{k+1}) = a_{k+1}, \sigma_{\nu_0}(z'_{k+1}) = a_{k+2} \neq (0, 0)$.

We conclude that there are m formulas in Γ_0 whose first arguments may be made pairwise distinct by the assignment σ_{ν_m}. Thus, there are m pairwise distinct formulas in Γ_0. $\square$

6 Induction and failure cut

In this section we prove that we cannot interpret (full) induction rule $\mathtt{Ind}$ without cuts, even for the induction rule for the predicate $\mathtt{N}t$, and we propose

$\mathtt{Ind}R$, a restriction of induction which is conditionally derivable without cuts.

Lemma 6.1 (Induction and cut) *There is a cut-free proof of $E_{2^x}, \mathtt{N}x \vdash \mathtt{N}2^x$ in cyclic proofs + induction rule, and no cut-free proof in cyclic proofs.*

Proof Indeed, there is a cut-free proof of $E_{2^x} \vdash \mathtt{N}2^0$: we use $=L$ on $2^0 = 1$ and $E_{2^x} \vdash \mathtt{N}1$, with $1 \equiv S0$. We prove $E_{2^x} \vdash \mathtt{N}S0$ from $\mathtt{N}R$ for S and $E_{2^x} \vdash \mathtt{N}0$, then $\mathtt{N}R$ for 0. There is a cut-free proof of $E_{2^x}, \mathtt{N}x \vdash \mathtt{N}2^{Sx}$, we use $\forall L$ on $\forall x.2^{Sx} = 2^x + 2^x$ and $E_{2^x}, 2^{Sx} = 2^x + 2^x, \mathtt{N}x \vdash \mathtt{N}2^{Sx}$, then $=L$ and $E_{2^x}, \mathtt{N}x, \mathtt{N}2^x \vdash \mathtt{N}(2^x{+}2^x)$. This latter has a cut-free cyclic proof by Lemma 4.1, point 3. We already proved that there is no cut-free proof of $E_{2^x}, \mathtt{N}x \vdash \mathtt{N}2^x$, this impliess that cut-free proofs do not conditionally derive $\mathtt{Ind}$-rule. $\Box$

We analyze our cyclic proof of $E_{2^x}, \mathtt{N}x \vdash \mathtt{N}2^x$. Implicitly, the proof receives a value of x and computes a value of 2^x in unary notation (with $0, S$ only): this is a basic example of non-polynomial computation. We assume that cuts are required by proofs hyding non-polynomial computations, and we study how to prevent this situation.

The proof of $E_{2^x}, \mathtt{N}x \vdash \mathtt{N}2^x$ includes a proof $E_{2^x}, \mathtt{N}2^x \vdash \mathtt{N}(2^x{+}2^x)$, in which we derive the assumption $\mathtt{N}2^x$ twice with some $\mathtt{N}L$-rule. This sub-proof defines a sub-recursion computing the value of $(2^x + 2^x)$ from the value of 2^x. The point is that the value of 2^x is the very value being recursively computed by our proof. It is known that, in order to prevent non-polynomial computation, *"the depth of sub-recursions ... cannot depend on the value being recursively computed"* ([2], §2). This suggests to forbid any $\mathtt{N}L$-rule whose main formula is the induction hypothesis $\mathtt{N}2^x$. We allow a $\mathtt{N}L$-rule inferring the assumption $\mathtt{N}x$.

More in general, to prevent the need of cuts, we define a weaker rule $\mathtt{Ind}R$ in which the assumption $F[x]$ of the induction step cannot be the main formula of an L-rule. $\mathtt{Ind}R$ may be interpreted in cyclic proofs without adding new cuts. Our impression is that this is the way we argue by induction in a cut-free cyclic proof, in general.

Formally, an R-proof of $\Gamma, \mathtt{N}x, F[x] \vdash F[Sx], \Delta$ for $F[x]$ is a cyclic proof in which we forbid the use of L-rules with main formula $F[x]$. The only rule allowed to infer $F[x]$ is $\mathtt{id}$, then we may apply R-rules from the right occurrence of $F[x]$ in the $\mathtt{id}$-rule.

We define the restriction $\mathtt{Ind}R$ of induction rule in which the second premise $\Gamma, \mathtt{N}x, F[x] \vdash F[Sx], \Delta$ in an R-rule for $F[x]$.

Lemma 6.2 ($\mathtt{Ind}R$ is conditionally derivable in cut-free proofs) *1. There is an R-cyclic proof Π_1 of $\Gamma, \mathtt{N}x, F[x] \vdash F[Sx], \Delta \Leftrightarrow$ there is a* *cyclic proof* Π *of* $\Gamma, \mathtt{N}x \vdash F[Sx], \Delta$ *with free assumption* $\Gamma, \mathtt{N}x \vdash F[x]$ *and* $\mathtt{N}x$ *in the free assumption ancestor of* $\mathtt{N}x$ *in the conclusion.*

Besides, Π *is cut-free* $\Leftrightarrow$ Π_1 *is cut-free.*

2. *Cut-free proofs conditionally derive the rule* $\mathtt{Ind}R$*.*

Proof 1. $\Leftarrow$. Assume we have a cyclic proof Π_1 of $\Gamma, \mathtt{N}x, F[x] \vdash F[Sx], \Delta$ in which the ancestors of $F[x]$ are infereed by no L-rule (including no $=L$-rule). We may define a proof Π of of $\Gamma, \mathtt{N}x \vdash F[x], \Delta$ with free assumption $\Gamma, \mathtt{N}x \vdash F[x]$, such that $\mathtt{N}x$ in the free assumption ancestor of $\mathtt{N}x$ in the conclusion, and Π is cut-free if Π_1 is cut-free.

We first rename all eigenvariables y in Π_1 in order to have $y \notin \mathtt{FV}(\Gamma, \mathtt{N}x \vdash \Delta)$, then we replace each node $\Gamma' \vdash \Delta'$ with $\Gamma, \mathtt{N}x, \Gamma' \vdash \Delta, \Delta'$, with $\Gamma, \mathtt{N}x, F[x] \vdash F[Sx], \Delta$ replaced by itself. All $\mathtt{N}x$ we add are an ancestor of $\mathtt{N}x$ in the conclusion.

We define in this way a proof Π_2 with at most the same number of subproofs, hence regular. For each infinite path π_2 of Π_2 there is some infinite path π_1 of Π_1. There is some infinitely progressing trace τ in π_1. τ is in π_2 and infinitely progressing, therefore Π_2 satisfies the global trace condition.

