Synthetic Computability without Choice

Yannick Forster

Inria, Cambium Team, Paris

PLS '24

Work done over the last 8ish years

Parts of the work presented are joint with Dominik Kirst, Gert Smolka, Felix Jahn, Fabian Kunze, Nils Lauermann, Niklas Mück, and Haoyi Zeng.

The Coq Undecidability Library has contributions by Dominique Larchey-Wendling, Andrej Dudenhefner, Janis Bailitis, Fabian Brenner, Edith Heiter, Marc Hermes, Johannes Hostert, Dominik Kirst, Mark Koch, Fabian Kunze, Gert Smolka, Simon Spies, Dominik Wehr, Maxi Wuttke, Nils Lauermann, Fabian Kunze, and Benjamin Peters.

Lead questions

How to do constructive reverse analysis of computability theory proofs?

Lead questions

How to do constructive reverse analysis of computability theory proofs?

How to do machine-checked proofs in computability theory?

Lead questions

How to do constructive reverse analysis of computability theory proofs?

How to do machine-checked proofs in computability theory?

Recipe to write textbooks on computability

1. Introduce favourite model of computation
   1.1 Prove s_n^m theorem (currying)
   1.2 Argue universal program
   1.3 Optional: Introduce a second model and argue equivalence
2. Introduce intuitive computability and Church Turing thesis
3. Develop computability theory relying on Church Turing thesis
   3.1 Undecidability of the halting problem
   3.2 Rice's theorem
   3.3 Reduction theory (Myhill isomorphism theorem, Post's simple and hypersimple sets)
   3.4 Oracle computation and Turing reducibility
4. Prove undecidability of concrete problems (PCP, CFGs)

Recipe to write textbooks on computability

1. Introduce favourite model of computation
   1.1 Prove s_n^m theorem (currying)
   1.2 Argue universal program
   1.3 Optional: Introduce a second model and argue equivalence
2. Introduce intuitive computability and Church Turing thesis
3. Develop computability theory relying on Church Turing thesis
   3.1 Undecidability of the halting problem relying on Church Turing thesis
   3.2 Rice's theorem relying on Church Turing thesis
   3.3 Reduction theory relying on Church Turing thesis
   3.4 Oracle computation relying on Church Turing thesis
4. Prove undecidability (PCP, CFGs) relying on Church Turing thesis

Computability proofs machine-checked in proof assistants

1. Introduce favourite model of computation
   1.1 Prove s_n^m theorem (currying)
   1.2 Argue universal program
   1.3 Optional: Introduce a second model and argue equivalence
2. Introduce intuitive computability and Church Turing thesis
3. Develop computability theory relying on Church Turing thesis
   3.1 Undecidability of the halting problem
   3.2 Rice's theorem
   3.3 Reduction theory
   3.4 Oracle computation
4. Prove undecidability (PCP, CFGs)

Computability proofs machine-checked in proof assistants

1. Introduce favourite model of computation ✓
   1.1 Prove s^m_n theorem (currying)
   1.2 Argue universal program
   1.3 Optional: Introduce a second model and argue equivalence
2. Introduce intuitive computability and Church Turing thesis
3. Develop computability theory relying on Church Turing thesis
   3.1 Undecidability of the halting problem
   3.2 Rice's theorem
   3.3 Reduction theory
   3.4 Oracle computation
4. Prove undecidability (PCP, CFGs)

Computability proofs machine-checked in proof assistants

1. Introduce favourite model of computation ✓
   1.1 Prove s^m_n theorem (currying) ✓
   1.2 Argue universal program
   1.3 Optional: Introduce a second model and argue equivalence
2. Introduce intuitive computability and Church Turing thesis
3. Develop computability theory relying on Church Turing thesis
   3.1 Undecidability of the halting problem
   3.2 Rice's theorem
   3.3 Reduction theory
   3.4 Oracle computation
4. Prove undecidability (PCP, CFGs)

Computability proofs machine-checked in proof assistants

1. Introduce favourite model of computation ✓
   1.1 Prove s^m_n theorem (currying) ✓
   1.2 Argue universal program ✓
   1.3 Optional: Introduce a second model and argue equivalence ✓
2. Introduce intuitive computability and Church Turing thesis
3. Develop computability theory relying on Church Turing thesis
   3.1 Undecidability of the halting problem
   3.2 Rice's theorem
   3.3 Reduction theory
   3.4 Oracle computation
4. Prove undecidability (PCP, CFGs)

Computability proofs machine-checked in proof assistants

1. Introduce favourite model of computation ✓
   1.1 Prove s^m_n theorem (currying) ✓
   1.2 Argue universal program ✓
   1.3 Optional: Introduce a second model and argue equivalence ✓
2. ~~Introduce intuitive computability and Church Turing thesis~~
3. Develop computability theory ~~relying on Church Turing thesis~~
   3.1 Undecidability of the halting problem
   3.2 Rice's theorem
   3.3 Reduction theory
   3.4 Oracle computation
4. Prove undecidability (PCP, CFGs)

Computability proofs machine-checked in proof assistants

1. Introduce favourite model of computation ✓
   - 1.1 Prove s^m_n theorem (currying) ✓
   - 1.2 Argue universal program ✓
   - 1.3 Optional: Introduce a second model and argue equivalence ✓
2. ~~Introduce intuitive computability and Church Turing thesis~~
3. Develop computability theory ~~relying on Church Turing thesis~~
   - 3.1 Undecidability of the halting problem ✓
   - 3.2 Rice's theorem
   - 3.3 Reduction theory
   - 3.4 Oracle computation
4. Prove undecidability (PCP, CFGs)

Computability proofs machine-checked in proof assistants

1. Introduce favourite model of computation ✓
   1.1 Prove s^m_n theorem (currying) ✓
   1.2 Argue universal program ✓
   1.3 Optional: Introduce a second model and argue equivalence ✓
2. ~~Introduce intuitive computability and Church Turing thesis~~
3. Develop computability theory ~~relying on Church Turing thesis~~
   3.1 Undecidability of the halting problem ✓
   3.2 Rice's theorem ✓
   3.3 Reduction theory
   3.4 Oracle computation
4. Prove undecidability (PCP, CFGs)

Computability proofs machine-checked in proof assistants

1. Introduce favourite model of computation ✓
   1.1 Prove s_n^m theorem (currying) ✓
   1.2 Argue universal program ✓
   1.3 Optional: Introduce a second model and argue equivalence ✓
2. ~~Introduce intuitive computability and Church Turing thesis~~
3. Develop computability theory ~~relying on Church Turing thesis~~
   3.1 Undecidability of the halting problem ✓
   3.2 Rice's theorem ✓
   3.3 Reduction theory ?
   3.4 Oracle computation ?
4. Prove undecidability (PCP, CFGs) ?

Theorem V *For every $m,n \geq 1$, there exists a recursive function $s_n{}^m$ of $m+1$ variables such that for all $x, y_1, \ldots, y_m$,*

$$\lambda z_1 \cdots z_n[\varphi_x^{(m+n)}(y_1, \ldots, y_m, z_1, \ldots, z_n)] = \varphi^{(n)}_{s_n{}^m(x,y_1,\ldots,y_m)}.$$

Proof. Take the case $m = n = 1$. (Proof is analogous for the other cases.) Consider the family of all partial functions of one variable which are expressible as $\lambda z[\varphi_x{}^{(2)}(y,z)]$ for various x and y. Using our standard formal characterization for functions of two variables, we can view this as a new formal characterization for a class of partial recursive functions of one variable. By Part III of the Basic Result, there exists a uniform effective procedure for going from sets of instructions in this new characterization to sets of instructions in the old. Hence, by Church's Thesis, there must be a recursive function f of two variables such that

$$\lambda z[\varphi_x{}^{(2)}(y,z)] = \varphi_{f(x,y)}.$$

This f is our desired $s_1{}^1$. ☒

The informal argument by appeal to Church's Thesis and Part III of the Basic Result can be replaced by a formal proof. (Indeed, the functions $s_n{}^m$ can be shown to be primitive recursive.) We refer the reader to Davis [1958] and Kleene [1952]. Theorem V is known as the *s-m-n theorem* and is due to Kleene. Theorem V (together with Church's Thesis) is a tool of great range and power.

THEOREM 1.1. *There is a primitive recursive function* $\gamma(r, y)$ *such that, for* $n \geqq 1$,

$$[r]^A_{1+n}(y, \mathfrak{x}^{(n)}) = [\gamma(r, y)]_n{}^A(\mathfrak{x}^{(n)}).$$

Intuitively, this result may be interpreted, for $A = \phi$, $n = 1$, as declaring the existence of an algorithm[1] by means of which, given any Turing machine Z and number m, a Turing machine Z_m can be found such that

$$\Psi_{Z^{(2)}}(m, x) = \Psi_{Z_m}(x).$$

Now it is clear that there exist Turing machines Z_m satisfying this last relation since, for each fixed m, $\Psi_{Z^{(2)}}(m, x)$ is certainly a partial recursive function of x. Hence, the content of our theorem (in this special case) is that Z_m can be found effectively in terms of Z and m. However, such a Z_m can readily be described as a Turing machine which, beginning at $\alpha = q_1 1^{x+1}$, proceeds to print $\bar{m} = 1^{m+1}$ to the left, eventually arriving at $\beta = q_N 1^{m+1} B 1^{x+1}$, and then proceeds to act like Z when confronted with

[1] Actually, an algorithm given by a *primitive* recursive function.

$q_1 1^{m+1} B 1^{x+1}$. As the general case does not differ essentially from this special case, all that is required for a formal proof is a detailed construction of Z_m and a careful consideration of the Gödel numbers. The reader who wishes to omit the tedious details, and simply accept the result, may well do so.

PROOF OF THEOREM 1.1. For each value of y, let W_y be the Turing machine consisting of the following quadruples:

$$\begin{array}{l} q_1\ 1\ L\ q_1 \\ q_1\ B\ L\ q_2 \\ \left.\begin{array}{l} q_{i+1}\ B\ 1\ q_{i+1} \\ q_{i+1}\ 1\ L\ q_{i+2} \end{array}\right\} 1 \leqq i \leqq y \\ q_{y+2}\ B\ 1\ q_{y+3}. \end{array}$$

Then, with respect to W_y,

$$\begin{aligned} q_1(\overline{\mathfrak{x}^{(n)}}) &\rightarrow q_1 B(\overline{\mathfrak{x}^{(n)}}) \\ &\rightarrow q_2 BB(\overline{\mathfrak{x}^{(n)}}) \\ &\rightarrow \cdots \\ &\rightarrow q_{y+3}(\overline{y, \mathfrak{x}^{(n)}}). \end{aligned}$$

Let r be a Gödel number of a Turing machine Z, and let

$$Z_y = W_y \cup Z^{(y+2)}.\dagger$$

Then, since the quadruples of $Z^{(y+2)}$ have precisely the same effect on $q_{y+3}(\overline{y, \mathfrak{x}^{(n)}})$ that those of Z have on $q_1(\overline{y, \mathfrak{x}^{(n)}})$, we have

$$\Psi^{(n)}_{Z_y;A}(\mathfrak{x}^{(n)}) = \Psi^{(1+n)}_{Z}(y, \mathfrak{x}^{(n)}) = [r]^A_{1+n}(y, \mathfrak{x}^{(n)}). \tag{1}$$

We now proceed to evaluate one of the Gödel numbers of Z_y as a function of r and y. The Gödel numbers of the quadruples that make up W_y are as follows:[1]

$$\begin{aligned} a &= \text{gn}\,(q_1\, 1\, L\, q_1) = 2^9 \cdot 3^{11} \cdot 5^5 \cdot 7^9, \\ b &= \text{gn}\,(q_1\, B\, L\, q_2) = 2^9 \cdot 3^7 \cdot 5^5 \cdot 7^{13}, \\ c(i) &= \text{gn}\,(q_{i+1}\, B\, 1\, q_{i+1}) = 2^{4i+9} \cdot 3^7 \cdot 5^{11} \cdot 7^{4i+9}, \ 1 \leqq i \leqq y, \\ d(i) &= \text{gn}\,(q_{i+1}\, 1\, L\, q_{i+2}) = 2^{4i+9} \cdot 3^{11} \cdot 5^5 \cdot 7^{4i+13}, \ 1 \leqq i \leqq y, \\ e(y) &= \text{gn}\,(q_{y+2}\, B\, 1\, q_{i+3}) = 2^{4y+13} \cdot 3^7 \cdot 5^{11} \cdot 7^{4y+17}. \end{aligned}$$

Thus, if we let

$$\varphi(y) = 2^a \cdot 3^b \cdot 5^{e(y)} \cdot \prod_{i=1}^{y} [\text{Pr}\,(i+3)^{c(i)}\, \text{Pr}\,(i+y+3)^{d(i)}],$$

then $\varphi(y)$ is a primitive recursive function, and, for each y, $\varphi(y)$ is a Gödel number of W_y.

We recall that the predicate IC (x), which is true if and only if x is the number associated with an internal configuration q_i, is primitive recursive, since

$$\text{IC}\,(x) \leftrightarrow \bigvee_{y=0}^{x} (x = 4y + 9).$$

Hence, the function $\iota(x)$, which is 1 when x is the number associated with a q_i and 0 otherwise, is primitive recursive. If h is the Gödel number of a quadruple, then the Gödel number of the quadruple obtained from this one by replacing each q_i by q_{i+y+2} is

$$f(h, y) = 2^{1\,\mathrm{Gl}\,h+4y+8} \cdot 3^{2\,\mathrm{Gl}\,h} \cdot 5^{3\,\mathrm{Gl}\,h+(4y+8)\iota(3\,\mathrm{Gl}\,h)} \cdot 7^{4\,\mathrm{Gl}\,h+4y+8}.$$

Here, $f(h, y)$ is primitive recursive. Hence, if we let

$$\theta(r, y) = \prod_{i=1}^{\mathfrak{L}(r)} \text{Pr}\,(i)^{f(i\,\mathrm{Gl}\,r,\, y)},$$

then $\theta(r, y)$ is a primitive recursive function and, for each y, $\theta(r, y)$ is a Gödel number of $Z^{(y+2)}$.

