Nondeterministic limits and certified exact real computation

Michal Konečný[1], Sewon Park[2], and Holger Thies[2]

Nineteenth International Conference on Computability and Complexity in Analysis
May 23, 2022

[1]Aston University [2]Kyoto University

Overview

1. Review the previous work (the last year CCA talk) which is
   Type theory with axiomatic real numbers extracted to Exact Real number Computation software's data type Reals
2. Review nondeterministic limit operations suggested by F. Braußе and N. Müller
3. Specify a principle called nondeterministic dependent choice and derive the nondeterministic limit operator
4. Using it, we define complex square roots and evaluate the extracted certified Haskell/AERN program
5. Conclude this talk

Constructive axiomatic structure of reals

- Constructive mathematics:

$$A \vee B \text{ is valid } \Leftrightarrow \text{deciding } A \text{ or } B \text{ is computable}$$

$$\exists(x : A).\ B(x) \text{ is valid } \Leftrightarrow \text{finding } x : A \text{ s.t. } B(x) \text{ is computable}$$

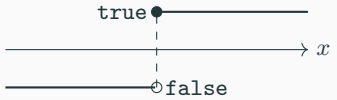
- Certified program extraction:

$$\forall(x : A).\ \exists(y : B).\ R(x, y)$$

  yields a program $\mathcal{P} : A \to B$ promised that $\forall(x : A).\ R(x, \mathcal{P}(x))$
- Classical axiomatization of reals is invalid:

$$\forall(x : \mathsf{R}).\ x \geq 0 \vee x < 0$$

  The sign function (any discontinuous function) is uncomputable



- Constructive axiomatization of reals

$$\text{proofs} \Leftrightarrow \text{programs in ERC framework (e.g., iRRAM, AERN, ARIADNE, } \cdots)$$

- CCA 2021 Talk "*From Coq proofs to certified exact real computation in AERN*":
  - Partial comparison $<$ and Nondeterminism M

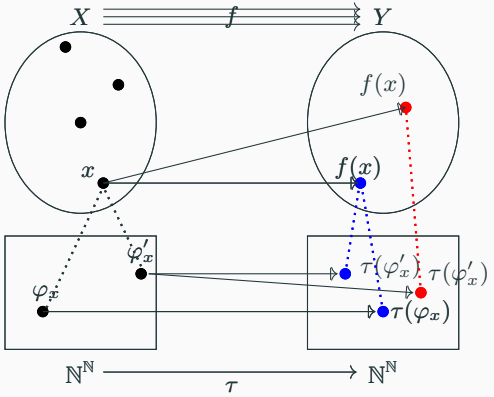
Nondeterminism

- A *representation* of X is a partial surjective function $\delta_X : \mathbb{N}^{\mathbb{N}} \rightharpoonup X$
- A function $f : X \to Y$ is *computed by* $\tau : \mathbb{N}^{\mathbb{N}} \rightharpoonup \mathbb{N}^{\mathbb{N}}$ if

$$\forall x \in X \,.\, \forall \varphi_x \in \mathbb{N}^{\mathbb{N}} \,.\, \delta_X(\varphi_x) = x \Rightarrow \delta_Y(\tau(\varphi)) = f(x)$$

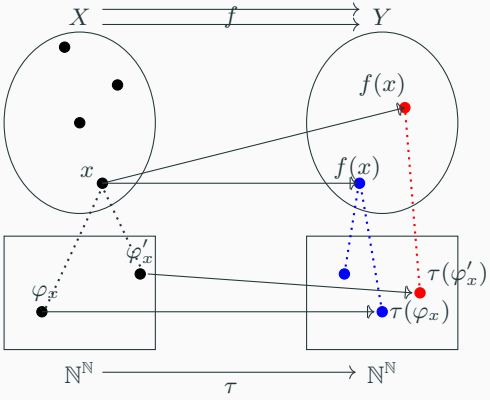
  $+, -, \times : \mathsf{R} \times \mathsf{R} \to \mathsf{R}$ computable. $<: \mathsf{R} \times \mathsf{R} \to \mathsf{bool}$ not computable
- A multi-function $f : X \rightrightarrows Y$ is *nondeterministically computed by* $\tau : \mathbb{N}^{\mathbb{N}} \rightharpoonup \mathbb{N}^{\mathbb{N}}$ if

$$\forall x \in X \,.\, \forall \varphi_x \in \mathbb{N}^{\mathbb{N}} \,.\, \delta_X(\varphi_x) = x \Rightarrow \delta_Y(\tau(\varphi)) \in f(x)$$