There are finitely many $\mathtt{id}$-rule for an ancestor of $F[x]$ in Π_2, say $\Gamma, \mathtt{N}x, \Gamma_i, F[x] \vdash F[x], \Delta, \Delta_i$ for $i = 1, \ldots, n$: these are the only rules inferring some ancestor of $F[x]$. The ancestors of $F[x]$ have no progress because we forbid L-rules for $F[x]$. Therefore we may remove all ancestors of $F[x]$ and we remove no progressing trace and the global trace condition is still true. The number of sub-proof may duplicate because some $F[x]$ on the left-hand side are ancestors and removed and some are not ancestors and not removed. Thus, regularity is preserved. We defined a proof Π_3 with open assumptions $\Gamma, \mathtt{N}x, \Gamma_i \vdash F[x], \Delta, \Delta_i$ for $i = 1, \ldots, n$, and with $\mathtt{N}x$ ancestor of $\mathtt{N}x$ in the conclusion. We prove each open assumption with $\mathtt{Weak}$ from new open assumptions $\Gamma, \mathtt{N}x \vdash F[x], \Delta$, while preserving regularity and global trace. This is a cyclic proof $\Pi = \Pi_4$ of $\Gamma \vdash F[x], \Delta$ with open assumption $\Gamma, \mathtt{N}x \vdash F[x], \Delta$, and $\mathtt{N}x$ ancestor of $\mathtt{N}x$ in the conclusion. In Π we inserted some $\mathtt{Weak}$-rules but no cut-rule, therefore if Π_1 is cut-free Π is cut-free.

$\Rightarrow$. Assume the converse. We rename all eigenvariables y of Π in order to have $y \notin \mathtt{FV}(F[x])$, then we add $F[x]$ everywhere in the proof, and we replace open assumptions $\Gamma, \mathtt{N}x, F[x] \vdash F[x], \Delta$ with the $\mathtt{id}$-rule.

2. Assume we have a cyclic proof Π_0 of $\Gamma, \vdash F[0]\Delta$ and Π_1 of $\Gamma, \mathtt{N}x, F[x] \vdash F[Sx], \Delta$ in which the ancestors of $F[x]$ use no L-rule. Let Π as in the previous point. From Π_0 and $\Pi[x'/x]$ with $x' \notin \mathtt{FV}(\Gamma, \mathtt{N}x \vdash F[x], \Delta)$ and the rule $\mathtt{N}L$ we may define a cyclic proof of $\Gamma, \mathtt{N}x \vdash F[x], \Delta$ with a rule $\mathtt{N}L$ in the root inferring $\mathtt{N}x$, and free assumption $\Gamma, \mathtt{N}x' \vdash F[x']$. $\mathtt{N}x$ in the root is the conclusion of a $\mathtt{N}L$-rule, hence there is a progress from $\mathtt{N}x$ to $\mathtt{N}x'$ in the premise. $\mathtt{N}x'$ is a descendant of $\mathtt{N}x'$ in each free assumption $\Gamma, \mathtt{N}x' \vdash F[x']$, therefore we have a progress from $\mathtt{N}x$ in the root to $\mathtt{N}x'$ in each free assumption.

   If we repeat the proof from the free assumption, choosing alternatively Π and $\Pi[x'/x]$, we define a regular proof Π'. Π' satisfies the global trace condition, because all infinite paths either are definitively in Π_0 or in some Π or $\Pi[x'/x]$ and include an infinitely progressing trace, or they pass through infinitely many Π and $\Pi[x'/x]$, and in this case $\mathtt{N}x$ in the root is infinitely progressing. Thus, $\mathtt{Ind}R$ is conditionally derivable without adding cuts, and cut-free proofs conditionally derive $\mathtt{Ind}R$.

□

7 Cyclic proofs: substitution and renaming

In order to prove a restricted version of cut-elimination, in this section we quickly recall some features of cyclic proofs: substitution and renaming rules.

A *substitution* is a map from finitely many first order variables to first order terms. A substitution is a variable substitution if it maps variables into variables, and a *renaming* if it is a bijection on variables. Substitutions are extended to terms/formulas/proof tree by compatibiliy, with renaming of bound variables to prevent variable capture.

We call an *infinitary binary tree* any possibly infinite tree in which each node has at most two children. We consider cyclic proofs as infinitary binary proof-trees for sequent calculus. The first group of rules are the usual rules for sequent calculus: identity rule, weakening, exchange, contraction, cut, left/right introduction for each logical connnective: $\vee, \wedge, \rightarrow, \forall, \exists$. As usual we often skip exchange and contraction rule, and we assume that left/right introduction and cut are merged with exchange and contraction: the inferred formulas and the assumptions formulas may be in any position in their side of the sequent, and inferring A may or may not include contraction on A.

Peano Arithmetic and Martin-Löf theory have more rules, induction rule, injectivity axioms for constructors and basic equality axioms, and in the case of Peano Arithmetic basic arithmetical axioms. The induction axiom for $\mathtt{N}$ and a formula F is $F[0/x], \forall x.(\mathtt{N}x, F \rightarrow F[Sx/x] \vdash F)$ for any F.

Cyclic proofs have different rules in their place:

1. *Substitution rule.* From $\Gamma \vdash \Delta$ and σ substitution we deduce $\sigma(\Gamma \vdash \Delta)$.
2. *Renaming rule.* From $\Gamma \vdash \Delta$ and σ renaming we deduce $\sigma(\Gamma \vdash \Delta)$. (This is a restriction of Substitution rule).
3. $(=L)$. From $\Gamma[a, b] \vdash \Delta[a, b]$ deduce $a = b, \Gamma[b, a] \vdash \Delta[b, a]$.
4. $(=R)$. $\Gamma \vdash \Delta, t = t$.
5. $(\mathtt{N}L)$. From $\Gamma, t = 0 \vdash \Delta$ and $\Gamma, t = Sx, \mathtt{N}x \vdash \Delta$ and x fresh ($x \notin \mathtt{FV}(\Gamma, t, \Delta)$) deduce $\Gamma, \mathtt{N}t \vdash \Delta$.
6. $(\mathtt{N}R)$: $\Gamma \vdash \mathtt{N}0$ and if $\Gamma \vdash \Delta, \mathtt{N}u$ then $\Gamma \vdash \Delta, \mathtt{N}Su$.

We add a left and right rule *for each inductive definition.* The fresh variables in the rules $\mathtt{N}L$, $\exists L$, $\forall R$ are the eigenvariables in the proof. Recall that induction is *not* assumed in cyclic proofs.

Assume c is some atomic predicate. We distinguish three sets of atomic predicates: logical (given with the first order languague), equality ($=$), and inductively defined predicates. We assume identity rule for logical predicates and we consider it both as a left-rule and a right-rule. We consider the identity rule as the introduction rule for logical predicates. We may derive identity for equality and for inductively defined predicates, in a cut-free way. Here are two examples.