Let $\tau(x) = 1$ if x is a Gödel number of a Turing machine; 0, otherwise. Then, by (11) of Chap. 4, Sec. 1, $\tau(x)$ is primitive recursive. Finally, let

$$\gamma(r, y) = (\varphi(y) * \theta(r, y))\tau(r).$$

Then $\gamma(r, y)$ is a primitive recursive function and, for each y, $\gamma(r, y)$ is a Gödel number of Z_y. Hence, by (1),

$$[\gamma(r, y)]_n{}^A(\mathfrak{x}^{(n)}) = [r]^A_{1+n}(y, \mathfrak{x}^{(n)}). \tag{2}$$

It remains only to consider the case where r is not a Gödel number of a Turing machine. In that case, $\gamma(r, y)$, as defined above, is 0 and, thus, is itself not the Gödel number of a Turing machine; so (2) remains correct.[1]

THEOREM 1.2 (Kleene's Iteration Theorem[2]). *For each* m *there is a primitive recursive function* $S^m(r, \mathfrak{y}^{(m)})$ *such that, for* $n \geqq 1$,

$$[r]^A_{m+n}(\mathfrak{y}^{(m)}, \mathfrak{x}^{(n)}) = [S^m(r, \mathfrak{y}^{(m)})]_n{}^A(\mathfrak{x}^{(n)}).$$

Note that Theorem 1.1 is simply Theorem 1.2 with $m = 1$.

```
section ‹The $s$-$m$-$n$ theorem›

text ‹For all $m, n > 0$ there is an $(m + 1)$-ary primitive recursive
function $s^m_n$ with
\[
  \varphi_p^{(m + n)}(c_1, \dots,c_m, x_1, \dots, x_n) =
  \varphi_{s^m_n(p, c_1, \dots,c_m)}^{(n)}(x_1, \dots, x_n)
\]
for all $p, c_1, \ldots, c_m, x_1, \ldots, x_n$. Here, $\varphi^{(n)}$ is a
function universal for $n$-ary partial recursive functions, which we will
represent by @{term "r_universal n"}›

text ‹The $s^m_n$ functions compute codes of functions. We start simple:
computing codes of the unary constant functions.›

fun code_const1 :: "nat ⇒ nat" where
  "code_const1 0 = 0"
| "code_const1 (Suc c) = quad_encode 3 1 1 (singleton_encode (code_const1 c))"

lemma code_const1: "code_const1 c = encode (r_const c)"
  by (induction c) simp_all

definition "r_code_const1_aux ≡
  Cn 3 r_prod_encode
    [r_constn 2 3,
     Cn 3 r_prod_encode
       [r_constn 2 1,
        Cn 3 r_prod_encode
          [r_constn 2 1, Cn 3 r_singleton_encode [Id 3 1]]]]"

lemma r_code_const1_aux_prim: "prim_recfn 3 r_code_const1_aux"
  by (simp_all add: r_code_const1_aux_def)

lemma r_code_const1_aux:
  "eval r_code_const1_aux [i, r, c] ↓= quad_encode 3 1 1 (singleton_encode r)"
  by (simp add: r_code_const1_aux_def)

definition "r_code_const1 ≡ r_shrink (Pr 1 Z r_code_const1_aux)"

lemma r_code_const1_prim: "prim_recfn 1 r_code_const1"
  by (simp_all add: r_code_const1_def r_code_const1_aux_prim)

lemma r_code_const1: "eval r_code_const1 [c] ↓= code_const1 c"
proof -
  let ?h = "Pr 1 Z r_code_const1_aux"
  have "eval ?h [c, x] ↓= code_const1 c" for x
    using r_code_const1_aux r_code_const1_def
    by (induction c) (simp_all add: r_code_const1_aux_prim)
  then show ?thesis by (simp add: r_code_const1_def r_code_const1_aux_prim)
qed

text ‹Functions that compute codes of higher-arity constant functions:›

definition code_constn :: "nat ⇒ nat ⇒ nat" where
  "code_constn n c ≡
    if n = 1 then code_const1 c
    else quad_encode 3 n (code_const1 c) (singleton_encode (triple_encode 2 n 0))"

lemma code_constn: "code_constn (Suc n) c = encode (r_constn n c)"
  unfolding code_constn_def using code_const1 r_constn_def
  by (cases "n = 0") simp_all

definition r_code_constn :: "nat ⇒ recf" where
  "r_code_constn n ≡
     if n = 1 then r_code_const1
     else
       Cn 1 r_prod_encode
        [r_const 3,
         Cn 1 r_prod_encode
          [r_const n,
           Cn 1 r_prod_encode
            [r_code_const1,
             Cn 1 r_singleton_encode
              [Cn 1 r_prod_encode
                [r_const 2, Cn 1 r_prod_encode [r_const n, Z]]]]]]"

lemma r_code_constn_prim: "prim_recfn 1 (r_code_constn n)"
  by (simp_all add: r_code_constn_def r_code_const1_prim)

lemma r_code_constn: "eval (r_code_constn n) [c] ↓= code_constn n c"
  by (auto simp add: r_code_constn_def r_code_const1 code_constn_def r_code_const1_prim)

text ‹Computing codes of $m$-ary projections:›

definition code_id :: "nat ⇒ nat ⇒ nat" where
  "code_id m n ≡ triple_encode 2 m n"

lemma code_id: "encode (Id m n) = code_id m n"
  unfolding code_id_def by simp

text ‹The functions $s^m_n$ are represented by the following function.
The value $m$ corresponds to the length of @{term "cs"}.›

definition smn :: "nat ⇒ nat ⇒ nat list ⇒ nat" where
  "smn n p cs ≡ quad_encode
     3
     n
     (encode (r_universal (n + length cs)))
     (list_encode (code_constn n p # map (code_constn n) cs @ map (code_id n) [0..<n]))"

lemma smn:
  assumes "n > 0"
  shows "smn n p cs = encode
   (Cn n
     (r_universal (n + length cs))
     (r_constn (n - 1) p # map (r_constn (n - 1)) cs @ (map (Id n) [0..<n])))"
proof -
  let ?p = "r_constn (n - 1) p"
  let ?gs1 = "map (r_constn (n - 1)) cs"
  let ?gs2 = "map (Id n) [0..<n]"
  let ?gs = "?p # ?gs1 @ ?gs2"
  have "map encode ?gs1 = map (code_constn n) cs"
    by (intro nth_equalityI; auto; metis code_constn assms Suc_pred)
  moreover have "map encode ?gs2 = map (code_id n) [0..<n]"
    by (rule nth_equalityI) (auto simp add: code_id_def)
  moreover have "encode ?p = code_constn n p"
    using assms code_constn[of "n - 1" p] by simp
  ultimately have "map encode ?gs =
      code_constn n p # map (code_constn n) cs @ map (code_id n) [0..<n]"
    by simp
  then show ?thesis
    unfolding smn_def using assms encode.simps(4) by presburger
qed

text ‹The next function is to help us define @{typ recf}s corresponding
to the $s^m_n$ functions. It maps $m + 1$ arguments $p, c_1, \ldots, c_m$ to
an encoded list of length $m + n + 1$. The list comprises the $m + 1$ codes
of the $n$-ary constants $p, c_1, \ldots, c_m$ and the $n$ codes for all
$n$-ary projections.›

definition r_smn_aux :: "nat ⇒ nat ⇒ recf" where
    list_encode (map (code_constn n) (p # cs) @ map (code_id n) [0..<n])"
proof -
  let ?xs = "map (λi. Cn (Suc m) (r_code_constn n) [Id (Suc m) i]) [0..<Suc m]"
  let ?ys = "map (λi. r_constn m (code_id n i)) [0..<n]"
  have len_xs: "length ?xs = Suc m" by simp

  have map_xs: "map (λg. eval g (p # cs)) ?xs = map Some (map (code_constn n) (p # cs))"
  proof (intro nth_equalityI)
    show len: "length (map (λg. eval g (p # cs)) ?xs) =
        length (map Some (map (code_constn n) (p # cs)))"
      by (simp add: assms(2))

    have "map (λg. eval g (p # cs)) ?xs ! i = map Some (map (code_constn n) (p # cs)) ! i"
        if "i < Suc m" for i
    proof -
      have "map (λg. eval g (p # cs)) ?xs ! i = (λg. eval g (p # cs)) (?xs ! i)"
        using len_xs that by (metis nth_map)
      also have "... = eval (Cn (Suc m) (r_code_constn n) [Id (Suc m) i]) (p # cs)"
        using that len_xs
        by (metis (no_types, lifting) add.left_neutral length_map nth_map nth_upt)
      also have "... = eval (r_code_constn n) [the (eval (Id (Suc m) i) (p # cs))]"
        using r_code_constn_prim assms(2) that by simp
      also have "... = eval (r_code_constn n) [(p # cs) ! i]"
        using len that by simp
      finally have "map (λg. eval g (p # cs)) ?xs ! i ↓= code_constn n ((p # cs) ! i)"
        using r_code_constn by simp
      then show ?thesis
        using len_xs len that by (metis length_map nth_map)
    qed
    moreover have "length (map (λg. eval g (p # cs)) ?xs) = Suc m" by simp
    ultimately show "⋀i. i < length (map (λg. eval g (p # cs)) ?xs) ⟹
        map (λg. eval g (p # cs)) ?xs ! i =
        map Some (map (code_constn n) (p # cs)) ! i"
      by simp
  qed
  moreover have "map (λg. eval g (p # cs)) ?ys = map Some (map (code_id n) [0..<n])"
    using assms(2) by (intro nth_equalityI; auto)
  ultimately have "map (λg. eval g (p # cs)) (?xs @ ?ys) =
      map Some (map (code_constn n) (p # cs) @ map (code_id n) [0..<n])"
    by (metis map_append)
  moreover have "map (λx. the (eval x (p # cs))) (?xs @ ?ys) =
      map the (map (λx. eval x (p # cs)) (?xs @ ?ys))"
    by simp
  ultimately have *: "map (λg. the (eval g (p # cs))) (?xs @ ?ys) =
      (map (code_constn n) (p # cs) @ map (code_id n) [0..<n])"
    by simp

  have "∀i<length ?xs. eval (?xs ! i) (p # cs) = map (λg. eval g (p # cs)) ?xs ! i"
    by (metis nth_map)
  then have
    "∀i<length ?xs. eval (?xs ! i) (p # cs) = map Some (map (code_constn n) (p # cs)) ! i"
    using map_xs by simp
  then have "∀i<length ?xs. eval (?xs ! i) (p # cs) ↓"
    using assms map_xs by (metis length_map nth_map option.simps(3))
  then have xs_converg: "∀z∈set ?xs. eval z (p # cs) ↓"
    by (metis in_set_conv_nth)

  have "∀i<length ?ys. eval (?ys ! i) (p # cs) = map (λx. eval x (p # cs)) ?ys ! i"
    by simp
  then have
    "∀i<length ?ys. eval (?ys ! i) (p # cs) = map Some (map (code_id n) [0..<n]) ! i"
    using assms(2) by simp
  then have "∀i<length ?ys. eval (?ys ! i) (p # cs) ↓"
    by simp
  then have "∀z∈set (?xs @ ?ys). eval z (p # cs) ↓"
    using xs_converg by auto
  moreover have "recfn (length (p # cs)) (Cn (Suc m) (r_list_encode (m + n)) (?xs @ ?ys))"
    using assms r_code_constn_prim by auto
  ultimately have "eval (r_smn_aux n m) (p # cs) =
      eval (r_list_encode (m + n)) (map (λg. the (eval g (p # cs))) (?xs @ ?ys))"
    unfolding r_smn_aux_def using assms by simp
  then have "eval (r_smn_aux n m) (p # cs) =
      eval (r_list_encode (m + n)) (map (code_constn n) (p # cs) @ map (code_id n) [0..<n])"
    using * by metis
  moreover have "length (?xs @ ?ys) = Suc (m + n)" by simp
  ultimately show ?thesis
    using r_list_encode * assms(1) by (metis (no_types, lifting) length_map)
qed

text ‹For all $m, n > 0$, the @{typ recf} corresponding to $s^m_n$ is
given by the next function.›

definition r_smn :: "nat ⇒ nat ⇒ recf" where
 "r_smn n m ≡
    Cn (Suc m) r_prod_encode
     [r_constn m 3,
      Cn (Suc m) r_prod_encode
       [r_constn m n,
        Cn (Suc m) r_prod_encode
          [r_constn m (encode (r_universal (n + m))), r_smn_aux n m]]]"

lemma r_smn_prim [simp]: "n > 0 ⟹ prim_recfn (Suc m) (r_smn n m)"
  by (simp_all add: r_smn_def r_smn_aux_prim)

lemma r_smn:
  assumes "n > 0" and "length cs = m"
  shows "eval (r_smn n m) (p # cs) ↓= smn n p cs"
  using assms r_smn_def r_smn_aux smn_def r_smn_aux_prim by simp

lemma map_eval_Some_the:
  assumes "map (λg. eval g xs) gs = map Some ys"
  shows "map (λg. the (eval g xs)) gs = ys"
  using assms
  by (metis (no_types, lifting) length_map nth_equalityI nth_map option.sel)

text ‹The essential part of the $s$-$m$-$n$ theorem: For all $m, n > 0$
the function $s^m_n$ satisfies
\[
  \varphi_p^{(m + n)}(c_1, \dots,c_m, x_1, \dots, x_n) =
  \varphi_{s^m_n(p, c_1, \dots,c_m)}^{(n)}(x_1, \dots, x_n)
\] for all $p, c_i, x_j$.›

lemma smn_lemma:
  assumes "n > 0" and len_cs: "length cs = m" and len_xs: "length xs = n"
  shows "eval (r_universal (m + n)) (p # cs @ xs) =
    eval (r_universal n) ((the (eval (r_smn n m) (p # cs))) # xs)"
proof -
  let ?s = "r_smn n m"
  let ?f = "Cn n
    (r_universal (n + length cs))
    (r_constn (n - 1) p # map (r_constn (n - 1)) cs @ (map (Id n) [0..<n]))"
  have "eval ?s (p # cs) ↓= smn n p cs"
    using assms r_smn by simp
  then have eval_s: "eval ?s (p # cs) ↓= encode ?f"
    by (simp add: assms(1) smn)

  have "recfn n ?f"
    using len_cs assms by auto
  then have *: "eval (r_universal n) ((encode ?f) # xs) = eval ?f xs"
    using r_universal[of ?f n, OF _ len_xs] by simp

  let ?gs = "r_constn (n - 1) p # map (r_constn (n - 1)) cs @ map (Id n) [0..<n]"
    show "length (map (λg. the (eval g xs)) ?gs) = length (p # cs @ xs)"
      by (simp add: len_xs)
    have len: "length (map (λg. the (eval g xs)) ?gs) = Suc (m + n)"
      by (simp add: len_cs)
    moreover have "map (λg. the (eval g xs)) ?gs ! i = (p # cs @ xs) ! i"
      if "i < Suc (m + n)" for i
    proof -
      from that consider "i = 0" | "i > 0 ∧ i < Suc m" | "Suc m ≤ i ∧ i < Suc (m + n)"
        using not_le_imp_less by auto
      then show ?thesis
      proof (cases)
        case 1
        then show ?thesis using assms(1) len_xs by simp
      next
        case 2
        then have "?gs ! i = (map (r_constn (n - 1)) cs) ! (i - 1)"
          using len_cs
          by (metis One_nat_def Suc_less_eq Suc_pred length_map
            less_numeral_extra(3) nth_Cons' nth_append)
        then have "map (λg. the (eval g xs)) ?gs ! i =
            (λg. the (eval g xs)) ((map (r_constn (n - 1)) cs) ! (i - 1))"
          using len by (metis length_map nth_map that)
        also have "... = the (eval ((r_constn (n - 1) (cs ! (i - 1)))) xs)"
          using 2 len_cs by auto
        also have "... = cs ! (i - 1)"
          using r_constn len_xs assms(1) by simp
        also have "... = (p # cs @ xs) ! i"
          using 2 len_cs
          by (metis diff_Suc_1 less_Suc_eq_0_disj less_numeral_extra(3) nth_Cons' nth_append)
        finally show ?thesis .
      next
        case 3
        then have "?gs ! i = (map (Id n) [0..<n]) ! (i - Suc m)"
          using len_cs
          by (simp; metis (no_types, lifting) One_nat_def Suc_less_eq add_leE
            plus_1_eq_Suc diff_diff_left length_map not_le nth_append
            ordered_cancel_comm_monoid_diff_class.add_diff_inverse)
        then have "map (λg. the (eval g xs)) ?gs ! i =
            (λg. the (eval g xs)) ((map (Id n) [0..<n]) ! (i - Suc m))"
          using len by (metis length_map nth_map that)
        also have "... = the (eval ((Id n (i - Suc m))) xs)"
          using 3 len_cs by auto
        also have "... = xs ! (i - Suc m)"
          using len_xs 3 by auto
        also have "... = (p # cs @ xs) ! i"
          using len_cs len_xs 3
          by (metis diff_Suc_1 diff_diff_left less_Suc_eq_0_disj not_le nth_Cons'
            nth_append plus_1_eq_Suc)
        finally show ?thesis .
      qed
    qed
    ultimately show "map (λg. the (eval g xs)) ?gs ! i = (p # cs @ xs) ! i"
        if "i < length (map (λg. the (eval g xs)) ?gs)" for i
      using that by simp
  qed
  ultimately show ?thesis by simp
qed

theorem smn_theorem:
  assumes "n > 0"
  shows "∃s. prim_recfn (Suc m) s ∧
    (∀p cs xs. length cs = m ∧ length xs = n ⟶
        eval (r_universal (m + n)) (p # cs @ xs) =
        eval (r_universal n) ((the (eval s (p # cs))) # xs))"
  using smn_lemma exI[of _ "r_smn n m"] assms by simp
```