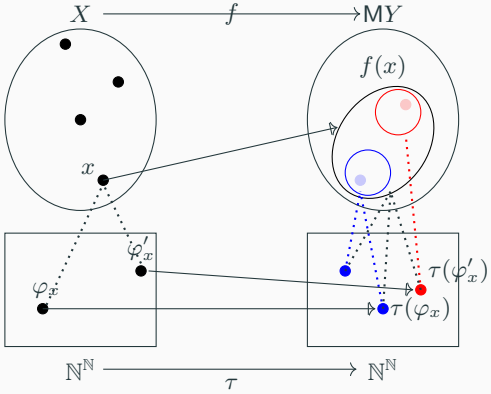


Multi-representations

- A *representation* of X is a partial surjective function $\delta_X :\subseteq \mathbb{N}^{\mathbb{N}} \to X$
- A multi-function $f : X \rightrightarrows Y$ is *nondeterministically computed by* $\tau : \mathbb{N}^{\mathbb{N}} \rightharpoonup \mathbb{N}^{\mathbb{N}}$ if $\forall x \in X\,.\,\forall \varphi_x \in \mathbb{N}^{\mathbb{N}}\,.$ $\delta_X(\varphi_x) = x \Rightarrow \delta_Y(\tau(\varphi)) \in f(x)$



- A *multi-representation* of X is a partial surjective multi-function $\delta_X :\subseteq \mathbb{N}^{\mathbb{N}} \rightrightarrows X$
- A function $f : X \to Y$ is *computed by* $\tau : \mathbb{N}^{\mathbb{N}} \rightharpoonup \mathbb{N}^{\mathbb{N}}$ if $\forall x \in X\,.\,\forall \varphi_x \in \mathbb{N}^{\mathbb{N}}\,.$ $\delta_X(\varphi_x) \ni x \Rightarrow \delta_Y(\tau(\varphi)) \ni f(x)$
- $\delta_{\mathsf{M}Y}(\varphi) = S :\Leftrightarrow \delta_Y(\varphi) \in S$



Axiomatization of reals and nondeterminism

- The category of multi-represented sets (and computable 'functions') as the model
- Axiomatize R unique up to iso. (mutli-)representation of real numbers [Hertling 99']:
  - constants $0, 1 : \mathsf{R}$
  - field operators $+, -, \times : \mathsf{R} \to \mathsf{R} \to \mathsf{R}$
  - partial mult. inversion $^{-1} : \forall x : \mathsf{R} \,.\, x \neq 0 \to \mathsf{R}$
  - Kleenean-valued order comparison $<: \mathsf{R} \to \mathsf{R} \to \mathsf{K}$
  - regular limit operation

$$\mathsf{lim} : \forall n, m \,.\, |s_n - s_m| < 2^{-n-m} \to \exists r : \mathsf{R} \,.\, \forall k \,.\, |r - s_k| < 2^{-k}$$

- Axiomatize nondeterminism monad M s.t.

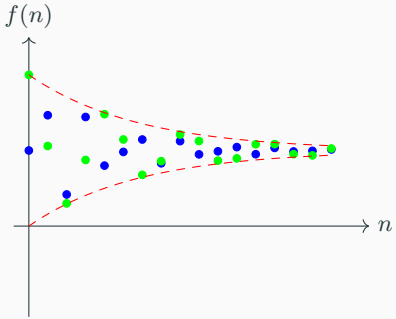
$$A \to \mathsf{M}B \Rightarrow \text{nondeterministic function from } A \text{ to } B$$

$$\mathsf{M}\,(A \vee B) \Rightarrow \text{nondeterministic decision if } A \text{ or } B$$

- E.g., soft sign: $\forall(x : \mathsf{R}).\ \mathsf{M}(x < 2^{-n} \vee x > -2^{-n})$
- Extend program extraction mapping R to `creal` in Haskell/AERN
- E.g., M is mapped to the identity monad in Haskell/AERN
- Constructive intermediate value theorem to root finding in Haskell/AERN
- Heron method to real square root in Haskell/AERN

Nondeterministic completeness

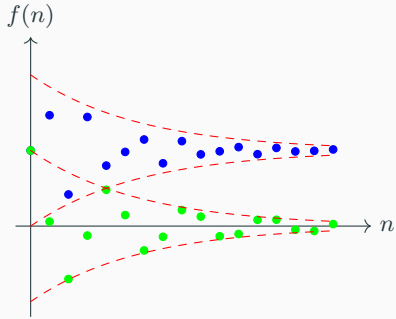
When $f : \mathsf{N} \to \mathsf{MR}$ converges to R



- Each nondeterministic section $s : \mathsf{N} \to \mathsf{R}$ of f is a regular Cauchy
- M-lifting of lim on s yields MR limits
- We get the limit point as all such limits are identical.

