Presented in

Paris VII University

A Generalized Realizability for Constructive Arithmetics

Saeed Salehi
Inst. of Math.
Polish Academy of Sciences
salehi@impan.gov.pl

Kleene's (r-) realizability

$n \ \mathbf{r} \ p \equiv p$ for atomic p, $p = \top, \bot$

$n \ \mathbf{r} \ A \wedge B \equiv (\pi_1(n) \ \mathbf{r} \ A) \wedge (\pi_2(n) \ \mathbf{r} \ B)$

$$n \ \mathbf{r} \ A \vee B \equiv (\pi_1(n) = 0 \wedge \pi_2(n) \ \mathbf{r} \ A) \vee (\pi_1(n) \neq 0 \wedge \pi_2(n) \ \mathbf{r} \ B)$$

$$n \ \mathbf{r} \ A \to B \equiv \forall x [x \ \mathbf{r} \ A \to \exists t \{ \mathbf{T} n, x, t \wedge \wedge \underbrace{\mathbf{U} t \ \mathbf{r} \ B}_{\varphi_n(x)\downarrow \ \mathbf{r} \ B} \}]$$

$$n \ \mathbf{r} \ \exists x A(x) \equiv \pi_2(n) \ \mathbf{r} \ A(\pi_1(n))$$

$$n \ \mathbf{r} \ \forall x A(x) \equiv \forall z \ \exists t [\mathbf{T} n, z, t \wedge \underbrace{\mathbf{U} t \ \mathbf{r} \ A(z)}_{\varphi_n(z)\downarrow \ \mathbf{r} \ A(z)}]$$

Soundness: $HA \vdash \varphi \Rightarrow \exists n \in \mathbb{N} \ HA \vdash n \ \mathbf{r} \ \varphi$

ECT_0 is

$$\forall x\,[A(x) \to \exists y\, B(x,y)] \longrightarrow \exists u\, \forall x\, [A(x) \to \exists v\, \{ \mathbf{T}u,x,v \wedge \\ \wedge\ B(x, \mathbf{U}v)\}]$$

in which A doesn't contain $\vee$ and $\exists$ is only in behind of atoms.

For HA in the language of PRA (and so containing PRA):

Completeness theorem of Troelstra:

$$HA \vdash \exists x\,(x\ \mathbf{r}\ \varphi) \iff HA + ECT_0 \vdash \varphi$$

q-realizability:

$$n\ \mathbf{q}\ A \to B \equiv (A \to B) \wedge \cdots$$

Soundness: $HA \vdash \varphi \Rightarrow HA \vdash n\ \mathbf{q}\ \varphi$ for some $n \in \mathbb{N}$

As applications:

- DP: $HA \vdash A \vee B \Rightarrow HA \vdash A$ or $HA \vdash B$
- EDN: $HA \vdash \exists x\, A(x) \Rightarrow HA \vdash A(n)$ for some $n \in \mathbb{N}$
- provably total functions of HA are recursive:

$$HA \vdash \forall x\, \exists y\, A(x,y) \Rightarrow HA \vdash \forall x\, \exists z\, \{\mathbf{T}m,x,z \wedge A(x, \mathbf{U}z)\}$$

for some $m \in \mathbb{N}$

Basic Logic and Basic Arithmetic

sequent calculus with the symbols $\top, \bot$ and an exception for the universal quantification:

For formulas A, B and $\bar{x}$ a finite sequences of variables $\forall \bar{x}\,(A \to B)$ is a formula.

for $\bar{x} = \phi$ we write $A \to B$

and for $A = \top$ $\quad \forall \bar{x}\, B(\bar{x})$.

Axioms

$A \Rightarrow A \qquad A \Rightarrow \top \qquad \bot \Rightarrow A$

$A \wedge \exists x B \Rightarrow \exists x (A \wedge B)$ $\quad$ x not free in A

$A \wedge (B \vee C) \Rightarrow (A \wedge B) \vee (A \wedge C)$

$\forall \bar{x}\,(A \to B) \wedge \forall \bar{x}\,(B \to C) \Rightarrow \forall \bar{x}\,(A \to C)$

$\forall \bar{x}\,(A \to B) \wedge \forall \bar{x}\,(A \to C) \Rightarrow \forall \bar{x}\,(A \to B \wedge C)$