Is there a need for machine-checked computability proofs?

Is there a need for machine-checked computability proofs?

1932 Gödel claims without proof that his decidability proof for the $[\exists^*\forall^2\exists^*, \text{all}, (0)]$ fragment of FOL could be extended to include equality.

... Lots of results depend on Gödel's claim.

Is there a need for machine-checked computability proofs?

1932 Gödel claims without proof that his decidability proof for the $[\exists^*\forall^2\exists^*, \text{all}, (0)]$ fragment of FOL could be extended to include equality.

... Lots of results depend on Gödel's claim.

1984 Goldfarb proves the undecidability of this fragment.

Is there a need for machine-checked computability proofs?

1932 Gödel claims without proof that his decidability proof for the $[\exists^*\forall^2\exists^*, \text{all}, (0)]$ fragment of FOL could be extended to include equality.

… Lots of results depend on Gödel's claim.

1984 Goldfarb proves the undecidability of this fragment.

1988 Kfoury, Tiuryn, and Urzyczyn: decidability of semi-unification. (POPL)

Is there a need for machine-checked computability proofs?

1932 Gödel claims without proof that his decidability proof for the $[\exists^*\forall^2\exists^*, \text{all}, (0)]$ fragment of FOL could be extended to include equality.

… Lots of results depend on Gödel's claim.

1984 Goldfarb proves the undecidability of this fragment.

1988 Kfoury, Tiuryn, and Urzyczyn: decidability of semi-unification. (POPL)

1990/93 Kfoury, Tiuryn, and Urzyczyn: *un*decidability of semi-unification (LICS).

Is there a need for machine-checked computability proofs?

1932 Gödel claims without proof that his decidability proof for the $[\exists^* \forall^2 \exists^*, \text{all}, (0)]$ fragment of FOL could be extended to include equality.

... Lots of results depend on Gödel's claim.

1984 Goldfarb proves the undecidability of this fragment.

1988 Kfoury, Tiuryn, and Urzyczyn: decidability of semi-unification. (POPL)

1990/93 Kfoury, Tiuryn, and Urzyczyn: *un*decidability of semi-unification (LICS).

1967 Minsky introduces 2-counter machines with inc and dec/jmp on nonzero, proves undecidability of 2CM-Halt with inc and dec/jmp on zero

Is there a need for machine-checked computability proofs?

1932 Gödel claims without proof that his decidability proof for the $[\exists^*\forall^2\exists^*, \text{all}, (0)]$ fragment of FOL could be extended to include equality.

... Lots of results depend on Gödel's claim.

1984 Goldfarb proves the undecidability of this fragment.

1988 Kfoury, Tiuryn, and Urzyczyn: decidability of semi-unification. (POPL)

1990/93 Kfoury, Tiuryn, and Urzyczyn: *un*decidability of semi-unification (LICS).

1967 Minsky introduces 2-counter machines with inc and dec/jmp on nonzero, proves undecidability of 2CM-Halt with inc and dec/jmp on zero

2022 Dudenhefner proves dec. of 2CM-Halt with inc and dec/jmp on nonzero

State of the art in machine-checked proofs

Theory up to universal machines and Rice's theorem

2011 λ-calculus in HOL4 by Norrish

2017 weak call-by-value λ-calculus in Coq by Forster and Smolka

2019 μ-recursive functions in Lean by Carneiro

2020 `PVS0` in `PVS` by Ferreira Ramos et al.

Miscellaneous results

2019 Bayer et al. prove Hilbert's 10th problem undecidable in Isabelle

2021 Kunze and Gäher prove Cook-Levin theorem in Coq

2021 Forster, Kunze, Wuttke, Smolka formalise polynomial time equivalence of Turing machines and call-by-value λ-calculus

2023 Balbach proves Cook-Levin theorem in Isabelle

Machine-checked textbook proofs

Theorem V *For every $m,n \geq 1$, there exists a recursive function $s_n{}^m$ of $m + 1$ variables such that for all $x, y_1, \ldots, y_m$,*

$$\lambda z_1 \cdots z_n[\varphi_x^{(m+n)}(y_1, \ldots, y_m, z_1, \ldots, z_n)] = \varphi^{(n)}_{s_n{}^m(x,y_1,\ldots,y_m)}.$$

Proof. Take the case $m = n = 1$. (Proof is analogous for the other cases.) Consider the family of all partial functions of one variable which are expressible as $\lambda z[\varphi_x{}^{(2)}(y,z)]$ for various x and y. Using our standard formal characterization for functions of two variables, we can view this as a new formal characterization for a class of partial recursive functions of one variable. By Part III of the Basic Result, there exists a uniform effective procedure for going from sets of instructions in this new characterization to sets of instructions in the old. Hence, by Church's Thesis, there must be a recursive function f of two variables such that

$$\lambda z[\varphi_x{}^{(2)}(y,z)] = \varphi_{f(x,y)}.$$

This f is our desired $s_1{}^1$.⊠

The informal argument by appeal to Church's Thesis and Part III of the Basic Result can be replaced by a formal proof. (Indeed, the functions $s_n{}^m$ can be shown to be primitive recursive.) We refer the reader to Davis [1958] and Kleene [1952]. Theorem V is known as the *s-m-n theorem* and is due to Kleene. Theorem V (together with Church's Thesis) is a tool of great range and power.

THEOREM 1.1. *There is a primitive recursive function* $\gamma(r, y)$ *such that, for* $n \geqq 1$,

$$[r]^A_{1+n}(y, \mathfrak{x}^{(n)}) = [\gamma(r, y)]_n{}^A(\mathfrak{x}^{(n)}).$$

Intuitively, this result may be interpreted, for $A = \phi$, $n = 1$, as declaring the existence of an algorithm[1] by means of which, given any Turing machine Z and number m, a Turing machine Z_m can be found such that

$$\Psi_{Z^{(2)}}(m, x) = \Psi_{Z_m}(x).$$

Now it is clear that there exist Turing machines Z_m satisfying this last relation since, for each fixed m, $\Psi_{Z^{(2)}}(m, x)$ is certainly a partial recursive function of x. Hence, the content of our theorem (in this special case) is that Z_m can be found effectively in terms of Z and m. However, such a Z_m can readily be described as a Turing machine which, beginning at $\alpha = q_1 1^{x+1}$, proceeds to print $\bar{m} = 1^{m+1}$ to the left, eventually arriving at $\beta = q_N 1^{m+1} B 1^{x+1}$, and then proceeds to act like Z when confronted with

[1] Actually, an algorithm given by a *primitive* recursive function.

$q_1 1^{m+1} B 1^{x+1}$. As the general case does not differ essentially from this special case, all that is required for a formal proof is a detailed construction of Z_m and a careful consideration of the Gödel numbers. The reader who wishes to omit the tedious details, and simply accept the result, may well do so.

PROOF OF THEOREM 1.1. For each value of y, let W_y be the Turing machine consisting of the following quadruples:

$$\begin{array}{l} q_1\ 1\ L\ q_1 \\ q_1\ B\ L\ q_2 \\ \left.\begin{array}{l} q_{i+1}\ B\ 1\ q_{i+1} \\ q_{i+1}\ 1\ L\ q_{i+2} \end{array}\right\} 1 \leqq i \leqq y \\ q_{y+2}\ B\ 1\ q_{y+3}. \end{array}$$

Then, with respect to W_y,

$$\begin{aligned} q_1(\overline{\mathfrak{x}^{(n)}}) &\rightarrow q_1 B(\overline{\mathfrak{x}^{(n)}}) \\ &\rightarrow q_2 BB(\overline{\mathfrak{x}^{(n)}}) \\ &\rightarrow \cdots \\ &\rightarrow q_{y+3}(\overline{y, \mathfrak{x}^{(n)}}). \end{aligned}$$

Let r be a Gödel number of a Turing machine Z, and let

$$Z_y = W_y \cup Z^{(y+2)}.\dagger$$

Then, since the quadruples of $Z^{(y+2)}$ have precisely the same effect on $q_{y+3}(\overline{y, \mathfrak{x}^{(n)}})$ that those of Z have on $q_1(\overline{y, \mathfrak{x}^{(n)}})$, we have

$$\Psi^{(n)}_{Z_y;A}(\mathfrak{x}^{(n)}) = \Psi^{(1+n)}_Z(y, \mathfrak{x}^{(n)}) = [r]^A_{1+n}(y, \mathfrak{x}^{(n)}). \qquad (1)$$

We now proceed to evaluate one of the Gödel numbers of Z_y as a function of r and y. The Gödel numbers of the quadruples that make up W_y are as follows:[1]

$$\begin{aligned} a &= \text{gn}\ (q_1\ 1\ L\ q_1) = 2^9 \cdot 3^{11} \cdot 5^5 \cdot 7^9, \\ b &= \text{gn}\ (q_1\ B\ L\ q_2) = 2^9 \cdot 3^7 \cdot 5^5 \cdot 7^{13}, \\ c(i) &= \text{gn}\ (q_{i+1}\ B\ 1\ q_{i+1}) = 2^{4i+9} \cdot 3^7 \cdot 5^{11} \cdot 7^{4i+9},\ 1 \leqq i \leqq y, \\ d(i) &= \text{gn}\ (q_{i+1}\ 1\ L\ q_{i+2}) = 2^{4i+9} \cdot 3^{11} \cdot 5^5 \cdot 7^{4i+13},\ 1 \leqq i \leqq y, \\ e(y) &= \text{gn}\ (q_{y+2}\ B\ 1\ q_{i+3}) = 2^{4y+13} \cdot 3^7 \cdot 5^{11} \cdot 7^{4y+17}. \end{aligned}$$

Thus, if we let

$$\varphi(y) = 2^a \cdot 3^b \cdot 5^{e(y)} \cdot \prod_{i=1}^{y} [\text{Pr}\ (i+3)^{c(i)}\ \text{Pr}\ (i+y+3)^{d(i)}],$$

then $\varphi(y)$ is a primitive recursive function, and, for each y, $\varphi(y)$ is a Gödel number of W_y.

We recall that the predicate IC (x), which is true if and only if x is the number associated with an internal configuration q_i, is primitive recursive, since

$$\text{IC}\ (x) \leftrightarrow \bigvee_{y=0}^{x} (x = 4y + 9).$$

Hence, the function $\iota(x)$, which is 1 when x is the number associated with a q_i and 0 otherwise, is primitive recursive. If h is the Gödel number of a quadruple, then the Gödel number of the quadruple obtained from this one by replacing each q_i by q_{i+y+2} is

$$f(h, y) = 2^{1\,\text{Gl}\,h+4y+8} \cdot 3^{2\,\text{Gl}\,h} \cdot 5^{3\,\text{Gl}\,h+(4y+8)\iota(3\,\text{Gl}\,h)} \cdot 7^{4\,\text{Gl}\,h+4y+8}.$$

Here, $f(h, y)$ is primitive recursive. Hence, if we let

$$\theta(r, y) = \prod_{i=1}^{\mathfrak{L}(r)} \text{Pr}\ (i)^{f(i\,\text{Gl}\,r,\,y)},$$

then $\theta(r, y)$ is a primitive recursive function and, for each y, $\theta(r, y)$ is a Gödel number of $Z^{(y+2)}$.