Reasoning on sections $s \in f$ and eliminating subsingletons $\mathsf{isSubsingleton}(X) \to \mathsf{M}X \to X$

When $f : \mathsf{N} \to \mathsf{MR}$ converges to MR

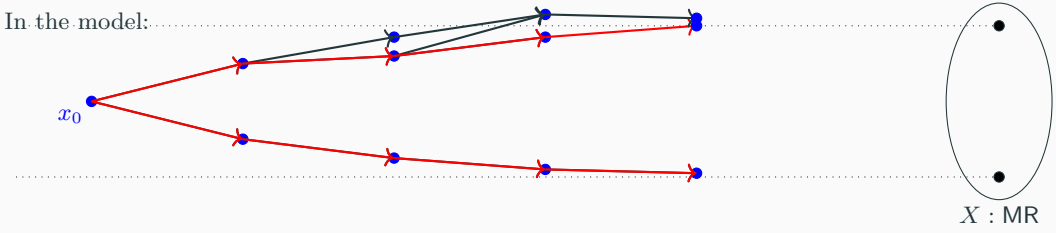


- necessary for complex roots, ...
- iRRAM's solution using discrete cache
- another approach N. Müller and F. Braße by via nondeterministic refinement
- structure of real numbers? nondeterminism? base language?

Nondeterministic refinement by F. Brauße and N .Müller

In order to construct $X : \mathsf{MR}$ via approximation,

- (**Initial Step**) compute $x_0 : \mathsf{R}$ s.t. x_0 is 2^{-0}-approximation to *one* $x \in X$
- (**Nondeterministic Refinement Step**) For each $n : \mathsf{N}$,
  given any 2^{-n} approximation $x_n : \mathsf{R}$ to *some* $x \in X$,
  nondeterministically compute x_{n+1} s.t.
  (1) x_{n+1} is a 2^{-n-1} approximation to some $x \in X$ (2) $|x_{n+1} - x_n| \leq 2^{-n-1}$.

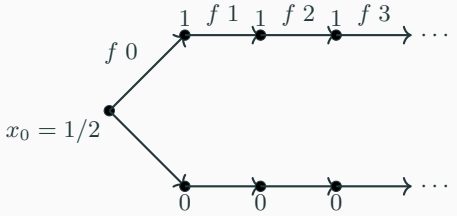


- Repeatedly applying, only one path in the tree gets *evaluated* nondeterministically
- Hence, limit point can be computed nondeterministically up to the countably many choices
- Repeating nondeterministic procedure $\Rightarrow$ nondeterministic sequence of deterministic elements with information on PATHS

Nondeterministic sequence v.s. sequence nondeterministically

Suppose

- $x_0 := 1/2$
- $f\ (n : \mathsf{N})\ (x : \mathsf{R}) := \begin{cases} 0 \text{ or } 1 \text{ nondeterministically} & \text{if } n = 0 \\ x & \text{otherwise.} \end{cases}$



- must give us $\{1/2, 0, 0, 0, 0, \cdots,\quad 1/2, 1, 1, 1, 1, \cdots\}$
- but the M-lifted primitive recursion gives us $\{1/2\} :: \{0, 1\} :: \{0, 1\} :: \{0, 1\} :: \cdots$ forgetting all information on paths.