1. *Identity for equality.* from $\vdash t = t$ (rule $=R$) we derive $t = u \vdash t = u$ (rule $=L$).
2. *Identity for* $\mathtt{N}$. It is enough to prove that we may derive derive $\mathtt{N}x \vdash \mathtt{N}x$ from $\mathtt{N}y \vdash \mathtt{N}y$ for any $y \not\equiv x$. We reason by cases with the $\mathtt{N}L$ rule. First, we derive $\mathtt{N}x, x = 0 \vdash \mathtt{N}x$ from $\mathtt{N}x \vdash \mathtt{N}0$ (rule $=L$), then from rule $\mathtt{N}L$. Second, for any $y \not\equiv x$ we derive $\mathtt{N}y, x = Sy \vdash \mathtt{N}x$ from $\mathtt{N}y \vdash \mathtt{N}Sy$ (rule $=L$), then from $\mathtt{N}y \vdash \mathtt{N}y$ (rule $\mathtt{N}R$), as wished.

We derive (cut-free) the identity rule for compound formulas from identity for atomic formulas.

Regular infinitary binary trees have a finite graph representation. Assume Π is regular, with at most n subtrees. Thus, in each branch of Π there is a first node, among the first $n + 1$ nodes, which is the root of a subtree equal to the subtree of a previous node. If we include a back link from these nodes to the unique ancestor which is the root of an equal tree we obtain a finite graph representation of the infinite tree Π. There are graph representation with exactly n nodes.

Assume Π is some infinitary binary proof tree. Assume $A = p(\vec{t})$ has an inductive definition. A *trace* of an occurence of A in the left-hand side of some sequent of Π is any possibly list τ of ancestors of A in Π. A trace τ progresses whenever an element $p(\vec{t})$ of τ is the assumption formula of a case rule. The global trace condition for Π is: for any infinite branch β of Π there is some infinitely progressing trace τ included in β.

Assume Π is a regular infinitary proof tree and G is its graph representation. Then the global trace condition is decidable for Π: we sketch how. We claim without proof that global trace condition is equivalent to: every path π from a node α to itself in G has some power π^n including a trace τ progressing from some A in α to itself. There are infinitely many path from a node $\alpha \in G$ to itself when G is cyclic, but if we quotient them according to the trace relationship they define among inductively defined formulas A in the left-hand side of a sequent, they are reduced to finitely many. Thus, the global trace condition is decidable for regular trees.

Cyclic proofs are infinitary binary trees Π which are regular and satisfy the global trace condition. Finitely many subtrees implies finitely many sequents and finitely many variables, including the eigenvariables of the proof.

From now on, we consider cyclic proofs without the substitution rule: they are enough to interpret the induction axiom, and the substitution rule is derivable from the other rules if we have cuts. The ordinary cut-elimination procedure applies substitutions on proofs. On infinite proofs, the cut-elimination procedure has to be repeated infinitely many times, cyclically, and if the proof substitutions compose, then they may define infinitely many different formulas and a non-regular proof-tree. We ignore whether this happens, but this could be the reason why cyclic-proofs have no cut-elimination, even if they lack the induction rule. In order to preserve regularity, we will define a cut-elimination process involving a finite set of substitution $\mathcal{S} = \{[u_1/x_1], \ldots, [u_n/x_n]\}$ on proofs with $\vec{x} \cap \mathtt{FV}(\vec{u}) = \emptyset$: in this way the closure by composition of $\mathcal{S}$ is finite.

The induction statement has cut-free cyclic proofs, both with and without renaming. With renaming we may obtain shorter proofs for the induction statement (and shorter proofs in general).

Substitution rule may be replaced everywhere by a combination of the rules for $\to, \forall$ and cut, while preserving regularity and global trace condition. From now on we skip the substitution rule in cyclic proofs, and we only consider the renaming rule.

We may prove that cyclic proofs are closed under a substitution $[t/x]$ on proofs. This property is more difficult to prove than expected. Unlike the case of finite proofs, the number of different subtrees of the infinitary proof may double after substitution, because the substitution $[t/x]$ does not propagate to *all* occurrences of x in the proof. Indeed, x may disappear by a weakening rule, then x be inserted as a eigenvariable in the proof, and in this case x cannot be substituted. Apparently, closure under substitution is not required for eliminating quantifier-free cuts, therefore we skip it.

We define a renaming procedure $\Pi_2 = \Theta(\Pi_1)$ of a cyclic proof Π_1. Θ applies one renaming substitution ψ to each sequent of in Π_1, with two provisos.

1. In the case of a renaming rule we require commutation of renaming: if we deduce $\phi_1(\Gamma_1 \vdash \Delta_1)$ from $\Gamma_1 \vdash \Delta_1$ in Π_1 and $\phi_2(\Gamma_2 \vdash \Delta_2)$ from $\Gamma_2 \vdash \Delta_2$ in in Π_2, then we require two renaming maps ψ_1 on $\phi_1(\Gamma_1 \vdash \Delta_1)$ and ψ_2 on $\Gamma_1 \vdash \Delta_1$ such that $\psi_1\phi_1 = \phi_2\psi_2$.

2. In any other case of two consecutive nodes of in Π_1 if we apply two renaming ψ_1, ψ_2 then ψ_1, ψ_2 coincide on the variables common to the two sequents.

Renaming preserves being an infinitary proof, regularity and the global trace condition. There is a canonical renaming for infinitary proofs with substitution rule restricted to renaming. Renaming may increase exponentially the number of different subtrees.

Lemma 7.1 (Canonical Renaming) *Assume Π is an infinitary binary proof with conclusion $\Gamma \vdash \Delta$, and $V = \mathtt{FV}(\Gamma \vdash \Delta)$, and $\phi : V \to W$ is a bijection on variables. Assume Π has substitution rule restricted to renaming. Then there is some renaming Θ_ψ such that $\Pi_0 = \Theta_\psi(\Pi)$ has conclusion $\phi(\Gamma \vdash \Delta)$ and substitution rule restricted to the identity. If Π has the global trace condition (is regular) then Π_0 has the global trace condition (is regular).*

Proof We define Π_0 by applying ϕ through Π. Whenever we find some renaming rule: "from $\Theta \vdash \Xi$ deduce $\psi(\Theta \vdash \Xi)$", then we replace ϕ with $\phi\psi$ from the node $\Theta \vdash \Xi$, and we associate the renaming rule to `id`. Whenever we find some rule r with conclusion $\Theta \vdash \Xi$ and one assumption $\Theta' \vdash \Xi'$ with a variable x bound in the proof, we replace ϕ with ψ. ψ is obtained by restricting ϕ to $\mathtt{FV}(\Theta, \Xi)$, then adding y/x, with y the first fresh variable, i.e., the first $\not\in \mathtt{FV}(\Theta, \Xi)$. Global trace condition is preserved because trace and progress are not affected by renaming. Assume Π is regular. Then for some n each sequent in Π has at most n free variables: n is the maximum among the number of variables in the roots of the finitely many subtrees of Π. Since each node of Π_0 is some renaming of some node of Π, each sequent in Π_0 has at most n free variables. The the index i of a eigenvariable x in Π_0 is at most $n-1$. Indeed, when we create a eigenvariable, we assign to it the first index not in use, and there are at most $n-1$ variables different from the eigenvariable, therefore the first first index not in use is some $i \leq n-1$. Thus, the variables of Π_0 are among $\mathtt{FV}(\phi(\Gamma \vdash \Delta))$ or the initial segment $\{x_0, \ldots, x_{n-1}\}$ of X, hence are finitely many. Each subtree Π_1 of Π_0 is $\Theta_\psi(\Pi_2)$ for some subproof Π_2 of Π, and since we have finitely many Π_2 in Π, and finitely many variables in Ψ_0, then we have finitely many choices for ψ, hence finitely many $\Theta_\psi(\Pi_2)$ in Π_0. $\Box$

In the last line of the proof above, the number of subtrees may raise by a factor $n!$, with n the maximum number of free variable in a sequent. We say that two infinitary proofs are equivalent if they may be obtained one from the other by: renaming, adding/removing any number of identical renaming rules which are below a rule different from renaming. The previous lemma says that a cyclic proof is equivalent to a proof having identical renaming only.