$\forall \bar{x}\,(B \to A) \wedge \forall \bar{x}\,(C \to A) \Rightarrow \forall \bar{x}\,(B \vee C \to A)$

$\forall \bar{x}\,(A \to B) \Rightarrow \forall \bar{x}\,(A^t_x \to B^t_x)$ $\quad$ no var. in t is bounded in A nor B

$\forall \bar{x}\,(A \to B) \Rightarrow \forall \bar{y}\,(A \to B)$ $\quad$ no var. in $\bar{y}$ is bounded on left

$\forall x \bar{y}\,(B \to A) \Rightarrow \forall \bar{y}\,(\exists x B \to A)$ $\quad$ no var. in $\bar{y}$ is free on left

$\top \Rightarrow x = x \qquad x = y \wedge A \Rightarrow A^x_y$ $\quad$ A-atomic

Rules

$$\frac{A \Rightarrow B \quad B \Rightarrow C}{A \Rightarrow C} \qquad \frac{A \Rightarrow B \quad A \Rightarrow C}{A \Rightarrow B \wedge C} \qquad \frac{B \Rightarrow A \quad C \Rightarrow A}{B \vee C \Rightarrow A}$$

$$\frac{A \Rightarrow B}{A^x_t \Rightarrow B^x_t}$$ no var. in t is bounded on the top.

$$\frac{B \Rightarrow A}{\exists x B \Rightarrow A}$$ x not free in A

$$\frac{A \wedge B \Rightarrow C}{A \Rightarrow \forall \bar{x} (B \to C)}$$ no var. in $\bar{x}$ free in A

Basic Arithmetic

the language: Constant 0, $\underline{f}$, $\underline{R}$ for each primitive recursive function f and relation R.

S: successor function
Z: constant zero function
π^i_n: projection

$\Rightarrow \underline{Z}(x) = 0$

$\Rightarrow \underline{\pi}^i_n (x_1, \ldots, x_n) = x_i$

$\underline{S}x = 0 \Rightarrow \perp$

$\underline{S}x = \underline{S}y \Rightarrow x = y$

$\Rightarrow \underline{f}(\underline{g}_1, \ldots, \underline{g}_n) = \underline{h}$ if $f(g_1, \ldots, g_n) = h$

$\Rightarrow \underline{f}(\bar{x}, 0) = \underline{g}(\bar{x})$

$\Rightarrow \underline{f}(\bar{x}, y+1) = \underline{h}(\bar{x}, f(\bar{x}, y))$

if $\begin{cases} f(\bar{x}, 0) = g(\bar{x}) \\ f(\bar{x}, y+1) = h(\bar{x}, f(\bar{x}, y)) \end{cases}$

$\Rightarrow \underline{f}(\underline{n}) = \underline{m}$ $\quad \underline{n} = \underbrace{S \cdots S}_{n} 0$

if $\mathbb{N} \models f(n) = m$

$\underline{R}(\bar{x}) \Rightarrow \underline{\chi_R}(\bar{x}) = 1$

$\underline{\chi}_R(\bar{x}) = 1 \Rightarrow \underline{R}(\bar{x})$

χ_R is the charactristic func. of R

$\forall x \bar{y} \; (A(x) \to A(\underline{S}x)) \Rightarrow \forall x \bar{y} \; (A(0) \to A(x))$

$$\frac{A(x) \Rightarrow A(\underline{S}x)}{A(0) \Rightarrow A(x)}$$

- the primitive recursive $PR(x) \equiv$ " there is no use of minimalization in the 'program' of the function with 'code' x "

So if $\mathbb{N} \models PR(n)$ then φ_n is p.r. but not vice versa!

- the primitive recursive function $eq(x,y)$;

$$eq(m,n) = \begin{cases} 1 & m = n \\ 0 & m \neq n \end{cases}$$

let $\sim x = y \equiv eq(x,y) = 0$

we have $BA \vdash x = y \wedge \sim x = y \Rightarrow \perp$

So this is stronger than logical negation, since

$$BA \not\vdash x = y \wedge \neg x = y \Rightarrow \perp$$

also $BA \vdash \Rightarrow \forall x,y \, (x = y \vee \sim x = y)$

Primitive Recursive Realizability

$x \, r^{PR} \, p \equiv p$ for atomic p and $p = \top, \bot$

$x \, r^{PR} \, A \wedge B \equiv (\Pi_1(x) \, r^{PR} A) \wedge (\Pi_2(x) \, r^{PR} B)$