Definition

1. Given a sequence of types $P : \mathsf{N} \to \mathsf{Type}$
2. a sequential *classical* binary relations $R\ n : (P\ n) \to (P\ (n+1)) \to \mathsf{Prop}$,
3. an initial point $x : P\ 0$ and
4. a nondeterministic successor function

$$f : \Pi(n : \mathsf{N}).\ \Pi(x : P\ n).\ \mathsf{M}\Sigma(y : P\ (n+1)).\ R\ n\ x\ y$$

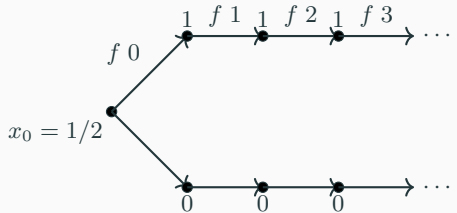
there nondeterministically is $g : \Pi(n : \mathsf{N}).\ P\ n$ such that

$$\forall(n : \mathsf{N}).\ R\ n\ (g\ n)\ (g\ (n+1))$$

and some coherence conditions

$$f\ (n : \mathsf{N})\ (x : \mathsf{R}) := \begin{cases} 0 \text{ or } 1 & \text{if } n = 0, \\ x & \text{otherwise} \end{cases}$$

$$R\ n\ x_n\ x_{n+1} :\equiv \begin{cases} x_0 = 1/2 \wedge (x_1 = 0 \vee x_1 = 1) & \text{if } n = 0, \\ x_n = x_{n+1} & \text{otherwise.} \end{cases}$$



Nondeterministic metric completeness

In order to construct $X : \mathsf{MR}$ via approximation,

- (**Initial Step**) compute $x_0 : \mathsf{R}$ s.t. x_0 is 2^{-0}-approximation to *one* $x \in X$
- (**Nondeterministic Refinement Step**) For each $n : \mathsf{N}$,
  given any 2^{-n} approximation $x_n : \mathsf{R}$ to *some* $x \in X$,
  nondeterministically compute x_{n+1} s.t.
  (1) x_{n+1} is a 2^{-n-1} approximation to some $x \in X$ (2) $|x_{n+1} - x_n| \leq 2^{-n-1}$.

Theorem

The above nondeterministic metric completeness is derivable.

Proof.

1. Define $R\ n\ x_n\ x_{n+1} :\equiv |x_{n+1} - x_n| \leq 2^{-n-1} \wedge (x_{n+1}$ is 2^{-n-1}-approximation to some $x \in X)$
2. Nondeterministic dependent choice yields $F : \mathsf{M}(\mathsf{N} \to \mathsf{R})$ such that
   - each $f \in F$ is a Cauchy sequence as for all $n : \mathsf{N}$
     $$|(f\ (n+1)) - (f\ n)| < 2^{-n-1}$$
   - each $f \in F$ and $n : \mathsf{N}$, $f(n)$ is a 2^{-n}-approximation to some $x \in X$.
3. Apply ordinary completeness yields $X : \mathsf{MR}$ limit points

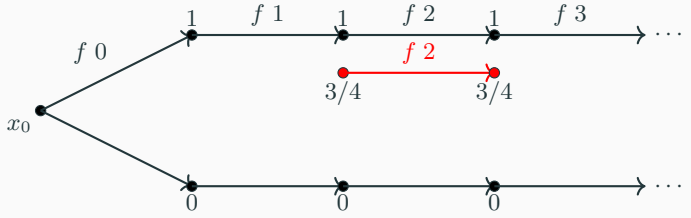
□

Overconcerned refinement

In order to construct $X : \mathsf{MR}$ via approximation,

- (**Initial Step**) compute $x_0 : \mathsf{R}$ s.t. x_0 is 2^{-0}-approximation to *one* $x \in X$
- (**Nondeterministic Refinement Step**) For each $n : \mathsf{N}$,
  given any 2^{-n} approximation $x_n : \mathsf{R}$ to *some* $x \in X$,
  nondeterministically compute x_{n+1} s.t.
  (1) x_{n+1} is a 2^{-n-1} approximation to some $x \in X$ (2) $|x_{n+1} - x_n| \leq 2^{-n-1}$.

- However $f\ n\ x := \begin{cases} 0 \text{ or } 1 & \text{if } n = 0, \\ x & \text{otherwise} \end{cases}$ is not a valid refinement for $\{0, 1\}$



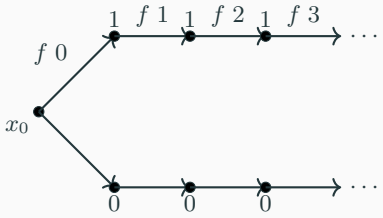
- $3/4$ is a 2^{-2}-approximation to 1
- $f\ 2\ (3/4) = 3/4$ is not a 2^{-3}-approximation to 1