All identical renaming may be removed according to the definition of proof equivalent. Indeed, the only case in which this would not be possible is a path in which all rules from some point on are identical renaming. But this cannot be: by the global trace condition every renaming rule is below some progress point, hence some non-renaming rule. Thus, each cyclic proof with renaming is equivalent to some cyclic proof without renaming: this transformation, however, may raise exponentially the size of the graph representation.

We consider an apparent weakening of the notion of regularity: a proof is cyclic-equivalent if it is equivalent to a cyclic proof. A cyclic equivalent proof has the global trace condition and finitely many subtrees up to proof equivalence. Conversely, if we apply any canonical renaming, from a cyclic equivalent proof we obtain a cyclic proof without renaming, but the number of subtrees raised by $n!$, with n the maximum number of free variable in a sequent.

Assume A is any quantifier-free formula occurrence in a cyclic proof Π. If A is an inductive predicate, a progress point B of A in Π is any progress point of a trace of Π starting from A. By definition, B is some ancestor of A in Π. If A is any quantifier-free formula, a minimal inductive ancestor of A in Π is any ancestor of A which is an inductive predicate and is the first found in some ancestor sequence from A in Π. A progress point of A in Π is any progress point of any minimal inductive ancestor of A in Π.

8 Cyclic proofs: cut-rule

In this section we formulate the problem of cut-elimination for ∞-proofs and for cyclic proofs.

We plan to prove that every ∞-proof Π_1 has a normal form Π_2 which is an ∞-proof. Since some cyclic proofs have no normal form, it will follow that Π_1 may be regular and its normal form Π_2 not regular. An A-cut is global in Π if some positive ancestor of A has a free variable which is some eigenvariable of some negative ancestor of A. In particular, if a cut is the conclusion of Π, by a renaming we may assume that the cut is global. We will prove that if all cuts of Π_1 are global then the normal form of Π_2 is regular. This includes the case of a unique cut in the root of Π, hence it implies that the cut rule on quantifier-free formulas is conditionally derivable within cut-free proofs.

We define an equivalence relation $A \sim B$ on quantifier-free formulas, meaning that A, B are the same if we neglect terms. We define $p(\vec{t}) \sim p(\vec{u})$. We define $A_1 \to A_2 \sim B_1 \to B_2$ if $B_1 \sim A_1$ and $A_2 \sim B_2$. If $c \equiv \vee, \wedge$ we define $A_1 c A_2 \sim B_1 c B_2$ if $A_1 \sim B_1$ and $A_2 \sim B_2$. In all other cases $A \sim B$ is false.

When $A \sim B$ we define $A = B$ as the list of equations between terms of A, B in the same position. We define $p(t_1, \ldots, t_n) = p(u_1, \ldots, u_n)$ as $t_1 = u_1, \ldots, t_n = u_n$. We define $A_1 \to A_2 = B_1 \to B_2$ as $B_1 = A_1, A_2 = B_2$. If $c \equiv \vee, \wedge$ we define $A_1 c A_2 = B_1 c B_2$ as $A_1 = B_1, A_2 = B_2$.

For instance, $p(a) = p(b)$ is $a = b$ and $p(a) \to q(b) = p(c) \to q(d)$ is $c = a, b = d$. Remark that pairs of terms occuring positively in A, B are written in the order: term of A/term of B, while pairs of terms occuring negatively in A, B are written in the reverse order: term of B/term of A. This choice is intended to simplify the cut-elimination proof. Alternatively, we could use the rule $=L$ in order to replace $a = b$ with $b = a$ whenever this is required during the proof.

If $p \neq q$, then $p(a) = q(b)$ is not defined because $p(\_), q(\_)$ are different.

We define a generalized cut-rule ν for $A \sim B$: from $\Gamma_1 \vdash \Delta_1, A$ and $B, \Gamma_2 \vdash \Delta_2$ we deduce $A = B, \Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2$. We call this rule an A, B-cut.

Generalized cut-rule is derivable from cut-rule and $=L$ and weakening. In the case $A \equiv B$ we will deduce $A = A, \Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2$. $A = A$ is is list of identities, and if we remove them with a cut the conclusion is $\Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2$. Thus, cut rule `cut` may be deduced from ν and cut rule for identities.

Remark on the restricted use of substitution in the cut elimination process. We may normalize a proof with only global cuts by normalizing all maximal cuts in it. The result is a cyclic proof if and only if all normalizations of a maximal cut produce a cyclic proof. Our cut-elimination process involving a finite set of substitution $\mathcal{S}$ of all pairs $[u_i/x_j$, where: $u_1, \dots, u_n$ are all terms occurring in some ancestor of a global cut and $x_1, \dots, x_n$ are the eigenvariables used to infer some ancestor of a global cut. Both terms and variables are finitely many because the proof is regular. Let $\mathcal{C}$ be the closure under composition of $\mathcal{C}$: we prove that $\mathcal{C}$ is finite. Indeed, by definition $\mathtt{FV}(\vec{u})$ includes no eigenvariables of a left rule whose main formula is an ancestor of a global cut. Thus, $\vec{x} \cap \mathtt{FV}(\vec{u}) = \emptyset$. In this way for all $[u/x], [v/y] \in \mathcal{S}$ we have $[u/x][v/y] = [v/y]$ if $x \equiv y$ and $[u/x][v/y] = [v/y][u/x]$ if $x \not\equiv y$, therefore $\mathcal{C}$ consists of all compositions $[u_1/x_1] \dots [u_k/x_k]$ of elements of $\mathcal{S}$ with $x_1, \dots, x_k$ in increasing alphabetic order, hence $\mathcal{C}$ is finite. During the cut-elimination process we will have arguments of the form $\sigma(\Pi)$, for $\sigma \in \mathcal{C}$ and Π subproof of the original proof. These proofs are finitely many, and this remark will be crucial while proving regularity of the normal form.

Thus, we assume that Π has only global cuts and the root of Π is a cut. Assume $\mathcal{A}$ is the set of cut-formulas of Π and $\mathcal{B}$ the cut closure of $\mathcal{A}$.