Let $\tau(x) = 1$ if x is a Gödel number of a Turing machine; 0, otherwise. Then, by (11) of Chap. 4, Sec. 1, $\tau(x)$ is primitive recursive. Finally, let

$$\gamma(r, y) = (\varphi(y) * \theta(r, y))\tau(r).$$

Then $\gamma(r, y)$ is a primitive recursive function and, for each y, $\gamma(r, y)$ is a Gödel number of Z_y. Hence, by (1),

$$[\gamma(r, y)]_n{}^A(\mathfrak{x}^{(n)}) = [r]^A_{1+n}(y, \mathfrak{x}^{(n)}). \qquad (2)$$

It remains only to consider the case where r is not a Gödel number of a Turing machine. In that case, $\gamma(r, y)$, as defined above, is 0 and, thus, is itself not the Gödel number of a Turing machine; so (2) remains correct.[1]

THEOREM 1.2 (Kleene's Iteration Theorem[2]). *For each* m *there is a primitive recursive function* $S^m(r, \mathfrak{y}^{(m)})$ *such that, for* $n \geqq 1$,

$$[r]^A_{m+n}(\mathfrak{y}^{(m)}, \mathfrak{x}^{(n)}) = [S^m(r, \mathfrak{y}^{(m)})]_n{}^A(\mathfrak{x}^{(n)}).$$

Note that Theorem 1.1 is simply Theorem 1.2 with $m = 1$.

```
section ‹The $s$-$m$-$n$ theorem›

text ‹For all $m, n > 0$ there is an $(m + 1)$-ary primitive recursive
function $s^m_n$ with
\[
  \varphi_p^{(m + n)}(c_1, \dots,c_m, x_1, \dots, x_n) =
  \varphi_{s^m_n(p, c_1, \dots,c_m)}^{(n)}(x_1, \dots, x_n)
\]
for all $p, c_1, \ldots, c_m, x_1, \ldots, x_n$. Here, $\varphi^{(n)}$ is a
function universal for $n$-ary partial recursive functions, which we will
represent by @{term "r_universal n"}›

text ‹The $s^m_n$ functions compute codes of functions. We start simple:
computing codes of the unary constant functions.›

fun code_const1 :: "nat ⇒ nat" where
  "code_const1 0 = 0"
| "code_const1 (Suc c) = quad_encode 3 1 1 (singleton_encode (code_const1 c))"

lemma code_const1: "code_const1 c = encode (r_const c)"
  by (induction c) simp_all

definition "r_code_const1_aux ≡
  Cn 3 r_prod_encode
    [r_constn 2 3,
     Cn 3 r_prod_encode
       [r_constn 2 1,
        Cn 3 r_prod_encode
          [r_constn 2 1, Cn 3 r_singleton_encode [Id 3 1]]]]"

lemma r_code_const1_aux_prim: "prim_recfn 3 r_code_const1_aux"
  by (simp_all add: r_code_const1_aux_def)

lemma r_code_const1_aux:
  "eval r_code_const1_aux [i, r, c] ↓= quad_encode 3 1 1 (singleton_encode r)"
  by (simp add: r_code_const1_aux_def)

definition "r_code_const1 ≡ r_shrink (Pr 1 Z r_code_const1_aux)"

lemma r_code_const1_prim: "prim_recfn 1 r_code_const1"
  by (simp_all add: r_code_const1_def r_code_const1_aux_prim)

lemma r_code_const1: "eval r_code_const1 [c] ↓= code_const1 c"
proof -
  let ?h = "Pr 1 Z r_code_const1_aux"
  have "eval ?h [c, x] ↓= code_const1 c" for x
    using r_code_const1_aux r_code_const1_def
    by (induction c) (simp_all add: r_code_const1_aux_prim)
  then show ?thesis by (simp add: r_code_const1_def r_code_const1_aux_prim)
qed

text ‹Functions that compute codes of higher-arity constant functions:›

definition code_constn :: "nat ⇒ nat ⇒ nat" where
  "code_constn n c ≡
    if n = 1 then code_const1 c
    else quad_encode 3 n (code_const1 c) (singleton_encode (triple_encode 2 n 0))"

lemma code_constn: "code_constn (Suc n) c = encode (r_constn n c)"
  unfolding code_constn_def using code_const1 r_constn_def
  by (cases "n = 0") simp_all

definition r_code_constn :: "nat ⇒ recf" where
  "r_code_constn n ≡
     if n = 1 then r_code_const1
     else
       Cn 1 r_prod_encode
         [r_const 3,
          Cn 1 r_prod_encode
            [r_const n,
             Cn 1 r_prod_encode
               [r_code_const1,
                Cn 1 r_singleton_encode
                  [Cn 1 r_prod_encode
                    [r_const 2, Cn 1 r_prod_encode [r_const n, Z]]]]]]"

lemma r_code_constn_prim: "prim_recfn 1 (r_code_constn n)"
  by (simp_all add: r_code_constn_def r_code_const1_prim)

lemma r_code_constn: "eval (r_code_constn n) [c] ↓= code_constn n c"
  by (auto simp add: r_code_constn_def r_code_const1 code_constn_def r_code_const1_prim)

text ‹Computing codes of $m$-ary projections:›

definition code_id :: "nat ⇒ nat ⇒ nat" where
  "code_id m n ≡ triple_encode 2 m n"

lemma code_id: "encode (Id m n) = code_id m n"
  unfolding code_id_def by simp

text ‹The functions $s^m_n$ are represented by the following function.
The value $m$ corresponds to the length of @{term "cs"}.›

definition smn :: "nat ⇒ nat ⇒ nat list ⇒ nat" where
  "smn n p cs ≡ quad_encode
     3
     n
     (encode (r_universal (n + length cs)))
     (list_encode (code_constn n p # map (code_constn n) cs @ map (code_id n) [0..<n]))"

lemma smn:
  assumes "n > 0"
  shows "smn n p cs = encode
   (Cn n
     (r_universal (n + length cs))
     (r_constn (n - 1) p # map (r_constn (n - 1)) cs @ (map (Id n) [0..<n])))"
proof -
  let ?p = "r_constn (n - 1) p"
  let ?gs1 = "map (r_constn (n - 1)) cs"
  let ?gs2 = "map (Id n) [0..<n]"
  let ?gs = "?p # ?gs1 @ ?gs2"
  have "map encode ?gs1 = map (code_constn n) cs"
    by (intro nth_equalityI; auto; metis code_constn assms Suc_pred)
  moreover have "map encode ?gs2 = map (code_id n) [0..<n]"
    by (rule nth_equalityI) (auto simp add: code_id_def)
  moreover have "encode ?p = code_constn n p"
    using assms code_constn[of "n - 1" p] by simp
  ultimately have "map encode ?gs =
      code_constn n p # map (code_constn n) cs @ map (code_id n) [0..<n]"
    by simp
  then show ?thesis
    unfolding smn_def using assms encode.simps(4) by presburger
qed

text ‹The next function is to help us define @{typ recf}s corresponding
to the $s^m_n$ functions. It maps $m + 1$ arguments $p, c_1, \ldots, c_m$ to
an encoded list of length $m + n + 1$. The list comprises the $m + 1$ codes
of the $n$-ary constants $p, c_1, \ldots, c_m$ and the $n$ codes for all
$n$-ary projections.›

definition r_smn_aux :: "nat ⇒ nat ⇒ recf" where
   list_encode (map (code_constn n) (p # cs) @ map (code_id n) [0..<n])"
proof -
  let ?xs = "map (λi. Cn (Suc m) (r_code_constn n) [Id (Suc m) i]) [0..<Suc m]"
  let ?ys = "map (λi. r_constn m (code_id n i)) [0..<n]"
  have len_xs: "length ?xs = Suc m" by simp

  have map_xs: "map (λg. eval g (p # cs)) ?xs = map Some (map (code_constn n) (p # cs))"
  proof (intro nth_equalityI)
    show len: "length (map (λg. eval g (p # cs)) ?xs) =
        length (map Some (map (code_constn n) (p # cs)))"
      by (simp add: assms(2))

    have "map (λg. eval g (p # cs)) ?xs ! i = map Some (map (code_constn n) (p # cs)) ! i"
        if "i < Suc m" for i
    proof -
      have "map (λg. eval g (p # cs)) ?xs ! i = (λg. eval g (p # cs)) (?xs ! i)"
        using len_xs that by (metis nth_map)
      also have "... = eval (Cn (Suc m) (r_code_constn n) [Id (Suc m) i]) (p # cs)"
        using that len_xs
        by (metis (no_types, lifting) add.left_neutral length_map nth_map nth_upt)
      also have "... = eval (r_code_constn n) [the (eval (Id (Suc m) i) (p # cs))]"
        using r_code_constn_prim assms(2) that by simp
      also have "... = eval (r_code_constn n) [(p # cs) ! i]"
        using len that by simp
      finally have "map (λg. eval g (p # cs)) ?xs ! i ↓= code_constn n ((p # cs) ! i)"
        using r_code_constn by simp
      then show ?thesis
        using len_xs len that by (metis length_map nth_map)
    qed
    moreover have "length (map (λg. eval g (p # cs)) ?xs) = Suc m" by simp
    ultimately show "⋀i. i < length (map (λg. eval g (p # cs)) ?xs) ⟹
        map (λg. eval g (p # cs)) ?xs ! i =
        map Some (map (code_constn n) (p # cs)) ! i"
      by simp
  qed
  moreover have "map (λg. eval g (p # cs)) ?ys = map Some (map (code_id n) [0..<n])"
    using assms(2) by (intro nth_equalityI; auto)
  ultimately have "map (λg. eval g (p # cs)) (?xs @ ?ys) =
      map Some (map (code_constn n) (p # cs) @ map (code_id n) [0..<n])"
    by (metis map_append)
  moreover have "map (λx. the (eval x (p # cs))) (?xs @ ?ys) =
      map the (map (λx. eval x (p # cs)) (?xs @ ?ys))"
    by simp
  ultimately have *: "map (λg. the (eval g (p # cs))) (?xs @ ?ys) =
      (map (code_constn n) (p # cs) @ map (code_id n) [0..<n])"
    by simp

  have "∀i<length ?xs. eval (?xs ! i) (p # cs) = map (λg. eval g (p # cs)) ?xs ! i"
    by (metis nth_map)
  then have
    "∀i<length ?xs. eval (?xs ! i) (p # cs) = map Some (map (code_constn n) (p # cs)) ! i"
    using map_xs by simp
  then have "∀i<length ?xs. eval (?xs ! i) (p # cs) ↓"
    using assms map_xs by (metis length_map nth_map option.simps(3))
  then have xs_converg: "∀z∈set ?xs. eval z (p # cs) ↓"
    by (metis in_set_conv_nth)

  have "∀i<length ?ys. eval (?ys ! i) (p # cs) = map (λx. eval x (p # cs)) ?ys ! i"
    by simp
  then have
    "∀i<length ?ys. eval (?ys ! i) (p # cs) = map Some (map (code_id n) [0..<n]) ! i"
    using assms(2) by simp
  then have "∀i<length ?ys. eval (?ys ! i) (p # cs) ↓"
    by simp
  then have "∀z∈set (?xs @ ?ys). eval z (p # cs) ↓"
    using xs_converg by auto
  moreover have "recfn (length (p # cs)) (Cn (Suc m) (r_list_encode (m + n)) (?xs @ ?ys))"
    using assms r_code_constn_prim by auto
  ultimately have "eval (r_smn_aux n m) (p # cs) =
      eval (r_list_encode (m + n)) (map (λg. the (eval g (p # cs))) (?xs @ ?ys))"
    unfolding r_smn_aux_def using assms by simp
  then have "eval (r_smn_aux n m) (p # cs) =
      eval (r_list_encode (m + n)) (map (code_constn n) (p # cs) @ map (code_id n) [0..<n])"
    using * by metis
  moreover have "length (?xs @ ?ys) = Suc (m + n)" by simp
  ultimately show ?thesis
    using r_list_encode * assms(1) by (metis (no_types, lifting) length_map)
qed

text ‹For all $m, n > 0$, the @{typ recf} corresponding to $s^m_n$ is
given by the next function.›

definition r_smn :: "nat ⇒ nat ⇒ recf" where
 "r_smn n m ≡
    Cn (Suc m) r_prod_encode
     [r_constn m 3,
      Cn (Suc m) r_prod_encode
       [r_constn m n,
        Cn (Suc m) r_prod_encode
          [r_constn m (encode (r_universal (n + m))), r_smn_aux n m]]]"

lemma r_smn_prim [simp]: "n > 0 ⟹ prim_recfn (Suc m) (r_smn n m)"
  by (simp_all add: r_smn_def r_smn_aux_prim)

lemma r_smn:
  assumes "n > 0" and "length cs = m"
  shows "eval (r_smn n m) (p # cs) ↓= smn n p cs"
  using assms r_smn_def r_smn_aux smn_def r_smn_aux_prim by simp

lemma map_eval_Some_the:
  assumes "map (λg. eval g xs) gs = map Some ys"
  shows "map (λg. the (eval g xs)) gs = ys"
  using assms
  by (metis (no_types, lifting) length_map nth_equalityI nth_map option.sel)

text ‹The essential part of the $s$-$m$-$n$ theorem: For all $m, n > 0$
the function $s^m_n$ satisfies
\[
  \varphi_p^{(m + n)}(c_1, \dots,c_m, x_1, \dots, x_n) =
  \varphi_{s^m_n(p, c_1, \dots,c_m)}^{(n)}(x_1, \dots, x_n)
\] for all $p, c_i, x_j$.›

lemma smn_lemma:
  assumes "n > 0" and len_cs: "length cs = m" and len_xs: "length xs = n"
  shows "eval (r_universal (m + n)) (p # cs @ xs) =
    eval (r_universal n) ((the (eval (r_smn n m) (p # cs))) # xs)"
proof -
  let ?s = "r_smn n m"
  let ?f = "Cn n
    (r_universal (n + length cs))
    (r_constn (n - 1) p # map (r_constn (n - 1)) cs @ (map (Id n) [0..<n]))"
  have "eval ?s (p # cs) ↓= smn n p cs"
    using assms r_smn by simp
  then have eval_s: "eval ?s (p # cs) ↓= encode ?f"
    by (simp add: assms(1) smn)

  have "recfn n ?f"
    using len_cs assms by auto
  then have *: "eval (r_universal n) ((encode ?f) # xs) = eval ?f xs"
    using r_universal[of ?f n, OF _ len_xs] by simp

  let ?gs = "r_constn (n - 1) p # map (r_constn (n - 1)) cs @ map (Id n) [0..<n]"
    show "length (map (λg. the (eval g xs)) ?gs) = length (p # cs @ xs)"
      by (simp add: len_xs)
    have len: "length (map (λg. the (eval g xs)) ?gs) = Suc (m + n)"
      by (simp add: len_cs)
    moreover have "map (λg. the (eval g xs)) ?gs ! i = (p # cs @ xs) ! i"
      if "i < Suc (m + n)" for i
    proof -
      from that consider "i = 0" | "i > 0 ∧ i < Suc m" | "Suc m ≤ i ∧ i < Suc (m + n)"
        using not_le_imp_less by auto
      then show ?thesis
      proof (cases)
        case 1
        then show ?thesis using assms(1) len_xs by simp
      next
        case 2
        then have "?gs ! i = (map (r_constn (n - 1)) cs) ! (i - 1)"
          using len_cs
          by (metis One_nat_def Suc_less_eq Suc_pred length_map
            less_numeral_extra(3) nth_Cons' nth_append)
        then have "map (λg. the (eval g xs)) ?gs ! i =
            (λg. the (eval g xs)) ((map (r_constn (n - 1)) cs) ! (i - 1))"
          using len by (metis length_map nth_map that)
        also have "... = the (eval ((r_constn (n - 1) (cs ! (i - 1)))) xs)"
          using 2 len_cs by auto
        also have "... = cs ! (i - 1)"
          using r_constn len_xs assms(1) by simp
        also have "... = (p # cs @ xs) ! i"
          using 2 len_cs
          by (metis diff_Suc_1 less_Suc_eq_0_disj less_numeral_extra(3) nth_Cons' nth_append)
        finally show ?thesis .
      next
        case 3
        then have "?gs ! i = (map (Id n) [0..<n]) ! (i - Suc m)"
          using len_cs
          by (simp; metis (no_types, lifting) One_nat_def Suc_less_eq add_leE
            plus_1_eq_Suc diff_diff_left length_map not_le nth_append
            ordered_cancel_comm_monoid_diff_class.add_diff_inverse)
        then have "map (λg. the (eval g xs)) ?gs ! i =
            (λg. the (eval g xs)) ((map (Id n) [0..<n]) ! (i - Suc m))"
          using len by (metis length_map nth_map that)
        also have "... = the (eval ((Id n (i - Suc m))) xs)"
          using 3 len_cs by auto
        also have "... = xs ! (i - Suc m)"
          using len_xs 3 by auto
        also have "... = (p # cs @ xs) ! i"
          using len_cs len_xs 3
          by (metis diff_Suc_1 diff_diff_left less_Suc_eq_0_disj not_le nth_Cons'
            nth_append plus_1_eq_Suc)
        finally show ?thesis .
      qed
    qed
    ultimately show "map (λg. the (eval g xs)) ?gs ! i = (p # cs @ xs) ! i"
        if "i < length (map (λg. the (eval g xs)) ?gs)" for i
      using that by simp
  qed
  ultimately show ?thesis by simp
qed

theorem smn_theorem:
  assumes "n > 0"
  shows "∃s. prim_recfn (Suc m) s ∧
    (∀p cs xs. length cs = m ∧ length xs = n ⟶
        eval (r_universal (m + n)) (p # cs @ xs) =
        eval (r_universal n) ((the (eval s (p # cs))) # xs))"
  using smn_lemma exI[of _ "r_smn n m"] assms by simp
```

