Cyclic Arithmetic (in context)

Alex Simpson

LFCS, School of Informatics
University of Edinburgh, UK
Irrationality of $\sqrt{2}$ — proof by \textit{descente infinie}

To prove: $\forall x, y \in \mathbb{N}. \ x > 0 \Rightarrow x^2 \neq 2y^2$.

Proof.

Suppose $x_0^2 = 2x_1^2$ where $x_0 > 0$  

N.B., it follows that $x_0 > x_1 > 0$

Then $\exists x_2. \ x_0 = 2x_2$ since 2 is a prime factor of $x_0^2$ hence of $x_0$

So $4x_2^2 = 2x_1^2$

i.e., $x_1^2 = 2x_2^2$

By repeating argument, we produce an infinite sequence $x_0 > x_1 > x_2 \ldots$ of numbers all $> 0$.

There is no such sequence. 

#
Naïve analysis of proof

The proof applies the Principle of Infinite Descent (PID)

\[(\forall n. (Q(n) \Rightarrow \exists m < n. Q(m))) \Rightarrow \neg Q(x)\]

which (in classical logic) is equivalent to complete induction

\[(\forall n. (\forall m < n. P(m)) \Rightarrow P(n)) \Rightarrow P(x)\]

which is in turn derivable as a consequence of simple induction

\[P(0) \land (\forall n. P(n) \Rightarrow P(n + 1)) \Rightarrow P(x)\]

(Conversely, complete induction trivially implies simple induction.)
Infinite proofs by infinite descent

So is proof by infinite descent just proof by induction?

A more general view is to consider a proof by infinite descent as an infinite proof, in which the full proof involves the entire construction of the infinite sequence.

What we have written down is a finite representation of this infinite proof.

There might then be other (more complex) infinite proofs by infinite descent whose underlying finite “pattern” is not given so simply as an instance of induction via PID.
Irrationality of $\sqrt{2}$ — infinite formal proof

\[
\begin{align*}
0 &< x_0, \ x_0^2 = 2x_1^2 \implies 0 < x_1 < x_0 \land \exists x_2. x_0 = 2x_2 \\
0 &< x_0, \ x_0^2 = 2x_1^2 \implies x_1 < x_0, \ 0 < x_1, \ 4x_2^2 = 2x_1^2 \implies (\text{Cut})
\end{align*}
\]

The infinite proof contains one infinite branch. Along this branch there occurs a sequence of terms (in fact variables)

\[x_0, \ x_1, \ x_2, \ldots\]

and an infinite sequence of left-hand-side sequent formulas

\[x_1 < x_0 \quad x_2 < x_1 \quad x_3 < x_2 \quad x_4 < x_3 \quad \ldots\]
Totality of Ackermann’s function

\[ A(0,n) = n + 1 \]
\[ A(m,0) = A(m-1,1) \quad m > 0 \]
\[ A(m,n) = A(m-1,A(m,n-1)) \quad m, n > 0 \]
Totality of Ackermann’s function

\[ A(m, n, r) \iff (m = 0 \land r = n + 1) \]
\[ \lor (m > 0, n = 0 \land A(m - 1, 1, r)) \]
\[ \lor (m, n > 0 \land \exists s. A(m, n - 1, s) \land A(m - 1, s, r)) \]
Totality of Ackermann’s function

\[ A(m, n, r) \iff (m = 0 \land r = n + 1) \]
\[ \lor (m > 0, n = 0 \land A(m - 1, 1, r)) \]
\[ \lor (m, n > 0 \land \exists s. A(m, n - 1, s) \land A(m - 1, s, r)) \]
Totality of Ackermann’s function

If an infinite path goes through (A) or (C) infinitely often, then there is an infinite sequence \( m, m-1, m-2, \ldots \).

Otherwise, eventually path runs through (B) only, in which case there is an infinite sequence \( n, n-1, n-2, \ldots \).
A formal system for infinite descent

First-order language for arithmetic, with terms $0, s(t), t + u, t \times u$, with equality $t = u$ and strict order relation $t < u$.

Sequents $\Gamma \Longrightarrow \Delta$, with $\Gamma, \Delta$ finite sets of formulas.