The set $\mathcal{S}$ of Π-states is the set of finite trees S whose branches are made with the rule ν, and with leaves some subtrees $\Pi_1, \dots, \Pi_k$ of Π. We rename all eigenvariables in Π_i which are not eigenvariables of an ancestor of a cut in order to make them not occurring in any Π_j with $j \neq i$. We require that the cut-formulas of S are exactly the formulas in the leaves which are ancestors of some cut-formula in Π.

A Π-state S is a tree made with the rule ν only, we do not counts the nodes of the subtrees $\Pi_1, \dots, \Pi_k$ of Π as nodes of S.

If we fix a bound b to the height of a tree-state $S \in \mathcal{S}$, then up to renaming of eigenvariable not used for an ancestor of a cut there are finitely many trees with bound b.

The $\mathcal{P}$-states are the states of the algorithm removing the cut in Π with only global cuts, for instance removing the unique cut in $\Pi = \mathtt{cut}(\Pi_1, \Pi_2)$ for cut-free Π_1, Π_2.

9 Trivial cut-elimination: removing identities

We define a procedure eliminating any list of assumptions $t = t$ from left-hand side of a sequent.

Eliminating $t = t$ from the left-hand side of a sequent is equivalent to eliminate a cut with $\vdash t = t$.

Lemma 9.1 (Cut elimination for $t = t$) *Assume $\Pi : \Gamma \vdash \Delta$ is a cyclic proof whose only cuts are with some $t = t$. Then there is some cut-free cyclic proof $\Pi_0 : \Gamma \vdash \Delta$.*

Proof We define Π_0 by removing all ancestors of some cutted $t = t$. In the case $t = t$ is inferred by $=L$ in: "from $\Theta \vdash \Xi$ deduce $t = t, \Theta \vdash \Xi$", we replace $=L$ with its assumption. We cannot remove $=L$ for $t = t$ infinitely many times consecutively, otherwise Π would contain an infinite branch β definitely containing only $=L$, hence β would include no infinitely progressing trace. Thus, we defined a correct infinitary binary tree Π_0, with the same conclusion as Π. We check that Π_0 is cyclic.

1. Π_0 *has the global trace condition.* Any infinite branch γ of Π_0 is obtained from some branch β of Π with at least the same nodes, hence infinite. β has some infinitely progressing trace τ. We never remove progress points of τ while forming γ, hence τ is in γ.

2. Π_0 *is regular.* Each subtree of Π_0 is obtained from some subtree Π_1 of Π crossing out finitely many identities of the form $t = t$. For each Π_1 in Π there are finitely many possibilities of crossing out identities. Thus, the number of subtrees of Π_0 is finite.

$\square$

Lemma 9.2 (Equation) *Assume A, B are quantifier-free formulas and $A \sim B$. There are cut-free finite proofs (hence cyclic proofs) $\Pi_{A,B} : \Gamma, A = B, A \vdash B, \Delta$ and $\Pi'_{A,B} : \Gamma, A = B, B \vdash A, \Delta$.*

Proof We define $\Pi_{A,B}$ from the identity rule $\Gamma, A = B, A \vdash A, \Delta$. If $A = B$ is the sublist of non-identical $t_1 = u_1, \ldots, t_n = u_n$, we use $=L$ for $t_1 = u_1$ if $t_1 \not\equiv u_1$, then for $t_2 = u_2$ if $t_2 \not\equiv u_2$, and so forth. In all cases if $t_i \not\equiv u_i$ we switch t_i and u_i in the first A in the right-hand side. The result is $\Gamma, A = B, A \vdash B, \Delta$. $\square$

Since we have a rule for elimination of equality, whenever we have formulas $A[a, b]$ and $a = b$ in a cut-free proof we may also have $A[b, a]$.

10 A cut-elimination algorithm for ∞-proofs

In this section we define a normalization procedure for ∞-proofs, which may destroy regularity.

We consider an ∞-proof Π having the generalized cut-free $\nu(\Pi_1, \Pi_2)$ instead of the cut-rule. We write $\Pi : \Gamma \vdash \Delta$ for: Π has conclusion $\Gamma \vdash \Delta$

We say that Π is in head-normal form when the root r at the root of Π is $\neq \nu$.

We define a cut-elimination procedure whose goal is reducing $\Pi : \Gamma \vdash \Delta$ to some $\Pi_0 : \Gamma \vdash \Delta$ in head-normal form. Then the procedure is recursively applied to the premises of r. For a generic infinite proof-tree the procedure may fail to terminate for some nodes. We prove that in the case Π has the global trace condition then $\Pi : \Gamma \vdash \Delta$ always reduces to a normal form $\Pi_0 : \Gamma \vdash \Delta$, and Π_0 has the global trace condition. However, Π may be regular and Π_0 be not regular.

When we cut $\Gamma \vdash \Delta, Su$ with $t = Sx, \mathtt{N}x, \Gamma \vdash \Delta$ we perform a substitution $[u/x]$ on the eigenvariable x. There are finitely many terms u which are witnesses of a $\mathtt{N}R$-rule in a regular proof, but in general substitutions may nest and in this case they may produce infinitely many terms. In the particular case we remove global cuts, then for any two substitutions $[u/x], [v/y]$ the terms u, v include no eigenvariables, therefore we $x, y \notin \mathtt{FV}(u)$ and our substitution cannot nest.

We may use our procedure to remove an ordinary cut: from $\Gamma_1 \vdash A, \Delta_1$ and $A, \Gamma_2 \vdash \Delta_2$ deduce $\Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2$. Since $A \sim A$, we first deduce deduce $A = A, \Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2$, we remove cuts, then we cut all identities in $A = A$ and we obtain a cut-free cyclic proof of $\Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2$.

Assume the last rule r of Π is $\neq \nu$. Then we recursively reduce all premises of r (if any). If there is no assumption then the procedure termine. Thus, whenever we obtain a finite cut-free proof the procedure terminate.

Assume $\Pi = \nu(\Pi_1, \Pi_2)$ with $\Pi_1 : \Gamma_1 \vdash \Delta_1, C$ and $\Pi_2 : C, \Gamma_2 \vdash \Delta_2$ and c is the first connective of C.

Assume that for $i = 1, 2$ we have $\Pi_i = r_i(\{\Pi_{i,j} | j < a_i\})$ for some r_i of arity a_i. If $r_1 = \nu$ we reduce on Π_1. If $r_1 = \mathtt{sub}$ we apply substitution on the unique assumption of the rule. Assume $r_1 \neq \nu, \mathtt{sub}$. If $r_1 = \mathtt{id}$ then $\Pi \rightsquigarrow \mathtt{Weak}(\Pi_2)$. Assume $r_1 \neq \nu, \mathtt{sub}, \mathtt{id}$. If r_1 does not infer C we move r_1 outside ν: then $\Pi \rightsquigarrow r_1(\{\nu(\Pi_{i,j}, \Pi_2) | j < a_i\})$. Assume r_1 infers C. If $r_1 = \mathtt{Weak}$ then $\Pi \rightsquigarrow \mathtt{Weak}(r_1)$. Assume r_1 infers C and $r_1 \neq \nu, \mathtt{sub}, \mathtt{id}, \mathtt{Weak}$.