Synthetic mathematics to the rescue

Analytic mathematics

Objects of the logic | model | structures under investigation

Synthetic mathematics to the rescue

Analytic mathematics

Objects of the logic — model — structures under investigation

Synthetic mathematics*

Objects of the logic — are turned into — structures under investigation

via axioms

*only possible in constructive mathematics

Synthetic mathematics to the rescue

Analytic mathematics

Objects of the logic | model | structures under investigation

Synthetic mathematics*

Objects of the logic | are turned into | structures under investigation

via axioms

*only possible in constructive mathematics

Constructive mathematics to the rescue

Church-Turing thesis:

"Every intuitively computable function is μ-recursive."

Kreisel [1965]

Constructive mathematics to the rescue

Church-Turing thesis:
"Every intuitively computable function is μ-recursive."

as an axiom in constructive mathematics

$$\text{CT} := \forall f : \mathbb{N} \to \mathbb{N}.\ \exists c : \mathbb{N}.\ \textit{the } c\textit{-th } \mu\textit{-recursive function computes } f$$

Kreisel [1965]

Overview

1. Axiom-free “synthetic” computability
2. The axiom CT and its status in Coq
3. Fully Synthetic Computability á la Richman and Bauer
4. Synthetic Computability without choice
5. Synthetic Oracle Computability
6. More results
7. The Coq Library of Undecidability Proofs

Definitions

Decidability

$\exists f : \mathbb{N} \to \mathbb{B}. \forall x.\ px \leftrightarrow fx = \text{true}$ $\wedge\ f$ *is computable*

$\exists f : \mathbb{N} \to \mathbb{B}. \forall x.\ px \leftrightarrow fx = \text{true}$

Definitions

Decidability

$\exists f : \mathbb{N} \to \mathbb{B}. \forall x.\ px \leftrightarrow fx = \text{true}$ $\quad$ $\exists f : \mathbb{N} \to \mathbb{B}. \forall x.\ px \leftrightarrow fx = \text{true}$

$\wedge\ f$ *is computable*

Semi-decidability

$\exists f : \mathbb{N} \rightharpoonup \mathbb{N}. \forall x.\ px \leftrightarrow fx \downarrow$ $\quad$ $\exists f : \mathbb{N} \to \mathbb{B}. \forall x.\ px \leftrightarrow fx \downarrow$

$\wedge\ f$ *is computable*

Definitions

Decidability

$\exists f : \mathbb{N} \to \mathbb{B}. \forall x.\ px \leftrightarrow fx = \text{true}$ $\exists f : \mathbb{N} \to \mathbb{B}. \forall x.\ px \leftrightarrow fx = \text{true}$

$\land\ f$ *is computable*

Semi-decidability

$\exists f : \mathbb{N} \rightharpoonup \mathbb{N}. \forall x.\ px \leftrightarrow fx \downarrow$ $\exists f : \mathbb{N} \to \mathbb{B}. \forall x.\ px \leftrightarrow fx \downarrow$

$\land\ f$ *is computable*

Many-one reducibility

$\exists f : \mathbb{N} \to \mathbb{N}. \forall x.\ px \leftrightarrow q(fx)$ $\exists f : \mathbb{N} \to \mathbb{N}. \forall x.\ px \leftrightarrow q(fx)$

$\land\ f$ *is computable*

Definitions

Decidability

$\exists f : \mathbb{N} \to \mathbb{B}. \forall x.\ px \leftrightarrow fx = \text{true}$ $\quad$ $\exists f : \mathbb{N} \to \mathbb{B}. \forall x.\ px \leftrightarrow fx = \text{true}$

$\land$ f *is computable*

Semi-decidability

$\exists f : \mathbb{N} \rightharpoonup \mathbb{N}. \forall x.\ px \leftrightarrow fx \downarrow$ $\quad$ $\exists f : \mathbb{N} \to \mathbb{B}. \forall x.\ px \leftrightarrow fx \downarrow$

$\land$ f *is computable*

Many-one reducibility

$\exists f : \mathbb{N} \to \mathbb{N}. \forall x.\ px \leftrightarrow q(fx)$ $\quad$ $\exists f : \mathbb{N} \to \mathbb{N}. \forall x.\ px \leftrightarrow q(fx)$

$\land$ f *is computable*

Enumerability, one-one reducibility, truth-table reducibility, …

Myhill isomorphism theorem

Theorem

Let X and Y be enumerable discrete types, $p : X \to \mathbb{P}$, and $q : Y \to \mathbb{P}$. If $p \preceq_1 q$ and $q \preceq_1 p$, then there exist $f : X \to Y$ and $g : Y \to X$ such that for all $x : X$ and $y : Y$:

$$px \leftrightarrow q(fx), \quad qy \leftrightarrow p(gy), \quad g(fx) = x, \quad f(gy) = y$$

jww Felix Jahn and Gert Smolka [CPP '23]

Post's theorem

Theorem (Post 1944)

$p : \mathbb{N} \to \mathbb{P}$ is decidable if it is semi-decidable and its complement is

Post's theorem

Theorem (Post 1944, Troelstra van Dalen 1988)

$p : \mathbb{N} \to \mathbb{P}$ is decidable if it is semi-decidable and its complement is
is equivalent to
Markov's principle $\forall f : \mathbb{N} \to \mathbb{B}.\ \neg\neg(\exists n.\ f n = \text{true}) \to \exists n.\ f n = \text{true}$

CT is inconsistent in classical systems...

$$\mathsf{CT} := \forall f : \mathbb{N} \to \mathbb{N}.\ \exists c : \mathbb{N}.\ \forall x.\ \varphi_c x \downarrow f x$$

...because the characteristic function of the self-halting problem is not general recursive.

$$f n := \textbf{ if } \varphi_n n \downarrow \textbf{ then } 1 \textbf{ else } 0$$

Troelstra and van Dalen [1988]

CT is inconsistent in classical systems…

$$\text{CT} := \forall f : \mathbb{N} \to \mathbb{N}.\ \exists c : \mathbb{N}.\ \forall x.\ \varphi_c x \downarrow fx$$

…because the characteristic function of the self-halting problem is not general recursive.

$$fn := \textbf{ if } \varphi_n n \downarrow \textbf{ then } 1 \textbf{ else } 0$$

Formally in ZF:

$$f := \{(n,1) \mid \varphi_n n \downarrow\} \cup \{(n,0) \mid \varphi_n n \uparrow\}$$

Now f is a total functional relation because f is …

☑ functional

☐ total

Troelstra and van Dalen [1988]

CT is inconsistent in classical systems…

$$\text{CT} := \forall f : \mathbb{N} \to \mathbb{N}.\ \exists c : \mathbb{N}.\ \forall x.\ \varphi_c x \downarrow f x$$

…because the characteristic function of the self-halting problem is not general recursive.

$$f n := \textbf{if } \varphi_n n \downarrow \textbf{ then } 1 \textbf{ else } 0$$

Formally in ZF:

$$f := \{(n, 1) \mid \varphi_n n \downarrow\} \cup \{(n, 0) \mid \varphi_n n \uparrow\}$$

Now f is a total functional relation because f is …

☑ functional

☑ total (proof by contradiction, i.e. LEM)

Troelstra and van Dalen [1988]

CT is inconsistent in classical systems...

$$\text{CT} := \forall f : \mathbb{N} \to \mathbb{N}.\ \exists c : \mathbb{N}.\ \forall x.\ \varphi_c x \downarrow fx$$

...because the characteristic function of the self-halting problem is not general recursive.

$$fn := \textbf{ if } \varphi_n n \downarrow \textbf{ then } 1 \textbf{ else } 0$$

Formally in ZF:

$$f := \{(n, 1) \mid \varphi_n n \downarrow\} \cup \{(n, 0) \mid \varphi_n n \uparrow\}$$

Now f is a total set-theoretic function because f is ...

☑ functional

☑ total (proof by contradiction, i.e. LEM)

Troelstra and van Dalen [1988]

CT is consistent in constructive systems

$$\mathsf{CT} := \forall f : \mathbb{N} \to \mathbb{N}.\, f \textit{ is general recursive}$$

- Heyting arithmetic, Kleene [1945]
- Russian style constructive mathematics, Markov [1954]
- HoTT (MLTT + propositional truncation + univalence), Swan and Uemura [2019]
- MLTT, Pédrot [2024]

Slogans of (Coq's) Type Theory

Types and functions are native

- Inductive types $\mathbb{N}$, $\mathbb{B}$, $A \times B$ and so on
- The function type $A \to B$ consists exactly of programs in a *total*, strongly typed programming language

Propositions behave constructively

- Propositions are types
- Proofs are programs
- (Total, functional) relations are functions $A \to B \to \mathbb{P}$
- Classical principles are independent:

$$\text{DNE} := \forall P : \mathbb{P}.\ \neg\neg P \to P \qquad \text{LEM} := \forall P : \mathbb{P}.\ P \vee \neg P$$

Slogans of (Coq's) Type Theory CIC

Types and functions are native

- Inductive types $\mathbb{N}$, $\mathbb{B}$, $A \times B$ and so on
- The function type $A \to B$ consists exactly of programs in a *total*, strongly typed programming language

Propositions behave constructively

- Propositions are types in a separate, impredicative universe $\mathbb{P}$
- Proofs are programs, no large eliminations from $\mathbb{P}$ to $\mathbb{T}$
- (Total, functional) relations are functions $A \to B \to \mathbb{P}$
- Classical principles are independent:

$$\text{DNE} := \forall P : \mathbb{P}.\ \neg\neg P \to P \qquad \text{LEM} := \forall P : \mathbb{P}.\ P \vee \neg P$$

CT is not inconsistent in CIC

$$f n := \textbf{if } \varphi_n n \downarrow \textbf{ then } \text{true} \textbf{ else } \text{false}$$

CT is not inconsistent in CIC

$$f n := \textbf{if } \varphi_n n \downarrow \textbf{ then } \text{true } \textbf{else } \text{false}$$

decision can not be implemented

CT is not inconsistent in CIC

$$f n := \textbf{if } \varphi_n n \downarrow \textbf{ then } \text{true } \textbf{else} \text{ false}$$

However, we can define the graph relation $G : \mathbb{N} \to \mathbb{B} \to \mathbb{P}$

$$G n b := \varphi_n n \downarrow \leftrightarrow b = \text{true}$$

CT is not inconsistent in CIC

$$f n := \textbf{if } \varphi_n n \downarrow \textbf{ then } \text{true} \textbf{ else } \text{false}$$

However, we can define the graph relation $G : \mathbb{N} \to \mathbb{B} \to \mathbb{P}$

$$G n b := \varphi_n n \downarrow \leftrightarrow b = \text{true}$$

☑ G is functional

☐ G is total

CT is not inconsistent in CIC

$$f n := \textbf{if } \varphi_n n \downarrow \textbf{ then } \text{true } \textbf{else } \text{false}$$

However, we can define the graph relation $G : \mathbb{N} \to \mathbb{B} \to \mathbb{P}$

$$G n b := \varphi_n n \downarrow \leftrightarrow b = \text{true}$$

☑ G is functional

☑ G is total (using proof by contradiction, i.e. LEM)

Relations to functions: Choice principles

The axiom of choice: “every total relation contains a function”

$$\mathsf{AC}_{A,B} := \forall R : A \to B \to \mathbb{P}.(\forall a.\exists b.\ Rab) \to \exists f : A \to B.\forall a.\ Ra(fa)$$

Relations to functions: Choice principles

The axiom of choice: “every total relation contains a function”

$$\mathsf{AC}_{A,B} := \forall R : A \to B \to \mathbb{P}.(\forall a.\exists b.\ Rab) \to \exists f : A \to B.\forall a.\ Ra(fa)$$

Curry Howard isomorphism:

A proof of $\exists b.pb$ is a pair.

A proof of $\forall a.pa$ is a function.

Relations to functions: Choice principles

The axiom of choice: “every total relation contains a function”

$$\mathsf{AC}_{A,B} := \forall R : A \to B \to \mathbb{P}.(\forall a.\exists b.\ Rab) \to \exists f : A \to B.\forall a.\ Ra(fa)$$

Curry Howard isomorphism:

A proof of $\exists b.pb$ is a pair.

A proof of $\forall a.pa$ is a function.

A proof of $\forall a.\exists b.\ Rab$ is a function returning a pair.

Relations to functions: Choice principles

The axiom of choice: “every total relation contains a function”

$$\text{AC}_{A,B} := \forall R : A \to B \to \mathbb{P}.(\forall a.\exists b.\ Rab) \to \exists f : A \to B.\forall a.\ Ra(fa)$$

Curry Howard isomorphism:

A proof of $\exists b.pb$ is a pair.

A proof of $\forall a.pa$ is a function.

A proof of $\forall a.\exists b.\ Rab$ is a function returning a pair.