Standard sequent calculus rules for first-order classical logic with equality, including

$$
\frac{\Gamma \Longrightarrow A, \Delta \quad \Gamma, A \Longrightarrow \Delta}{\Gamma \Longrightarrow \Delta} \quad (\text{Cut})
$$

$$
\frac{\Gamma \Longrightarrow \Delta}{\Gamma[\theta] \Longrightarrow \Delta[\theta]} \quad (\text{Subst})
$$

The axioms and rule from the next slide.
$t < u, u < v \Rightarrow t < v$

$t < u, u < t \Rightarrow$

$\quad \Rightarrow t < u, t = u, u < t$

$\quad \Rightarrow 0 = t, 0 < t$

$t < u \Rightarrow s(t) < s(u)$

$\quad \Rightarrow t < s(t)$

$t < u, u < s(t) \Rightarrow$

$\quad \Rightarrow t + 0 = t$

$\quad \Rightarrow t + s(u) = s(t + u)$

$\quad \Rightarrow t \times 0 = 0$

$\quad \Rightarrow t \times s(u) = t + (t \times u)$

$\Gamma, t = s(x) \Rightarrow \Delta \quad x$ fresh

$\Gamma, 0 < t \Rightarrow \Delta$
Definition of $\infty$-proof

An $\infty$-proof is a possibly infinite tree of rule applications that satisfies the following soundness condition

(SC) Along every infinite branch $(\Gamma_i \implies \Delta_i)_i$, for some $N \geq 0$, there exists a sequence of terms $(t_i)_{i \geq N}$, the trace, such that, $\forall i \geq N$,

$$t_i = \theta_i(t_{i+1}) \text{ or } (\theta_i(t_{i+1}) = t_i) \in \Gamma_i \text{ or } (\theta_i(t_{i+1}) < t_i) \in \Gamma_i,$$

where, if the $(i+1)$-th rule along the path (which has conclusion $\Gamma_i \implies \Delta_i$) is a (Subst) rule, then $\theta_i$ is the substitution used in the rule application, otherwise $\theta_i$ is the identity function.

Furthermore, $(\theta_i(t_{i+1}) < t_i) \in \Gamma_i$ holds (the trace progresses) at infinitely many $i$.

N.B., $\infty$-proofs are finitely-branching non-well-founded trees
Soundness theorem

Theorem. If a sequent $\Gamma \implies \Delta$ has an $\infty$-proof then it is true.

Proof sketch. Suppose $\Gamma \implies \Delta$ is false under some interpretation of its free variables.

The local soundness of the inference rule produces an infinite branch through the $\infty$-proof of $\Gamma \implies \Delta$ such that every sequent $\Gamma_i \implies \Delta_i$ along the branch is false under an induced interpretation $\rho_i$ of its free variables.

Condition (SC) produces a sequence of terms $(t_i)_{i \geq N}$ along the infinite branch such that, for every $i \geq N$, either $\rho_i(t_1) = \rho_{i+1}(t_{i+1})$ or $\rho_i(t_1) > \rho_{i+1}(t_{i+1})$. Moreover, the latter holds infinitely often. #
Completeness theorem

Theorem. If $\Gamma \vdash \Delta$ is a true sequent then it has an $\infty$-proof without (Subst) and using only atomic applications of (Cut).

Proof idea. Simulate the sequent calculus $\omega$-rule.

\[
\begin{align*}
\Gamma[s(0)] & \vdash \Delta[s(0)] & x_2 > 0, \Gamma[s(s(x_2))] & \vdash \Delta[s(s(x_2))] \\
x_2 < x_1, \Gamma[s(s(x_2))] & \vdash \Delta[s(s(x_2))] \\
\Gamma[s(s(0))] & \vdash \Delta[s(s(0))] & x_1 = s(x_2), \Gamma[s(x_1)] & \vdash \Delta[s(x_1)] \\
x_1 > 0, \Gamma[s(x_1)] & \vdash \Delta[s(x_1)] \\
x_1 < t, \Gamma[s(x_1)] & \vdash \Delta[s(x_1)] & t = s(x_1), \Gamma[t] & \vdash \Delta[t] \\
t = 0, \Gamma[t] & \vdash \Delta[t] & t > 0, \Gamma[t] & \vdash \Delta[t] \\
\Gamma[t] & \vdash \Delta[t]
\end{align*}
\]
Digression: a proof-theoretic project

It should be possible to give a syntactic proof of the eliminability of (Subst) and non-atomic instances of (Cut) from $\infty$-proofs.

This should be achievable using Mints’ continuous cut elimination.

The novelty compared with other applications of continuous cut elimination would be to show that the soundness condition (SC) is preserved under cut elimination.