If $r_2 = \nu$ we reduce on Π_2. If $r_2 = \mathtt{sub}$ we apply substitution on the unique assumption of the rule. If $r_2 = \mathtt{id}$ then $\Pi \rightsquigarrow \mathtt{Weak}(\Pi_1)$. Assume $r_2 \neq \nu, \mathtt{sub}, \mathtt{id}$. Assume r_2 does not infer C. We move r_2 outside ν: then $\Pi \rightsquigarrow r_2(\{\nu(\Pi_1, \Pi_{2,j}) | j \leq a_i\})$. Assume r_2 infers C. If $r_2 = \mathtt{Weak}$ then $\Pi \rightsquigarrow r_2$. Assume r_2 infers C and $r_2 \neq \nu, \mathtt{sub}, \mathtt{id}, \mathtt{Weak}$. In this case we perform a mix reduction, according to the value of the outermost connective c.

Assume $c \equiv \vee, \wedge, \rightarrow$. We consider as example the case $c \equiv \vee$. In this case $C = C_1 \vee C_2$ and Π_1 has a unique assumption $\Pi_{1,1}$ inferring $\Gamma \vdash \Delta, C_j$ for some j, while Π_2 has two assumption, with each $\Pi_{2,j}$ inferring $C_j, \Gamma \vdash \Delta$ for $y = 1, 2$. Then $\Pi \rightsquigarrow \nu(\Pi'_1, \Pi'_2)$, with $\Pi'_1 = \nu(\Pi_{1,1}, \Pi_2)$ and $\Pi'_2 = \nu(\Pi_1, \Pi_{2,j})$.

Assume c is some atomic predicate. We distinguish three sets of atomic predicates: logical ($p(\vec{t})$), equality ($=$), and inductively defined predicates.

Assume c is a logical predicate: then $A = p(\vec{t})$ and $B = p(\vec{u})$. This is the only case in which we need the assumption $A = B$. Then $\Pi_1, \Pi_2 \rightsquigarrow \mathtt{id}$ and $\Pi \rightsquigarrow \Pi_0$, a proof of $A = B, A, \Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2, B$.

Assume c is the equality predicate. Then $\Pi_1 \rightsquigarrow {=}R : \Gamma \vdash \Delta.t = t$ and $\Pi_2 \rightsquigarrow {=}L(\Pi_2')$. In this case, the rule ${=}L$ deduces $u = v, \Gamma_2[u, v] \vdash \Delta_2[u, v]$ from $\Gamma_2[v, u] \vdash \Delta_2[v, u]$. We set $\Pi \rightsquigarrow {=}R({=}R(\Pi_2)) : t = u, t = v, \Gamma_2[u, v] \vdash \Delta_2[u, v]$.

Assume c is an inductively defined predicate: the example is $c \equiv \mathtt{N}$. Assume $\Pi_1 = \mathtt{N}R(\Pi_{1,1}) : \Gamma_1 \vdash \Delta_1, \mathtt{N}Su$ and $\Pi_2 = \mathtt{N}L(\Pi_{2,1}, \Pi_{2,2}) : \mathtt{N}t, \Gamma_2 \vdash \Delta_2$, with $\Pi_{1,1} : \Gamma_1 \vdash \Delta_1, \mathtt{N}u$ and $\Pi_{2,1} : t = 0, \Gamma_2 \vdash \Delta_2$ and $\Pi_{2,2} : t = Sx, \mathtt{N}x, \Gamma_2 \vdash \Delta_2$. Then $\Pi \rightsquigarrow {=}L(\nu(\Pi_{1,1}, [u/x]\Pi_{2,2}))$, where:

1. $[u/x]\Pi_{2,2} : t = Su, \mathtt{N}u, \Gamma_2 \vdash \Delta_2$
2. $\nu(\Pi_{1,1}, [u/x]\Pi_{2,2}) : t = Su, \Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2$
3. ${=}L(\nu(\Pi_{1,1}, [u/x]\Pi_{2,2})) : Su = t, \Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2$ is the required conclusion.

Theorem 10.1 (Cut-elimination for ∞-proofs) *If Π is an ∞-proof then Π eventually reduces to some cut-free ∞-proof Π_0.*

Proof Let Π_0 be the limit of the reduction process, defined as the set of nodes which eventually stop changing.

1. We prove that Π_0 is well-defined and cutfree. If all nodes of Π_0 are defined and are cut-free we are done. Assume this is not the case. If some node is undefined then some cut reduces to itself infinitely many times, and there is some node equal to a cut. Thus, some node of Π_0 is a cut. Take any cut-node α and the leftmost path π_0 in Π_0 from α. Either π_0 is infinite, or π_0 stops. In the first case we set $\pi = \pi_0$. In the second case, π_0 stops in a cut $\nu(\Pi_1, \Pi_2)$ reducing to itself infinitely many times. Thus, there is some trace τ_1 of the cut-formula of Π_1 passing infinitely many times through a main formula. Let π_1 be the path including τ. We set $\pi = \pi_1 @ \pi_2$. π is infinite, by the global trace condition we have an infinitely progressing trace τ in π.

   We claim that this cannot be. Let $p(\vec{t})$ be the inductive formula which is the element of τ. There are two possibilities: $p(\vec{t})$ is an ancestor of a formula in α or $p(\vec{t})$ is an ancestor of a formula in some cut above α.

   (a) Assume that $p(\vec{t})$ is an ancestor of a formula in α. Then either the cut in α would be replaced by the introduction rule of $p(\vec{t})$, or all progress points of τ would be removed while removing some cut. This is impossible because removing a cut may remove at most a finite prefix of τ

(b) Assume $p(\vec{t})$ is an ancestor of a cut formula above α. $p(\vec{t})$ is a formula in the left-hand-side, therefore $p(\vec{t})$ would be an ancestor of the cut-formula in the second premise of a cut. If the first premise reduces infinitely many times and π should take the first premise of the cut, while τ is in the second premise, contradiction. If the first premise stabilizes to a cut, then π should take the first premise of the cut, while τ is in the second premise, contradiction. If the first premise stabilizes to an introduction rule for the cut-formula, then the cut would remove a finite premix of τ and then stabilize, contradiction because τ is infinite.

Thus, Π_0 is cut-free.

2. We prove that Π_0 satisfies the global trace condition. Take any infinite path π_0 in Π_0. Then π_0 is the subsequence of some infinite path π in Π. π has some infinitely progressing trace τ. Removing a cut may remove at most a finite prefix of τ, therefore there is some infinitely progressing trace τ_1 in π_1.