- ☑ $\forall p : (\exists a.\ Ba) \to \mathbb{P}.\ (\forall (a : A)(b : Ba).\ p(a, b)) \to \forall (s : \exists a.\ Ba).\ ps$
- ☐ $\forall p : (\exists a.\ Ba) \to \mathbb{T}.\ (\forall (a : A)(b : Ba).\ p(a, b)) \to \forall (s : \exists a.\ Ba).\ ps$
- ☐ $\pi_1 : (\exists a.\ Ba) \to A$

Relations to functions: Choice principles

The axiom of choice: "every total relation contains a function"

$$\mathsf{AC}_{A,B} := \forall R : A \to B \to \mathbb{P}.(\forall a.\exists b.\ Rab) \to \exists f : A \to B.\forall a.\ Ra(fa)$$

Curry Howard isomorphism:

A proof of $\exists b.pb$ is a pair.

A proof of $\forall a.pa$ is a function.

A proof of $\forall a.\exists b.\ Rab$ is a function returning a pair.

☑ $\forall p : (\exists a.\ Ba) \to \mathbb{P}.\ (\forall (a : A)(b : Ba).\ p(a,b)) \to \forall (s : \exists a.\ Ba).\ ps$

☒ $\forall p : (\exists a.\ Ba) \to \mathbb{T}.\ (\forall (a : A)(b : Ba).\ p(a,b)) \to \forall (s : \exists a.\ Ba).\ ps$

☐ $\pi_1 : (\exists a.\ Ba) \to A$

Relations to functions: Choice principles

The axiom of choice: "every total relation contains a function"

$$\text{AC}_{A,B} := \forall R : A \to B \to \mathbb{P}.(\forall a.\exists b.\ Rab) \to \exists f : A \to B.\forall a.\ Ra(fa)$$

Curry Howard isomorphism:

A proof of $\exists b.pb$ is a pair.

A proof of $\forall a.pa$ is a function.

A proof of $\forall a.\exists b.\ Rab$ is a function returning a pair.

☑ $\forall p : (\exists a.\ Ba) \to \mathbb{P}.\ (\forall (a : A)(b : Ba).\ p(a, b)) \to \forall (s : \exists a.\ Ba).\ ps$

☒ $\forall p : (\exists a.\ Ba) \to \mathbb{T}.\ (\forall (a : A)(b : Ba).\ p(a, b)) \to \forall (s : \exists a.\ Ba).\ ps$

☒ $\pi_1 : (\exists a.\ Ba) \to A$

Relations to functions: Choice principles

The axiom of choice: "every total relation contains a function"

$$\mathsf{AC}_{A,B} := \forall R : A \to B \to \mathbb{P}.(\forall a.\exists b.\ Rab) \to \exists f : A \to B.\forall a.\ Ra(fa)$$

Theorem

The law of excluded middle and the axiom of countable choice together are inconsistent with CT:

$$\mathsf{LEM} \wedge \mathsf{AC}_{\mathbb{N},\mathbb{B}} \to \neg\mathsf{CT}$$

Which axioms keep CIC computational?

$$\mathsf{LEM} \land \mathsf{AC}_{\mathbb{N},\mathbb{B}} \to \neg\mathsf{CT}$$

- Can one of the assumptions be dropped? (No)
- Can one of the assumptions be weakened? (Yes)
- How much?

Weak(est) classical logical and choice principles

Theorem

$$\begin{array}{c} \text{LEM} \\ \land \\ \text{AC}_{\mathbb{N},\mathbb{B}} \end{array} \rightarrow \neg\text{CT}$$

Weak(est) classical logical and choice principles

Theorem

$$\mathsf{LEM} \land \forall R : \mathbb{N} \to \mathbb{B} \to \mathbb{P}.\ (\forall n. \exists\, b.\ Rnb) \to \exists f. \forall n.\ Rn(fn) \to \neg\mathsf{CT}$$

Weak(est) classical logical and choice principles

Theorem

$$\mathsf{LEM} \land \forall R : \mathbb{N} \to \mathbb{B} \to \mathbb{P}.\ (\forall n.\exists! b.\ Rnb) \to \exists f.\forall n.\ Rn(fn) \to \neg\mathsf{CT}$$

Weak(est) classical logical and choice principles

Theorem

$$\begin{array}{c}\text{LEM}\\ \wedge\\ \text{AUC}_{\mathbb{N},\mathbb{B}}\end{array} \to \neg\text{CT}$$

AUC: Axiom of unique choice

Weak(est) classical logical and choice principles

Theorem

$$\left(\forall P : \mathbb{P}.\ P \lor \neg P \;\land\; \mathsf{AUC}_{\mathbb{N},\mathbb{B}}\right) \to \neg\mathsf{CT}$$

AUC: Axiom of unique choice

Weak(est) classical logical and choice principles

Theorem

$$\forall f : \mathbb{N} \to \mathbb{B}. \quad (\exists n.\ fn = \mathsf{true}) \lor \neg(\exists n.\ fn = \mathsf{true}) \land \mathsf{AUC}_{\mathbb{N},\mathbb{B}} \to \neg\mathsf{CT}$$

AUC: Axiom of unique choice

Weak(est) classical logical and choice principles

Theorem

$$\forall f : \mathbb{N} \to \mathbb{B}.\ \neg\neg(\exists n.\ fn = \text{true}) \vee \neg(\exists n.\ fn = \text{true})$$

$$\wedge \qquad \to \neg\text{CT}$$

$$\text{AUC}_{\mathbb{N},\mathbb{B}}$$

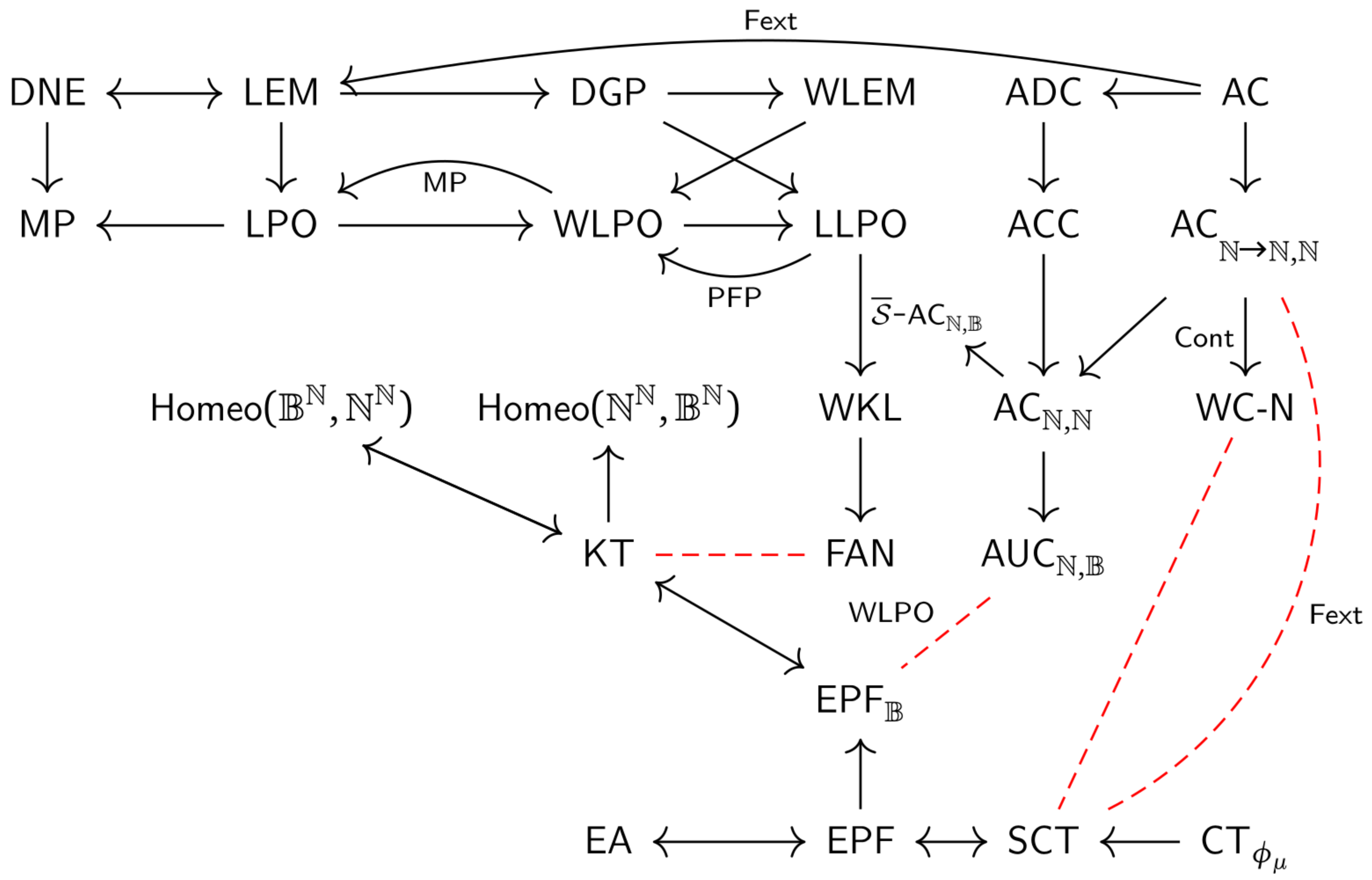
AUC: Axiom of unique choice

Weak(est) classical logical and choice principles

Theorem

$$\mathsf{WLPO} \land \mathsf{AUC}_{\mathbb{N},\mathbb{B}} \to \neg\mathsf{CT}$$

AUC: Axiom of unique choice
WLPO: Weak limited principle of omniscience



Fext
DNE
LEM
DGP
WLEM
ADC
AC
MP
MP
LPO
WLPO
LLPO
ACC
AC_{ℕ→ℕ,ℕ}
PFP
S̄-AC_{ℕ,𝔹}
Cont
Homeo(𝔹^ℕ, ℕ^ℕ)
Homeo(ℕ^ℕ, 𝔹^ℕ)
WKL
AC_{ℕ,ℕ}
WC-N
KT
FAN
AUC_{ℕ,𝔹}
WLPO
Fext
EPF_𝔹
EA
EPF
SCT
CT_{φ_μ}

Synthetic computability á la Richman

$\phi_c x$ is the value of the c-th μ-recursive function with input x

$$\mathsf{CT} \;:=\; \forall f : \mathbb{N} \to \mathbb{N}.\ \exists c : \mathbb{N}.\ \forall x.\ \phi_c x \rhd f x$$

Synthetic computability á la Richman

$$\mathsf{CT}' := \exists \phi. \forall f : \mathbb{N} \to \mathbb{N}.\ \exists c : \mathbb{N}.\ \forall x.\ \phi_c x \triangleright f x$$

Synthetic computability á la Richman, Bridges, and Bauer

$$\mathsf{CT}' := \exists \phi. \forall f : \mathbb{N} \to \mathbb{N}.\ \exists c : \mathbb{N}.\ \forall x.\ \phi_c x \triangleright f x$$

1967 Hartley Rogers' computability book is essentially synthetic

1983 Basic results in computable analysis by Richman

1987 More results in computable analysis by Bridges and Richman

2010 First steps in computability theory by Bauer, working in Hyland's effective topos

Synthetic computability á la Richman, Bridges, and Bauer

$$\text{CT}' := \exists \phi. \forall f : \mathbb{N} \to \mathbb{N}.\ \exists c : \mathbb{N}.\ \forall x.\ \phi_c x \triangleright f x$$

1967 Hartley Rogers' computability book is essentially synthetic

1983 Basic results in computable analysis by Richman

1987 More results in computable analysis by Bridges and Richman

2010 First steps in computability theory by Bauer, working in Hyland's effective topos

All assume the axiom of countable choice, resulting in

Theorem

There is an s^m_n operator for currying.

Synthetic computability á la Richman, Bridges, and Bauer

$$\mathsf{CT}' := \exists \phi. \forall f : \mathbb{N} \to \mathbb{N}.\ \exists c : \mathbb{N}.\ \forall x.\ \phi_c x \triangleright f x$$

1967 Hartley Rogers' computability book is essentially synthetic

1983 Basic results in computable analysis by Richman

1987 More results in computable analysis by Bridges and Richman

2010 First steps in computability theory by Bauer, working in Hyland's effective topos

All assume the axiom of countable choice, resulting in

Theorem

The law of excluded middle is false: $\neg(\forall P : \mathbb{P}.\ P \vee \neg P)$

Synthetic computability á la Richman, Bridges, and Bauer

$$\mathsf{CT}' := \exists \phi. \forall f : \mathbb{N} \to \mathbb{N}.\ \exists c : \mathbb{N}.\ \forall x.\ \phi_c x \rhd f x$$

1967 Hartley Rogers' computability book is essentially synthetic

1983 Basic results in computable analysis by Richman

1987 More results in computable analysis by Bridges and Richman

2010 First steps in computability theory by Bauer, working in Hyland's effective topos

Bridges and Richman [1987] remark

> *countable choice can be avoided by postulating an s^m_n operator*

Synthetic computability without choice

Assume

1. a (partial) function ϕ
2. universal for $\mathbb{N} \to \mathbb{N}$: $\forall f : \mathbb{N} \to \mathbb{N}. \exists c : \mathbb{N}. \forall x.\ \phi_c x \triangleright f x$,
3. a function $s : \mathbb{N} \to \mathbb{N} \to \mathbb{N}$
4. with the property that $\phi_{s(c,x)} y \equiv \phi_c \langle x, y \rangle$.

Equivalently, using *parametrical* universality

$$\mathsf{SCT} := \exists \phi.\ \forall f : \mathbb{N} \to \mathbb{N} \to \mathbb{N}. \exists \gamma : \mathbb{N} \to \mathbb{N}. \forall i.\ \phi_{\gamma i} \equiv f_i$$

Synthetic computability without choice

Assume

1. a (partial) function ϕ
2. universal for $\mathbb{N} \to \mathbb{N}$: $\forall f : \mathbb{N} \to \mathbb{N}. \exists c : \mathbb{N}. \forall x.\ \phi_c x \triangleright f x$,
3. a function $s : \mathbb{N} \to \mathbb{N} \to \mathbb{N}$
4. with the property that $\phi_{s(c,x)} y \equiv \phi_c \langle x, y \rangle$.

Equivalently, using *parametrical* universality

$$\text{SCT} := \exists \phi.\ \forall f : \mathbb{N} \to \mathbb{N} \to \mathbb{N}. \exists \gamma : \mathbb{N} \to \mathbb{N}. \forall i.\ \phi_{\gamma i} \equiv f_i$$

or using parameterised partial functions $\mathbb{N} \to \mathbb{N} \rightharpoonup \mathbb{N}$ (EPF),

Synthetic computability without choice

Assume

1. a (partial) function ϕ
2. universal for $\mathbb{N} \to \mathbb{N}$: $\forall f : \mathbb{N} \to \mathbb{N}. \exists c : \mathbb{N}. \forall x.\ \phi_c x \triangleright f x$,
3. a function $s : \mathbb{N} \to \mathbb{N} \to \mathbb{N}$
4. with the property that $\phi_{s(c,x)} y \equiv \phi_c \langle x, y \rangle$.