(In standard applications of continuous cut elimination, e.g., to $\omega$-proofs, one instead shows that well-foundedness is preserved by cut elimination.)
Irrationality of $\sqrt{2}$ — regular infinite proof

\[
\begin{align*}
\vdots & \\
0 < x_0, x_0^2 = 2x_1^2 & \rightarrow 0 < x_1 < x_0 \land \exists x_2. x_0 = 2x_2 \\
0 < x_1, x_1^2 = 2x_2^2 & \Rightarrow \\
0 < x_0, x_0^2 = 2x_1^2 & \Rightarrow \\
x_1 < x_0, 0 < x_1, 4x_2^2 = 2x_1^2 & \Rightarrow \\
\end{align*}
\]

The infinite proof contains one infinite branch. Along this branch we have the trace

\[x_0, x_0, x_1, x_0, x_0, x_1, x_0, x_0, x_1, \ldots\]

which progresses infinitely often via

\[x_1 < x_0 \quad x_1 < x_0 \quad x_1 < x_0 \quad x_1 < x_0 \quad \ldots\]
Totality of Ackermann’s function: regular infinite proof

\[
\begin{align*}
m = 0 & \implies A(m,n,n+1) \\
m > 0, n = 0 & \implies \exists r. A(m,n,r) \\
m > 0, n > 0 & \implies \exists r. A(m,n,r) \\
m > 0 & \implies \exists s.A(m,n,s) \\
m > 0 & \implies \exists r. A(m,n,r) \\
\end{align*}
\]
Regular $\infty$-proofs (a.k.a. circular/cyclic proofs)

An infinite tree is regular if it has only finitely many distinct subtrees. Equivalently, a regular tree is a tree that is generated by a finite directed (cyclic) graph

A regular $\infty$-proof is an $\infty$-proof whose proof tree is regular.

Regular $\infty$-proofs correspond to finitely presented proofs by infinite descent. They form an effective proof system because:

**Proposition.** The soundness condition (SC) is decidable over regular proof trees, presented as finite directed graphs.

**Proof method.** This follows from the theory of Büchi automata. One can show that (SC) is an $\omega$-regular property.

**Corollary.** Regular $\infty$-proofs are not complete for establishing truth.
Comparing $\infty$-proofs and $\omega$-proofs

$\infty$-proofs are finitely-branching non-well-founded trees
$\omega$-proofs are infinitely-branching well-founded trees

$\infty$-provability coincides with truth coincides with $\omega$-provability

Regular $\infty$-proof is finitary counterpart of $\infty$-proof.
Proof by induction is finitary counterpart of $\omega$-proof.

The main result of the talk is:

regular $\infty$-provability = provability by induction
Informal statement of main result:

regular proof by infinite descent = proof by induction

Regular $\infty$-proofs provide a formal system of cyclic proofs for statements of arithmetic.

We therefore call the resulting theory of regular-$\infty$-provable sentences Cyclic Arithmetic.

Formally, our main result is that

Cyclic Arithmetic = Peano Arithmetic
Main theorem, precise statement

**Theorem.** A sequent $\Gamma \Rightarrow \Delta$ has a regular $\infty$-proof if and only if the implication $\land \Gamma \Rightarrow \lor \Delta$ is provable in Peano Arithmetic (PA).
Main theorem, formally

Theorem. A sequent $\Gamma \Rightarrow \Delta$ has a regular $\infty$-proof if and only if the implication $\bigwedge \Gamma \Rightarrow \bigvee \Delta$ is provable in Peano Arithmetic (PA).

Proof that PA provable implies regular $\infty$-provable (cf. [BS]).
Enough to give regular $\infty$-proof for every instance of the Induction Schema of PA.

\[
\begin{align*}
A[0], \forall y. (A[y] \Rightarrow A[s(y)]) & \quad \Rightarrow \quad A[x_0] \\
A[0], \forall y. (A[y] \Rightarrow A[s(y)]) & \quad \Rightarrow \quad A[x_1] \\
x_1 < x_0, A[0], \forall y. (A[y] \Rightarrow A[s(y)]) & \quad \Rightarrow \quad A[s(x_1)] \\
x_0 = s(x_1), A[0], \forall y. (A[y] \Rightarrow A[s(y)]) & \quad \Rightarrow \quad A[x_0] \\
x_0 = 0, A[0] & \quad \Rightarrow \quad A[x_0] \\
x_0 > 0, A[0], \forall y. (A[y] \Rightarrow A[s(y)]) & \quad \Rightarrow \quad A[x_0] \\
A[0], \forall y. (A[y] \Rightarrow A[s(y)]) & \quad \Rightarrow \quad A[x_0]
\end{align*}
\]
Towards proof of converse

Lemma 1. If $G$ is a finite graph representing a regular $\infty$-proof $\Pi_G$ then $\text{ACA}_0$ proves “$\Pi_G$ satisfies (SC)”.

Proof outline. There exists a B"uchi-automaton $M$ whose emptiness witnesses that $\Pi_G$ satisfies (SC). Via a formalization of B"uchi’s complementation theorem, $\text{ACA}_0$ proves “$M$ empty implies $\Pi_G$ satisfies (SC)”. And, trivially, $\text{ACA}_0$ proves “$M$ empty”. □

Lemma 2. For every $n \geq 0$, $\text{ACA}_0$ proves “if $\Pi$ is an $\infty$-proof of $\Gamma \implies \Delta$, containing formulas of complexity at most $\Sigma^0_n$, then, for any assignment of numbers to free variables, the formula $\land \Gamma \implies \lor \Delta$ is $\Sigma^0_n$-true”.