We claim that in the case Π is a cyclic proof and all cuts of Π are global then the normal form of Π is a cyclic proof. We prove that the tree of cuts generated by the reduction process has only finitely many possible values. Indeed, this tree has leaves which are subformulas of Π with applied some substitution from a finite set, and this tree has an upper bound to its heigh. By regularity, there is a maximum number k of steps before a progress point from any point of Π. There is a maximum number h of steps before finding a trace progressing $k + 1$ times. When a branch goes definitely to the left it may have at most k more steps. Any branch has at most h steps. Thus the tree is finite. Each subtree of the normal form is obtained from one state of the reduction process, hence the normal form has finitely many subtrees.

References

[1] On the logical complexity of cyclic arithmetic, Anupam Das, unpublished draft. `http://www.anupamdas.com/wp/log-comp-cyc-arith/`

[2] Bellantoni, S. and Cook, S. A new recursion-theoretic characterization of the polytime functions, in: Computational Complexity (1992) 2: 97. `https://doi.org/10.1007/BF01201998`

[3] Berardi, Stefano and Tatsuta, Makoto. Classical system of Martin-Löf's inductive definitions is not equivalent to cyclic proof system. FOSSACS 2017, p. 301-317.

[4] Berardi, Stefano and Tatsuta, Makoto. Equivalence of inductive definitions and cyclic proofs under arithmetic. LICS 2017, p. 1-12.

[5] Brotherston, James (2006). Sequent calculus proof systems for inductive definitions, phd. thesis, Laboratory for Foundations of Computer Science, School of Informatics, University of Edinburgh.

[6] Buss, Samuel R. Handbook of proof theory, volume 137. Elsevier, 1998

[7] Simpson, Alex. Cyclic Arithmetic is equivalent to Peano Arithmetic. FOSSACS 2017, p. 283-300.

11 Appendix 1. The strength of the quantifier-free fragment of cyclic proofs

In this section we describe which formulas may be interpreted by inductive predicates and quantifier-free formulas in cyclic proofs.

Definable inductive predicates in Martin-Löf theory inductive definitions are exactly the Σ^0_1-predicates. Indeed, it is immediate that all inductive predicates are Σ^0_1-predicates. We prove that every Σ^0_1-predicate is inductively definable. If f is any primitive recursive n-ary map, then $f(\vec{x}) = y$ is inductively definable as some predicate of arity $n{+}1$, which we denote as $f(\vec{x}], y)$. Indeed, $f(\vec{x}) = 0$ is inductively definable by the clause $f(\vec{x}], 0)$, and $f(\vec{x}) = x_i$ by the clause $f(\vec{x}], x_i)$, and $f(\vec{x}) = Sx_i$ by the clause $f(\vec{x}, Sx_i)$. If $f(\vec{x}) = y$ and $g(\vec{x}, y) = z$ are inductive then $h(\vec{x}) = g(\vec{x}, f(\vec{x}))$ is definable by the clause: if $f(\vec{x}, y)$ and $g(\vec{x}, y, z)$ then $h(\vec{x}, z)$. If $f(\vec{x}) = y$ and $g(\vec{x}, y, n) = z$ are inductive then we may define $h(\vec{x}, 0) = f(\vec{x})$, $h(\vec{x}, n+1) = g(\vec{x}, h(\vec{x}, n), n)$. h is definable by the clauses: if$f(\vec{x}, y)$ then $h(\vec{x}, 0, y)$ and if $h(\vec{x}, n, y)$ and $g(\vec{x}, y, n, z)$ then $h(\vec{x}, n+1, z)$. Any Σ^0_1-predicate $p(\vec{x})$ is definable by $\exists x. f(\vec{x}, x) = 0$, therefore by the clause: if $f(\vec{x}, x, 0)$ then $p(\vec{x})$.

All totality statements $t(\vec{x})$ for primitive recursive maps $f(\vec{x})$ are expressible by the clause: if $f(\vec{x}, y)$ then $t(\vec{x})$. For any primitive recursive map $f(\vec{x})$ we may prove $\mathtt{N}(x_1), \ldots, \mathtt{N}(x_n) \vdash t(\vec{x})$ by induction. If we assume that successor is injective and never zero, we may prove all axioms of Robinson arithmetic. Thus, the quantifier-free fragment of Martin-Löf contains I-Σ^0_1-arithmetic.

12 Appendix 2. Robinson's arithmetic in cyclic proofs

In this section we explain how to interpret Robinson's axioms thorugh inductive definitions. As a consequence, connective-free cyclic proofs are far more expressive than we expect, they prove the same theorems without alternating quantifiers as Arithmetic with Σ^0_2-induction. In particular, they prove the consistency of arithmetic with Σ^0_2-induction, and this theorem has no cut-free proof.

We consider as inductive definitions exactly all *"productions" defined in Brotherston thesis*, Def. 2.2.1, p. 27. We define an inductive predicate $d(x,y)$ for "x,y are different integers", as follows: $d(0,Sy)$ and $d(Sx,0)$ and if $d(x,y)$ then $d(Sx,Sy)$. Using $d(x,y)$ we may define the *negation* of the $0,S$-axioms and of the axiom for $+,*$. We define: if $0 = Sx$ then Z, and if $Sx = Sy$ and $d(x,y)$ then S. Then $\neg Z$ is equivalent to $\forall x.0 \neq Sx$ and $\neg S$ is equivalent to $\forall x.\neg(Sx = Sy \wedge d(x,y))$. We claim that this is a way of stating injectivity of successor.

By $\mathtt{N}L$ we may prove $\vdash t = u, d(t,u)$ from $\vdash d(0,Sy)$ and $\vdash d(Sx,0)$ and $\vdash 0 = 0$ and $\vdash x = y, d(x,y)$ for any $x,y \not\in \mathtt{FV}(t,u)$. The first three sequents are axioms and in the forth one both $\mathtt{N}t$ and $\mathtt{N}u$ progress. This is a cyclic proof.

Using rule dL twice and weakening, we prove that $x = y, d(x,y) \vdash Z, S$ is a consequence of $Sx = 0 \vdash Z$ and $0 = Sy \vdash Z$ and $Sx = Sy, d(x,y) \vdash S$. All these sequents are axioms.

Besides, we may prove $\vdash 0 \neq Sx, Z$ and $Sx = Sy \to x = y, S$. Thus, we derive $\vdash (x \not{y}) \leftrightarrow d(x,y), Z, S$.

If we interpret $\Gamma \vdash \Delta$ as $\Gamma \vdash \Delta, Z, S$ then zero and successor axioms are derivable. We may complete the interpretation of Robinson's arithmetic of the base and the inductive case of the definition of $+$ and $*$. We express their negations. The original axioms are: $x + 0 = x$ and $x + Sy = S(x + y)$ and $x* = x$ and $x * Sy = (x * y) + y$. Their negations are expressed as follow: if $d(x + 0, x)$ then $Z+$, if $d(x + Sy, S(x + y))$ then $S+$, if $d(x * 0, 0)$ then $Z*$, if $d(x * Sy, x * y + x)$ then $S*$. Let $\Xi = Z, S, Z+, S+, Z*, S*$: this is the list of negations of 6 Robinson's axiom. The only Robinson's axioms missing is expressed by the rule $\mathtt{N}L$. Thus we interpret $\Gamma \vdash \Delta$ as $\Gamma \vdash \Delta, \Xi$: in this way all Robinson's axioms are derivable.