Equivalently, using *parametrical* universality

$$\mathsf{SCT} := \exists \phi.\ \forall f : \mathbb{N} \to \mathbb{N} \to \mathbb{N}. \exists \gamma : \mathbb{N} \to \mathbb{N}. \forall i.\ \phi_{\gamma i} \equiv f_i$$

or using parameterised partial functions $\mathbb{N} \to \mathbb{N} \rightharpoonup \mathbb{N}$ (EPF),
or using parameterised boolean functions $\mathbb{N} \to \mathbb{N} \rightharpoonup \mathbb{B}$ ($\mathsf{SCT}_{\mathbb{B}}$),

Synthetic computability without choice

Assume

1. a (partial) function ϕ
2. universal for $\mathbb{N} \to \mathbb{N}$: $\forall f : \mathbb{N} \to \mathbb{N}. \exists c : \mathbb{N}. \forall x.\ \phi_c x \triangleright f x$,
3. a function $s : \mathbb{N} \to \mathbb{N} \to \mathbb{N}$
4. with the property that $\phi_{s(c,x)} y \equiv \phi_c \langle x, y \rangle$.

Equivalently, using *parametrical* universality

$$\text{SCT} := \exists \phi.\ \forall f : \mathbb{N} \to \mathbb{N} \to \mathbb{N}. \exists \gamma : \mathbb{N} \to \mathbb{N}. \forall i.\ \phi_{\gamma i} \equiv f_i$$

or using parameterised partial functions $\mathbb{N} \to \mathbb{N} \rightharpoonup \mathbb{N}$ (EPF),
or using parameterised boolean functions $\mathbb{N} \to \mathbb{N} \rightharpoonup \mathbb{B}$ ($\text{SCT}_{\mathbb{B}}$),
or using parametrically enumerable predicates $\mathbb{N} \to \mathbb{N} \to \mathbb{P}$ (EA).

Synthetic computability without choice

Assume

1. a (partial) function ϕ
2. universal for $\mathbb{N} \to \mathbb{N}$: $\forall f : \mathbb{N} \to \mathbb{N}. \exists c : \mathbb{N}. \forall x.\ \phi_c x \triangleright f x$,
3. a function $s : \mathbb{N} \to \mathbb{N} \to \mathbb{N}$
4. with the property that $\phi_{s(c,x)} y \equiv \phi_c \langle x, y \rangle$.

due to strict separation of functions and logic in Coq
the law of excluded middle can be consistently assumed

1. Introduce favourite model of computation
   1.1 Prove s^m_n theorem (currying)
   1.2 Argue universal program
   1.3 Optional: Introduce a second model and argue equivalence
2. Define Church Turing thesis as axiom (SCT, EPF, EA)
3. Develop computability theory relying on axiom
   3.1 Undecidability of the halting problem
   3.2 Rice's theorem
   3.3 Reduction theory (Myhill isomorphism theorem, Post's simple and hypersimple sets)
   3.4 Oracle computation and Turing reducibility
   3.5 Kolmogorov complexity
   3.6 Kleene-Post and Post's hierarchy theorem
4. Prove undecidability of concrete problems (PCP, CFGs)

1. Introduce favourite model of computation

   1.1 Prove s^m_n theorem (currying)

   1.2 Argue universal program

   1.3 Optional: Introduce a second model and argue equivalence

2. Define Church Turing thesis as axiom (SCT, EPF, EA) ✓

3. Develop computability theory relying on axiom ✓

   3.1 Undecidability of the halting problem ✓

   3.2 Rice's theorem ✓

   3.3 Reduction theory (Myhill isomorphism theorem, Post's simple and hypersimple sets) ✓

   3.4 Oracle computation and Turing reducibility ✓

   3.5 Kolmogorov complexity ✓

   3.6 Kleene-Post and Post's hierarchy theorem ✓

4. Prove undecidability of concrete problems (PCP, CFGs, needs CT) ✓

Principles in CIC

- Law of excluded middle LEM and Markov's Principle MP are
  - consistent (important to formalise textbook proofs)

Principles in CIC

- Law of excluded middle LEM and Markov's Principle MP are
  - consistent (important to formalise textbook proofs)
  - but not provable (important for analysing minimal requirements)

Principles in CIC

- Law of excluded middle LEM and Markov's Principle MP are
  - consistent (important to formalise textbook proofs)
  - but not provable (important for analysing minimal requirements)
- Axioms of choice, countable choice, and countable Π^0_1-choice are
  - consistent (nice to know)

Principles in CIC

- Law of excluded middle LEM and Markov's Principle MP are
  - consistent (important to formalise textbook proofs)
  - but not provable (important for analysing minimal requirements)
- Axioms of choice, countable choice, and countable Π^0_1-choice are
  - consistent (nice to know)
  - but not provable (otherwise LEM $\wedge$ CT would be inconsistent)

Principles in CIC

- Law of excluded middle LEM and Markov's Principle MP are
  - consistent (important to formalise textbook proofs)
  - but not provable (important for analysing minimal requirements)
- Axioms of choice, countable choice, and countable Π^0_1-choice are
  - consistent (nice to know)
  - but not provable (otherwise LEM $\wedge$ CT would be inconsistent)
- Axiom of countable Σ^0_1-choice is provable

Principles in CIC

- Law of excluded middle LEM and Markov's Principle MP are
  - consistent (important to formalise textbook proofs)
  - but not provable (important for analysing minimal requirements)
- Axioms of choice, countable choice, and countable Π_1^0-choice are
  - consistent (nice to know)
  - but not provable (otherwise LEM $\wedge$ CT would be inconsistent)
- Axiom of countable Σ_1^0-choice is provable

$\Rightarrow$ enables constructive reverse mathematics for computability

- not too strong (no Π_1^0-choice, LEM, MP)
- just strong enough (countable Σ_1^0-choice)
- This is not the case in (all?) other type theories

Other type theories

- Martin-Löf Type Theory (e.g. Agda) with $\exists x.px := \Sigma x.px$:
  Proves AC, so LLPO $\to \neg$CT.
- Martin-Löf Type Theory (e.g. Agda) with $\exists x.px := \neg\neg\Sigma x.px$:
  Does not prove AC, but Π^0_1-$\mathrm{AC}_{\mathbb{N},\mathbb{B}} \to \neg$CT
- Homotopy Type Theory with $\exists x.px := ||\Sigma x.px||$:
  Proves AUC, so WLPO $\to \neg$CT.

Constructive Reverse Mathematics in CIC

Fred Richman:

"Countable choice is a blind spot for constructive mathematicians in much the same way as excluded middle is for classical mathematicians."

Richman [2000, 2001]

Constructive Reverse Mathematics in CIC

Fred Richman:

“Countable choice is a blind spot for constructive mathematicians in much the same way as excluded middle is for classical mathematicians.”

Me:

“CIC is a suitable base system for constructive (reverse) mathematics sensitive to applications of countable choice.”

Richman [2000, 2001]

Three Flavours

- No axioms
  - Morally identify computable functions with functions
  - Can prove results not relying on a universal machine
- With CT as axiom
  - Needs a model of computation
  - Allows proving undecidability of concrete problems
  - Allows talking e.g. about the arithmetical hierarchy
- With SCT as axiom
  - No need for model of computation

Conjecture

The following are consistent in CIC:

- CT (implies in particular SCT)
- LEM (implies in particular MP)
- functional extensionality
- Uniformisation: “Every total relation contains a total functional subrelation.”

Synthetic Oracle Computability

Oracle computability

We call $F : (Q \to A \to \mathbb{P}) \to (I \to O \to \mathbb{P})$ an (oracle-)computable functional if there is a computation tree $\tau : I \to \mathbb{L}A \rightharpoonup Q + O$ such that

$$\forall Rio.\ FRio \leftrightarrow \exists qs\ as.\ \tau i\ ;\ R \vdash qs\ ;\ as\ \ \wedge\ \ \tau\ i\ as \triangleright \text{out}\ o$$

where the interrogation relation $\sigma; R \vdash qs; as$ is inductively defined:

$$\frac{}{\sigma\ ;\ R \vdash []\ ;\ []} \qquad \frac{\sigma\ ;\ R \vdash qs\ ;\ as \qquad \sigma as \triangleright \text{ask}\ q \qquad Rqa}{\sigma\ ;\ R \vdash qs \mathbin{+\!\!+} [q]\ ;\ as \mathbin{+\!\!+} [a]}$$

where we use the shorthands ask q and out o for the respective injections into the sum type $Q + O$ for better intuition.

Turing reducibility

$$\hat{p} \;:=\; \lambda x b.\begin{cases} px & \text{if } b = \text{true} \\ \neg px & \text{if } b = \text{false}, \end{cases}$$

A predicate $p : X \to \mathbb{P}$ Turing reduces to $q : Y \to \mathbb{P}$ if:

$$p \preceq_{\mathsf{T}} q \;:=\; \exists F.\, F \textit{ is computable} \land \forall x b.\, \hat{p}xb \leftrightarrow F\hat{q}xb$$

jww with Niklas Mück and Dominik Kirst [APLAS ’23]

Semi-decidability

$p : X \to \mathbb{P}$ is semi-decidable relative to $q : Y \to \mathbb{P}$ if there is a computable

$$F : (Y \to \mathbb{B} \to \mathbb{P}) \to X \to \mathbb{1} \to \mathbb{P}$$

with

$$\forall x.\, px \leftrightarrow F\,\hat{q}\,x\,\star\,.$$

Theorem (PT)

We have $p \preceq_\mathsf{T} q$ if

- *q is classical ($\forall y.\ qy \lor \neg qy$),*
- *p is semi-decidable in q*
- *the complement of p is semi-decidable in q*

The arithmetical hierarchy

All first-order logic formulas is equivalent to a formula in preens normal form if and only if LEM holds.

We can define a predicate $p : \mathbb{N} \to \mathbb{P}$ to be

- Σ_0 and Π_0 if it is expressible as quantor-free arithmetical formula.
- Σ_{n+1} if there is a quantor-free arithmetical formula q with $\forall x.\ px \leftrightarrow \exists \vec{y_1} \forall \vec{y_2} \ldots \nabla \vec{y_n}.\ q(x, \vec{y_1}, \vec{y_2}, \ldots, \vec{y_n})$
- Π_{n+1} if there is a quantor-free arithmetical formula q with $\forall x.\ px \leftrightarrow \forall \vec{y_1} \exists \vec{y_2} \ldots \nabla \vec{y_n} \ldots .\ q(x, \vec{y_1}, \vec{y_2}, \ldots, \vec{y_n})$

jww Niklas Mück and Dominik Kirst [CSL '24]

The arithmetical hierarchy

All first-order logic formulas is equivalent to a formula in preens normal form if and only if LEM holds.

We can define a predicate $p : \mathbb{N} \to \mathbb{P}$ to be

- Σ_0 and Π_0 if it is expressible as quantor-free arithmetical formula.
- Σ_{n+1} if there is a quantor-free arithmetical formula q with $\forall x.\ px \leftrightarrow \exists \vec{y_1} \forall \vec{y_2} \dots \nabla \vec{y_n}.\ q(x, \vec{y_1}, \vec{y_2}, \dots, \vec{y_n})$
- Π_{n+1} if there is a quantor-free arithmetical formula q with $\forall x.\ px \leftrightarrow \forall \vec{y_1} \exists \vec{y_2} \dots \nabla \vec{y_n} \dots .\ q(x, \vec{y_1}, \vec{y_2}, \dots, \vec{y_n})$

Or replace *quantor-free* by *decidable*.

Theorem

Both definitions are equivalent under CT.

jww Niklas Mück and Dominik Kirst [CSL '24]

Ever seen this principle?

Markov's Principle

$$\mathsf{MP} := \forall f : \mathbb{N} \to \mathbb{B}. \quad \neg\neg(\exists n.\ fn = \mathsf{true}) \leftrightarrow (\exists n.\ fn = \mathsf{true})$$

Anonymised Markov's Principle

$$\mathsf{AMP} := \forall f : \mathbb{N} \to \mathbb{B}. \exists g : \mathbb{N} \to \mathbb{B}.\ \neg\neg(\exists n.\ fn = \mathsf{true}) \leftrightarrow (\exists n.\ gn = \mathsf{true})$$

Ever seen this principle?

Markov's Principle

$$\mathsf{MP} := \forall f : \mathbb{N} \to \mathbb{B}. \quad \neg\neg(\exists n.\ fn = \mathsf{true}) \leftrightarrow (\exists n.\ fn = \mathsf{true})$$

Anonymised Markov's Principle

$$\mathsf{AMP} := \forall f : \mathbb{N} \to \mathbb{B}. \exists g : \mathbb{N} \to \mathbb{B}.\ \neg\neg(\exists n.\ fn = \mathsf{true}) \leftrightarrow (\exists n.\ gn = \mathsf{true})$$

Principle of Finite Possibility

$$\mathsf{PFP} := \forall f : \mathbb{N} \to \mathbb{B}. \exists g : \mathbb{N} \to \mathbb{B}. \quad \neg(\exists n.\ fn = \mathsf{true}) \leftrightarrow (\exists n.\ gn = \mathsf{true})$$

Axioms for Oracle computability

Given a universal $\theta : \mathbb{N} \to (\mathbb{N} \rightharpoonup \mathbb{N})$, construct universal

$$\xi : \mathbb{N} \to (\mathbb{N} \to \mathbb{L}\mathbb{B} \to \mathbb{N} + \mathbb{1})$$

enumerating any possible tree.

Given a tree $\sigma : \mathbb{N} \to \mathbb{L}\mathbb{B} \to \mathbb{N} + \mathbb{1}$ define

$$\hat{\sigma} R x := \exists qs\, as.\ \sigma \mathbin{;} R \vdash qs \mathbin{;} as \land \sigma\ as \triangleright \text{out} \star$$

$$\Xi_c R x := \widehat{\xi c} R x$$

We define the Turing jump q' of a predicate $q : \mathbb{N} \to \mathbb{P}$ as

$$q' c := \Xi_c\, \hat{q}\, c$$

Theorem

q' is semi-decidable in q, but its complement is not.