Proof. The soundness proof for $\infty$-proofs is directly formalizable. □

(N.B., the restriction to $\Sigma^0_n$ formulas is needed for the truth predicate to be expressible.)
Proof that regular $\infty$-provable implies PA provable.

Suppose $G$ is a finite graph representing a regular $\infty$-proof $\Pi_G$ with conclusion $\Gamma \implies \Delta$.

Let $n$ be such that every formula in $G$ is at most $\Sigma_0^n$.

By Lemma 1, ACA$_0$ proves “$\Pi_G$ satisfies (SC)”.

By Lemma 2, ACA$_0$ proves “for any assignment to free variables, the formula $\land \Gamma \implies \lor \Delta$ is $\Sigma_0^n$-true”.

By the reflection property of the $\Sigma_0^n$-truth predicate, ACA$_0$ proves $\land \Gamma \implies \lor \Delta$.

But ACA$_0$ is conservative over PA.

Hence, PA proves $\land \Gamma \implies \lor \Delta$. \qed
Open Problem. Give a direct syntactic translation from regular $\omega$-proofs to proofs in PA.

The combinatorics of this seem nontrivial.

A similar syntactic translation should be able to resolve the following conjecture.

Conjecture. Intuitionistic regular $\omega$-proofs are conservative over Heyting Arithmetic. I.e.,

\[ \text{Intuitionistic Cyclic Arithmetic} = \text{Heyting Arithmetic} \]

This is just one instance amongst many other similar questions concerning the equivalence of cyclic and inductive proofs. We now survey some of these.
First-order logic with mutual inductive definitions [BS]

Example:

\[
\begin{array}{ccc}
E(0) & E(x) & O(x) \\
O(s(x)) & E(s(x)) \\
\end{array}
\]

Conjecture [BS]. Regular $\infty$-proofs for mutual inductive definitions are conservative over proofs by mutual induction.
First-order logic with mutual inductive definitions [BS]

Example:

\[
\begin{array}{ccc}
E(0) & E(x) & O(x) \\
O(s(x)) & E(s(x)) & \\
\end{array}
\]

Conjecture [BS]. Regular $\infty$-proofs for mutual inductive definitions are conservative over proofs by mutual induction.

Conjecture. Regular $\infty$-proofs for mutual iterated inductive definitions are conservative over proofs by mutual induction.
First-order logic with mutual inductive definitions [BS]

Example:

\[
\begin{array}{ccc}
E(0) & E(x) & O(x) \\
O(s(x)) & E(s(x)) & \\
\end{array}
\]

Conjecture [BS]. Regular \(\infty\)-proofs for mutual inductive definitions are conservative over proofs by mutual induction.

Conjecture. Regular \(\infty\)-proofs for mutual iterated inductive definitions are conservative over proofs by mutual induction.

Conjecture. Regular \(\infty\)-proofs for first-order \(\mu\)-calculus are conservative over proofs by induction/coinduction.
Modal $\mu$-calculus

Analogue of regular $\infty$-proofs: the refutations of [NW 97]

It is straightforward to prove that refutations are sound and complete for establishing (in)validity [NW 97].

Analogue of proof by induction: Kozen’s Hilbert-style axiomatization for the modal $\mu$-calculus.

The reducibility of regular $\infty$-proofs to inductive proofs is thus a consequence of Walukiewicz’ completeness theorem for the modal $\mu$-calculus.

Conversely, a direct reduction from regular $\infty$-proofs to inductive proofs would provide an alternative proof of Walukiewicz’ completeness theorem.
List of questions and directions

1. Characterise logical theory given by $\Sigma^0_1$ regular proofs.
2. Give syntactic proof of non-atomic cut-elimination for $\infty$-proofs.
3. Give direct translation from regular $\infty$-proofs to proofs in PA.
4. Quantify blow-up required when translating a regular $\infty$-proof to a PA proof.
5. Are intuitionistic regular $\infty$-proofs conservative over HA?
6. Prove equivalence of regular $\infty$-proof and proof by induction for mutual (iterated) inductive definitions and first-order $\mu$-calculus.
7. Alternative proof of Walukiewicz’ completeness theorem for modal $\mu$-calculus.
8. Investigate wider classes of $\infty$-proofs with finite presentations; e.g., pushdown, generated by (higher-order) recursion schemes.
9. Cyclic proofs for probabilistic logics.
Main reference plus selected related work (chronological)