Nondeterministic metric completeness with invariant

In order to construct $X : \mathsf{MR}$ via approximation,
encode refinements as an informative invariant $I : \mathsf{N} \to \mathsf{R} \to \mathsf{Type}$
($I\ n\ x_n$ is the invariant for x_n appears in n'th refinement)

- (**Initial Step**) compute (x_0, t_0) s.t. $x_0 : \mathsf{R}$ is 2^{-0}-approximation to *one* $x \in X$ and $t_0 : I\ 0\ x_0$
- (**Nondeterministic Refinement Step with Invariant**) for each $n : \mathsf{N}$
  given a 2^{-n} approximation $x_n : \mathsf{R}$ to *some* $x \in X$ and $t_n : I\ n\ x_n$,
  nondeterministically compute (x_{n+1}, t_{n+1}) such that
  (1) x_{n+1} is a 2^{-n-1}-approx of some $x \in X$, (2) $|x_{n+1} - x_n| \leq 2^{-n-1}$, (3) $t_{n+1} : I\ (n+1)\ x_{n+1}$

- $f\ n\ x := \begin{cases} 0 \text{ or } 1 & \text{if } n = 0, \\ x & \text{otherwise} \end{cases}$
- $I\ n\ x :\equiv n > 0 \to (x = 0) \vee (x = 1)$
- Each entry of refinement step $n > 0$, one can test if $x = 0$ or $x = 1$
- Each end of refinement step, one must give boolean term indicating $x = 0$ or $x = 1$



Nondeterministic approximation of complex square roots

- Complex square root $\sqrt{}: \mathbb{C} \rightrightarrows \mathbb{C}$ does not admit continuous singlevalue section
- When $|a+ib| < 2^{-2(n+2)}$, then $|\sqrt{a+ib}| < 2^{-n-1}$
- When $|a+ib| > 0$, the four cases, $\sqrt{a+ib}$ can be computed exactly, using real square roots
  - When $a > 0$: $\sqrt{a+ib} = p(a,b)$ When $a < 0$: $\sqrt{a+ib} = q(a,b)$
  - When $b > 0$: $\sqrt{a+ib} = r(a,b)$ When $b < 0$: $\sqrt{a+ib} = s(a,b)$
- Nondeterministically decidable:
  - $\mathsf{M}\big(|a+ib| < 2^{-2(n+2)} \vee |a+ib| > 0\big)$
  - $|a+ib| > 0 \to \mathsf{M}\big(a > 0 \vee a < 0 \vee b > 0 \vee b < 0\big)$

Approximate $\sqrt{a+ib}$ by 2^{-n-1}:

$$
\begin{array}{llcl}
\textbf{case} & |a+ib| < 2^{-2(n+2)} & \Rightarrow & \textbf{return } 0 \\
\| & |a+ib| > 0 & \Rightarrow & \textbf{case} \quad a > 0 \Rightarrow \textbf{return } p(a,b) \\
 & & & \quad \| \quad a < 0 \Rightarrow \textbf{return } q(a,b) \\
 & & & \quad \| \quad b > 0 \Rightarrow \textbf{return } r(a,b) \\
 & & & \quad \| \quad b < 0 \Rightarrow \textbf{return } s(a,b)
\end{array}
$$

- Small $a+ib$ where $a, b > 0$

$$0, 0, 0, 0, 0, \sqrt{a+ib}, \sqrt{a+ib}, \sqrt{a+ib}, 0, 0, 0, 0, 0, -\sqrt{a+ib}, -\sqrt{a+ib}, -\sqrt{a+ib}$$

Nondeterministic refinement for complex square roots

In order to construct $X : \mathsf{MR}$ via approximation,

- (**Nondeterministic Refinement Step**) For each $n : \mathsf{N}$,
  given any 2^{-n} approximation $x_n : \mathsf{R}$ to *some* $x \in X$,
  nondeterministically compute x_{n+1} s.t.
  (1) x_{n+1} is a 2^{-n-1} approximation to some $x \in X$ (2) $|x_{n+1} - x_n| \leq 2^{-n-1}$.