$x \, r^{PR} \, A \vee B \equiv (\Pi_1(x) = 0 \wedge \Pi_2(x) \, r^{PR} A) \vee (\sim \Pi_1(x) = 0 \wedge \Pi_2(x) \, r^{PR} B)$

$x \, r^{PR} \, \exists z B(z) \equiv \Pi_2(x) \, r^{PR} B(\Pi_1(x))$

$$x \, r^{PR} \, \forall \bar{z} (A \to B) \equiv PR(x) \wedge \forall y, \bar{z} \big(y \, r^{PR} A(\bar{z}) \longrightarrow \exists w \{ T x, \langle y, \bar{z} \rangle, w \wedge U w \, r^{PR} B(\bar{z}) \} \big)$$

$\varphi_x \langle y, \bar{z} \rangle \, r \, B(\bar{z})$

also for $x \, r^{PR} (A \Rightarrow B)$ write two sequents:

$\Rightarrow PR(x)$ $\qquad$ $y \, r^{PR} A(\bar{z}) \Rightarrow \exists w \{ T x, \langle y, \bar{z} \rangle, w \wedge U w \, r^{PR} B(\bar{z}) \}$

$\bar{z}$ are all free var. of the seq.

We identify $\bar{z} = (z_1, \dots, z_n)$ with $\langle z_1, \langle z_2, \langle \dots z_n \rangle \dots \rangle$

Soundness

if $BA \vdash A \Rightarrow B$ then $BA \vdash n \, r^{PR} (A \Rightarrow B)$

for a natural $n \in \mathbb{N}$.

Another form of church's thesis

$$\forall x\, \exists y\, B(x,y) \Rightarrow \exists u \left[PR(u) \wedge \forall x B(x, \varphi_u(x)) \right]$$

Generalized form of CH : GCT^{PR}

$$\forall \bar{x}, z \left(z\, r^{PR}_{A(\bar{x})} \longrightarrow \exists y\, B(\bar{x}, y) \right) \Longrightarrow \exists u \Big[PR(u) \wedge$$
$$\wedge\ \forall \bar{x}, z \left(z\, r^{PR} A(\bar{x}) \longrightarrow \exists w \{ T_{u,\langle \bar{x}, z\rangle, w} \wedge B(\bar{x}, Uw) \} \right) \Big]$$

Completeness :

$BA \vdash \exists x\, (x\, r^{PR}_{(A \Rightarrow B)})$ iff

$BA + GCT^{PR} \vdash A \Rightarrow B$

q – PR – realizability

- $x \mathbf{q}^{PR} \forall \bar{z}\big(A(\bar{z}) \to B(\bar{z})\big) \equiv \forall \bar{z}\big(A(\bar{z}) \to B(\bar{z})\big) \wedge PR(x) \wedge \cdots$
- $x \mathbf{q}^{PR} (A \Rightarrow B)$ are three sequents : $\Rightarrow PR(x)$ $\quad A \Rightarrow B$

$y \mathbf{q}^{PR} A(\bar{z}) \Rightarrow \exists w \{ \mathbf{T}\, x, \langle y, \bar{z} \rangle, w \wedge \mathbf{U} w\, \mathbf{q}^{PR} B(\bar{z}) \}$

$\bar{z} = \langle z_1, \langle z_2, \cdots \rangle\rangle$ all free var. of the seq.

Theorem. $BA \vdash x \mathbf{q}^{PR} A \Rightarrow A$

$BA \vdash A \Rightarrow B$ then $BA \vdash n \mathbf{q}^{PR} (A \Rightarrow B)$ for some $n \in \mathbb{N}$

Applications:

- if $BA \vdash A \vee B$ then $BA \vdash A$ or $BA \vdash B$
- if $BA \vdash \exists x A(x)$ then $BA \vdash A(n)$ for some $n \in \mathbb{N}$
- if $BA \vdash \forall \bar{x} \exists y A(\bar{x}, y)$ then $BA \vdash \forall \bar{x} A(\bar{x}, f\bar{x})$ for a p.r. (symbol) f.
- if $BA \vdash \Rightarrow \exists y A(\bar{x}, y)$ then $BA \vdash \Rightarrow A(\bar{x}, f\bar{x})$ for a p.r. f.

(totaly provable functions of BA are primitive recursive.)