We conjecture:

1. the quantifier-free fragment of `LKID` with Robinson's axioms is equivalent to I-Σ^0_2-arithmetic.

2. the cut-free and quantifier-free fragment of $\mathtt{CLKID}^{\omega}$ with Robinson's axioms is equivalent to polynomial arithmetic.

The reason is the same in both cases: we may express Σ^0_1-formulas of arithmetic (with the inductive predicate $\mathtt{N}$ and $0, S, +, *$) through quantifier-free formulas of LKID (with all inductive definitions).

13 Appendix 3. Proofs with cyclic context

Assume L is a language without function symbols: L consists of logical predicates, constants and inductive predicates defined out of them. We are looking for a set of ∞-proofs including cyclic proofs for the language L. This set should have cut-elimination and should be described by finite automata. Cyclic proofs for L have no cut-elimination: we checked that there are algorithm requiring non-constant space which may be proved terminating by a cyclic proof with cuts, and no cyclic proof without cuts.

Cyclic proofs have finitely many context. We define *proofs with cyclic context*, in which contexts are inductively defined using two operations: concatenation of contexts and creation of fresh variables. We inductively define at the same time the lists of pairwise distinct variables of the context. We call these proofs: proofs with cyclic context. They are defined by finite graphs. A graph node may be the conclusion of one rule for each possible shape of the context decorating it. The unfolding of the graph may give a pseudu-proof with infinite contexts, but correct proofs

As example, we consider the canonical cut-free ∞-proof of $\mathtt{B}(x, y) \vdash \mathtt{F}(x, y)$. We prove $\mathtt{B}(x, y) \vdash \mathtt{F}(x, y)$ by $\mathtt{B}L$ with first premise $R(x, y) \vdash \mathtt{F}(x, y)$ and second premise $\mathtt{B}(x, a), R(a, y) \vdash \mathtt{F}(x, y)$ (a fresh). The first premise is proved from $R(x, y) \vdash R(x, y)$, which is proved by id. We prove the second premise $\mathtt{B}(x, a), R(a, y) \vdash \mathtt{F}(x, y)$ by $\mathtt{B}L$ with first premise $R(x, a), R(a, y) \vdash \mathtt{F}(x, y)$ and second premise $\mathtt{B}(x, b), R(b, a), R(a, y) \vdash \mathtt{F}(x, y)$ (b fresh). The first premise is proved from $R(x, a), R(a, y) \vdash R(x, a)$ (which is an id) and $R(x, a), R(a, y) \vdash \mathtt{F}(a, y)$, which is proved from $R(x, a), R(a, y) \vdash R(a, y)$ (which is an id). We prove a general version of the second premise: $\mathtt{B}(x, b), R(b, a), \Gamma[a, \vec{a}, y] \vdash \mathtt{F}(x, y)$. Here $\Gamma[a, \vec{a}, y]$ denotes a context we will inductively define. The base case is $\Gamma[a, \vec{a}, y] = R(a, y)$ and $\vec{a} = \mathtt{nil}$. The base case covers $\mathtt{B}(x, b), R(b, a), R(a, y) \vdash \mathtt{F}(x, y)$. We prove $\mathtt{B}(x, b), R(b, a), \Gamma[a, \vec{a}, y] \vdash \mathtt{F}(x, y)$ by $\mathtt{B}L$ with the following premises.

1. *First premise:* $R(x, b), R(b, a), \Gamma[a, \vec{a}, y] \vdash \mathtt{F}(x, y)$. We prove it by $\mathtt{F}R$ with first premise $R(x, b), R(b, a), \Gamma[a, \vec{a}, y] \vdash R(x, b)$ (which is an id-rule) and $R(x, b), R(b, a), \Gamma[a, \vec{a}, y] \vdash \mathtt{F}(b, y)$, which we prove by Weak

and $R(b,a), \Gamma[a,\vec{a},y] \vdash \mathtt{F}(b,y)$. Here we loop. If $R(b,a), \Gamma[a,\vec{a},y] = R(b,a), R(a,y)$, then we already considered the case. If $R(b,a), \Gamma[a,\vec{a},y] = R(b,a), R(a,c), \Gamma[\vec{a},y]$, then $R(b,a), R(a,c), \Gamma[\vec{a},y] \vdash \mathtt{F}(b,y)$ is a renaming by $[b/x, a/b, c/a]$ of $R(x,b), R(b,a), \Gamma[\vec{a},y] \vdash \mathtt{F}(x,y)$, which we already considered. Fresh variables are supposed to be pairwise distinct, hence $\Gamma[\vec{a},y][b/x, a/b, c/a] \equiv \Gamma[\vec{a},y]$.

2. *Second premise:* $\mathtt{B}(x,c), R(c,b), R(b,a), \Gamma[a,\vec{a},y] \vdash \mathtt{F}(x,y)$. This is an instance of $\mathtt{B}(x,c), R(c,b), \Gamma[b,a,\vec{a},y] \vdash \mathtt{F}(x,y)$, which is an instance of $\mathtt{B}(x,c), R(c,b), \Gamma[b,\vec{b},y] \vdash \mathtt{F}(x,y)$, hence a renaming of the root $\mathtt{B}(x,b), R(b,a), \Gamma[a,\vec{a},y] \vdash \mathtt{F}(x,y)$. We loop.

We have a notion of global trace condition for proofs with cyclic contexts. We ask that in each infinite path π, either there is a trace of the inductive definition of some context which is infinitely progressing, or there is a trace of some inductively defined predicate which is infinitely progressing.

We prove the global trace condition for the unfolding of the proof-tree Π we just defined. Take any path π in Π. Either π chooses the first premise of at least one $\mathtt{B}L$-rule, or π always chooses the second premise. In the first case the left-hand side of the sequent in π reduces by one at each step in π, therefore π is finite. In the second case π is the rightmost path in the proof-tree. At each step the unique assumption $\mathtt{B}(x,y)$ progresses, therefore if π is infinite there is some infinitely progressing trace in π.

The same argument saying that cut-free cyclic proofs may only derive the convergence of polynomial-time algorithms works for proofs with cyclic contexts. Instead, proofs with cyclic contexts are not limited to constant space algorithms, because for such proofs the contexts may be of any size.

In order to add function symbols to the language L, we should consider cyclic contexts and terms. We have inductive definitions of the proof-tree, of the contexts, and of the terms. This means that contexts and terms could be infinite, but are not infinite in correct proofs. Also in this case, 2-Ramsey theorem may be used to prove soundness for this notion of proof. Assume we forbid inductive definitions discarding variables in L. Then we conjecture: the set of algorithms we may prove convergent with cyclic contexts and term and cut-free proofs is the set of primitive recursive algorithms.