Refine 2^{-n}-approx $x + iy$ of $\sqrt{a + ib}$ to 2^{-n-1}-approx:

$$
\begin{array}{llll}
\textbf{case} & |a+ib| < 2^{-2(n+2)} & \Rightarrow & \textbf{return } 0 \\
\| & |a+ib| > 0 & \Rightarrow & \textbf{case} \quad a > 0 \quad \Rightarrow \quad \textbf{return } p(a,b) \\
 & & & \| \quad a < 0 \quad \Rightarrow \quad \textbf{return } q(a,b) \\
 & & & \| \quad b > 0 \quad \Rightarrow \quad \textbf{return } r(a,b) \\
 & & & \| \quad b < 0 \quad \Rightarrow \quad \textbf{return } s(a,b)
\end{array}
$$

- Small $a + ib$ where $a, b > 0$

$$0, 0, 0, 0, 0, \sqrt{a+ib}, \sqrt{a+ib}, \sqrt{a+ib}, 0, 0, 0, 0, 0, -\sqrt{a+ib}, -\sqrt{a+ib}, -\sqrt{a+ib}$$

- Only with a promise that $x + iy$ is 2^{-n}-approx does not say about branch
- If we choose $r(a, b)$ in the refinement but it was $x + iy = p(a, b)$,

$$|x_{n+1} - x_n| \leq 2^{-n-1}$$

Nondeterministic refinement for complex square roots

- (**Nondeterministic Refinement Step with Invariant**) for each $n : \mathsf{N}$
  given a 2^{-n} approximation $x_n : \mathsf{R}$ to *some* $x \in X$ and $t_n : I\ n\ x$,
  nondeterministically compute (x_{n+1}, t_{n+1}) such that
  (1) x_{n+1} is a 2^{-n-1}-approx of some $x \in X$, (2) $|x_{n+1} - x_n| \leq 2^{-n-1}$, (3) $t_{n+1} : I\ (n+1)\ x_{n+1}$

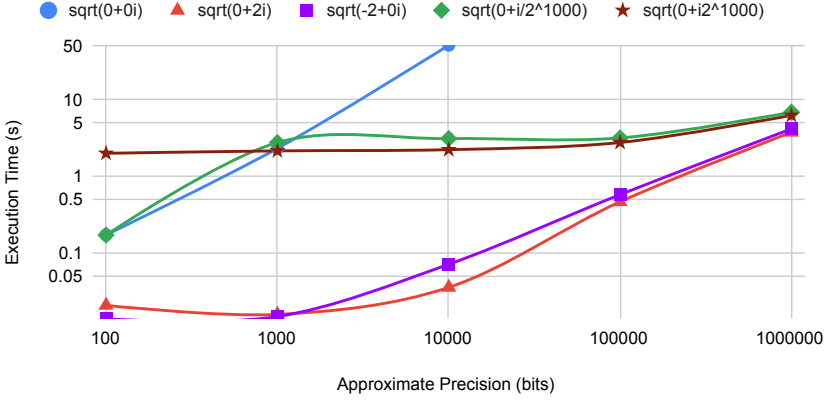
Let $I\ n\ (x + iy) \equiv \left(|a + ib| < 2^{-2(n+2)} \wedge x + iy = 0\right) \vee (x + iy) \cdot (x + iy) = a + ib$

Refine 2^{-n}-approx $x + iy$ of $\sqrt{a + ib}$ given $t : I\ n\ (x + iy)$:

destruct t
| $\left(|a + ib| < 2^{-2(n+2)} \wedge x + iy = 0\right) \Rightarrow$
  case $|a + ib| < 2^{-2(n+2)} \Rightarrow$ **return** $0, L$
  || $|a + ib| > 0 \Rightarrow$ **case** $a > 0 \Rightarrow$ **return** $p(a, b), R$
  || $a < 0 \Rightarrow$ **return** $q(a, b), R$
  || $b > 0 \Rightarrow$ **return** $r(a, b), R$
  || $b < 0 \Rightarrow$ **return** $s(a, b), R$
| $(x + iy) \cdot (x + iy) = a + ib \Rightarrow$ **return** $x + iy, R$

Experimental results

1. Implemented the axiomatization and the complex square root in Coq
2. Nondeterministic dependent choice mapped to primitive recursor in Haskell
3. `https://github.com/holgerthies/coq-aern`



(i7-4710MQ CPU, 16GB RAM, Ubuntu 18.04, Haskell Stackage LTS 17.2)

Conclusion and Future Works

In this talk,

- we formalized a nondeterministic version of constructive metric completeness of reals
- we specified more basic property of nondeterminism that makes the completeness provable

Future work includes

- various subset and function representations in our system
- continuity principle
- practical implementations e.g., exact real linear algebra library

There is a talk at NASA Formal Methods 2022 by Holger Thies this Friday!

Thank you for your attention!