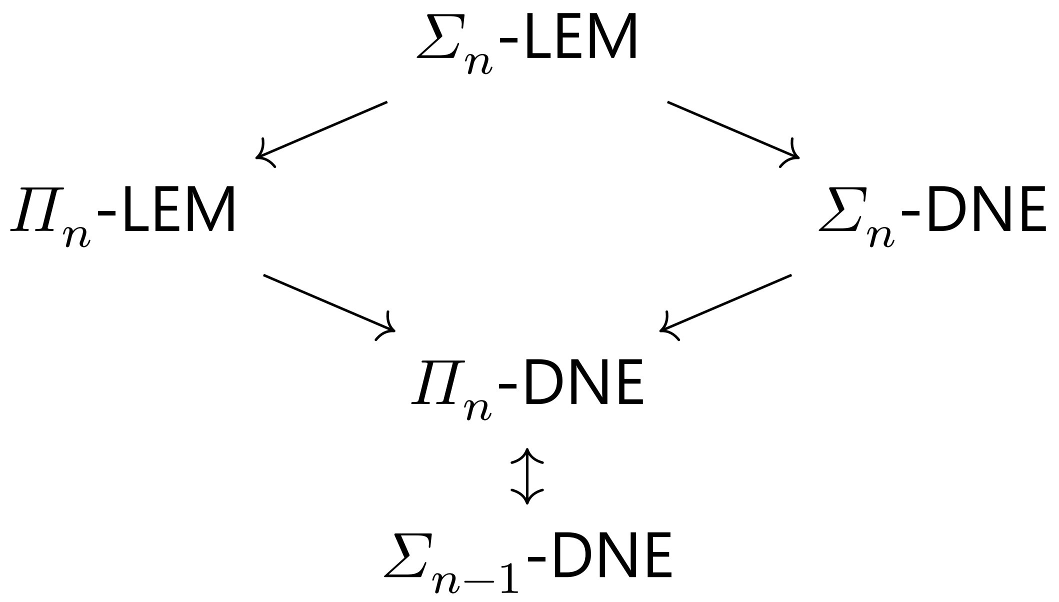
Classical logic in the arithmetical hierarchy

Σ_n-LEM $:= \forall k. \forall p : \mathbb{N}^k.\ \Sigma_n p \to \forall v. pv \lor \neg pv$

Π_n-LEM $:= \forall k. \forall p : \mathbb{N}^k.\ \Pi_n p \to \forall v. pv \lor \neg pv$

Σ_n-DNE $:= \forall k. \forall p : \mathbb{N}^k.\ \Sigma_n p \to \forall v. \neg\neg pv \to pv$

Π_n-DNE $:= \forall k. \forall p : \mathbb{N}^k.\ \Pi_n p \to \forall v. \neg\neg pv \to pv$



Y. Akama, S. Berardi, S. Hayashi, and U. Kohlenbach, An arithmetical hierarchy of the law of excluded middle and related principles (2004)

Post's hierarchy theorem

Theorem (Post)

Assuming Σ^0_n-LEM:

- *A unary predicate A is Σ_{n+1} iff it is semi-decidable relative to $\emptyset^{(n)}$.*
- *If A is Σ_n, then $A \preceq_T \emptyset^{(n)}$.*

jww with Niklas Mück and Dominik Kirst [CSL '24]

Friedberg-Muchnik

Post's problem: Is there an undecidable, enumerable problem which is not Turing-reducible from the halting problem?

Simplest proof due to Soare (low simple predicates), based on priority method.

jww Haoyi Zeng and Dominik Kirst [TYPES '24], Takako Nemoto has an analytic constructive analysis, Logic Colloqium '23

Markov's principle

$$
\begin{aligned}
\mathsf{MP}_{\mathbb{P}} &:= \forall A : \mathbb{N} \to \mathbb{P}.\ (\forall n.\ An \lor \neg An) \to \quad \neg\neg(\exists n.\ An) \to (\exists n.\ An) \\
\mathsf{MP}_{\mathbb{B}} &:= \forall f : \mathbb{N} \to \mathbb{B}.\quad \neg\neg(\exists n.\ fn = \mathsf{true}) \to (\exists n.\ fn = \mathsf{true}) \\
\mathsf{MP}_{\mathsf{T}} &:= \forall f : \mathbb{N} \to \mathbb{B}.\ \text{Turing-computable } f \to \neg\neg(\exists n.\ fn = \mathsf{true}) \to (\exists n.\ fn = \mathsf{true})
\end{aligned}
$$

Markov's principle

$$\begin{aligned}
\mathsf{MP}_{\mathbb{P}} &:= \forall A : \mathbb{N} \to \mathbb{P}.\ (\forall n.\ An \lor \neg An) \to \neg\neg(\exists n.\ An) \to (\exists n.\ An) \\
\mathsf{MP}_{\mathbb{B}} &:= \forall f : \mathbb{N} \to \mathbb{B}.\ \neg\neg(\exists n.\ fn = \mathsf{true}) \to (\exists n.\ fn = \mathsf{true}) \\
\mathsf{MP}_{\mathsf{T}} &:= \forall f : \mathbb{N} \to \mathbb{B}.\ \text{Turing-computable } f \to \neg\neg(\exists n.\ fn = \mathsf{true}) \to (\exists n.\ fn = \mathsf{true}) \\
\mathsf{MP}_{\mathsf{PR}} &:= \forall f : \mathbb{N} \to \mathbb{B}.\ \text{primitive-recursive } f \to \neg\neg(\exists n.\ fn = \mathsf{true}) \to (\exists n.\ fn = \mathsf{true})
\end{aligned}$$

Markov's principle

$$\mathsf{MP}_{\mathbb{P}} := \forall A : \mathbb{N} \to \mathbb{P}.\ (\forall n.\ An \lor \neg An) \to \neg\neg(\exists n.\ An) \to (\exists n.\ An)$$

$$\mathsf{MP}_{\mathbb{B}} := \forall f : \mathbb{N} \to \mathbb{B}.\ \neg\neg(\exists n.\ fn = \mathsf{true}) \to (\exists n.\ fn = \mathsf{true})$$

$$\mathsf{MP}_{\mathsf{PR}} := \forall f : \mathbb{N} \to \mathbb{B}.\ \text{primitive-recursive}\ f \to \neg\neg(\exists n.\ fn = \mathsf{true}) \to (\exists n.\ fn = \mathsf{true})$$

Markov's principle

$$\begin{aligned}
\mathsf{MP}_{\mathbb{P}} &:= \forall A : \mathbb{N} \to \mathbb{P}.\ (\forall n.\ An \lor \neg An) \to & \neg\neg(\exists n.\ An) \to (\exists n.\ An) \\
\mathsf{MP}_{\mathbb{B}} &:= \forall f : \mathbb{N} \to \mathbb{B}. & \neg\neg(\exists n.\ fn = \mathsf{true}) \to (\exists n.\ fn = \mathsf{true})
\end{aligned}$$

$$\mathsf{MP}_{\mathsf{PR}} := \forall f : \mathbb{N} \to \mathbb{B}.\ \text{primitive-recursive } f \to \neg\neg(\exists n.\ fn = \mathsf{true}) \to (\exists n.\ fn = \mathsf{true})$$

Kreisel [1959]: $\mathsf{MP}_{\mathsf{PR}}$ does not hold in HA^{ω}, using lawless (choice) sequences

Smorynski [1973]: M_{PR} is not equivalent to $\mathsf{MP}_{\mathbb{P}}$ over HA^{ω}

Cohen, Forster, Kirst, da Rocha Paiva, Rahli [2024]: all not equivalent over MLTT + truncation

Results

Rice's theorem

$$\text{EPF} := \exists \phi. \forall f : \mathbb{N} \to \mathbb{N} \nrightarrow \mathbb{N}. \exists \gamma.\ \forall ix.\ \phi_{\gamma i} x \triangleright f_i x$$

$$\text{EA} := \exists \varphi. \forall p : \mathbb{N} \to \mathbb{N} \to \mathbb{P}.$$
$$(\exists f. \forall i.\ f_i \textit{ enumerates } p_i) \to \exists \gamma. \forall i.\ \varphi_{\gamma i} \textit{ enumerates } p_i$$

Rice's theorem

$$\mathsf{EPF} := \exists \phi. \forall f : \mathbb{N} \to \mathbb{N} \nrightarrow \mathbb{N}. \exists \gamma.\ \forall i x.\ \phi_{\gamma i} x \triangleright f_i x$$

$$\mathsf{EA} := \exists \varphi. \forall p : \mathbb{N} \to \mathbb{N} \to \mathbb{P}.$$

$$(\exists f. \forall i.\ f_i \textit{ enumerates } p_i) \to \exists \gamma. \forall i.\ \varphi_{\gamma i} \textit{ enumerates } p_i$$

Theorem

Given EPF every $p : (\mathbb{N} \rightharpoonup \mathbb{N}) \to \mathbb{P}$ is undecidable if it

1. *is extensional:* $\forall f f' : \mathbb{N} \rightharpoonup \mathbb{N}. (\forall x.\ f x \equiv f' x) \to p f \leftrightarrow p f'$
2. *is non-trivial:* $\exists f_1 f_2.\ p f_1 \wedge \neg p f_2$

Rice's theorem

$$\text{EPF} := \exists \phi. \forall f : \mathbb{N} \to \mathbb{N} \nrightarrow \mathbb{N}. \exists \gamma.\ \forall i x.\ \phi_{\gamma i} x \triangleright f_i x$$

$$\text{EA} := \exists \varphi. \forall p : \mathbb{N} \to \mathbb{N} \to \mathbb{P}. \\ (\exists f. \forall i.\ f_i \textit{ enumerates } p_i) \to \exists \gamma. \forall i.\ \varphi_{\gamma i} \textit{ enumerates } p_i$$

Theorem

Given EA every $p : (\mathbb{N} \to \mathbb{P}) \to \mathbb{P}$ *is undecidable if it*

1. *is extensional:* $\forall q q' : \mathbb{N} \to \mathbb{P}. (\forall x.\ q x \leftrightarrow q' x) \to p q \leftrightarrow p q'$
2. *is non-trivial:* $\exists q_1 q_2$ *both enumerable*. $p q_1 \wedge \neg p f_2$

$$\mathsf{EPF} := \exists \phi. \forall f : \mathbb{N} \to \mathbb{N} \nrightarrow \mathbb{N}. \exists \gamma.\ \forall i x.\ \phi_{\gamma i} x \triangleright f_i x$$

Lemma

Let ϕ *be given as in* EPF *and* $\gamma : \mathbb{N} \to \mathbb{N}$*, then there exists* c *s.t.* $\phi_{\gamma c} \equiv \phi_c$*.*

Theorem

Let ϕ *be given as in* EPF *and* $p : \mathbb{N} \to \mathbb{P}$*. If* p *treats elements as codes w.r.t.* ϕ *and is non-trivial, then* p *is undecidable.*

Proof.

Let f decide p and let pc_1 and $\neg pc_2$. Define $h_x y :=$ **if** fx *then* $\phi_{c_2} y$ **else** $\phi_{c_1} y$ and let γ via EPF be s.t. $\phi_{\gamma x} \equiv h_x$. Let c be a fixed-point for γ.
Case analysis on fc:

- If $fc =$ true we have pc and $\phi_c \equiv \phi_{\gamma c} \equiv h_c \equiv \phi_{c_2}$. Thus pc_2, contradiction.
- If $fc =$ false we have $\neg pc$ and $\phi_c \equiv \phi_{\gamma c} \equiv h_c \equiv \phi_{c_1}$. Thus $\neg pc_1$, contradiction.

□

Simple predicates

Definition

A predicate $p : \mathbb{N} \to \mathbb{P}$ is called *simple* if

- it is enumerable,
- its complement is infinite,
- its complement has no enumerable infinite subpredicate.

jww Felix Jahn [CSL ’23]

Simple predicates

Definition

A predicate $p : \mathbb{N} \to \mathbb{P}$ is called *simple* if

- it is enumerable,
- its complement is infinite,
- its complement has no enumerable infinite subpredicate.

Definition

A predicate $p : \mathbb{N} \to \mathbb{P}$ is *infinite* if there exists an injection of type $\mathbb{N} \to \mathbb{N}$ returning only elements in p.

jww Felix Jahn [CSL '23]

Simple predicates

Definition

A predicate $p : \mathbb{N} \to \mathbb{P}$ is called *simple* if

- it is enumerable,
- its complement is infinite,
- its complement has no enumerable infinite subpredicate.

Definition

A predicate $p : \mathbb{N} \to \mathbb{P}$ is *infinite* if there exists an injection of type $\mathbb{N} \to \mathbb{N}$ returning only elements in p.

Theorem

Every infinite predicate has an enumerable infinite subpredicate.

jww Felix Jahn [CSL '23]

Simple predicates

Definition

A predicate $p : \mathbb{N} \to \mathbb{P}$ is called *simple* if

- it is enumerable,
- its complement is infinite,
- its complement has no enumerable infinite subpredicate.

Definition

A predicate $p : \mathbb{N} \to \mathbb{P}$ is *infinite* if $\forall n. \exists x > n.\ px$.

Theorem (Meta)

Every definable predicate which can be proved infinite can be proved to have an enumerable subpredicate.

jww Felix Jahn [CSL ’23]

Simple predicates

Definition

A predicate $p : \mathbb{N} \to \mathbb{P}$ is called *simple* if

- it is enumerable,
- its complement is infinite,
- its complement has no enumerable infinite subpredicate.

Definition

A predicate $p : \mathbb{N} \to \mathbb{P}$ is *infinite* if there is no list covering p.

Theorem

A simple predicate exists.

jww Felix Jahn [CSL '23]

Kolmogorov complexity

We call a partial function $\mathcal{D} : \mathbb{N} \rightharpoonup \mathbb{N}$ a *description mode*. We call y a description of x if $\mathcal{D}y \triangleright x$. $|n|$ is the length of the bit string representing a number n.

$$\forall y'x.\ \mathcal{D}'y' \triangleright x \to \exists y.\ \mathcal{D}y \triangleright x \land |y| < |y'| + d.$$

$$\mathcal{C}xs := s \text{ is } \mu s.\ \exists y.\ s = |y| \land \mathcal{D}y \triangleright x$$

$$\mathcal{N}(x) := \mathcal{C}x < x$$

Lemma

$\forall x. \neg\neg\exists s.\ \mathcal{C}xs$

Theorem

$\mathcal{N}$ *is simple*

jww Nils Lauermann and Fabian Kunze [ITP '22]

Church's thesis in MLTT

$$\forall f : \mathbb{N} \to \mathbb{N}. \Sigma n.\ n\text{-}\textit{th machine computes } f$$

Church's thesis in MLTT

$$\forall f : \mathbb{N} \to \mathbb{N}. \Sigma n.\ n\textit{-th machine computes } f$$

$$\exists Q : (\mathbb{N} \to \mathbb{N}) \to \mathbb{N}.\ Q f \textit{ computes } f$$

Church's thesis in MLTT

$$\forall f : \mathbb{N} \to \mathbb{N}. \Sigma n.\ n\textit{-th machine computes } f$$

$$\exists Q : (\mathbb{N} \to \mathbb{N}) \to \mathbb{N}.\ Q f \textit{ computes } f$$

Pierre-Marie Pédrot @ LICS '24:
"Upon This Quote I Will Build My Church Thesis"

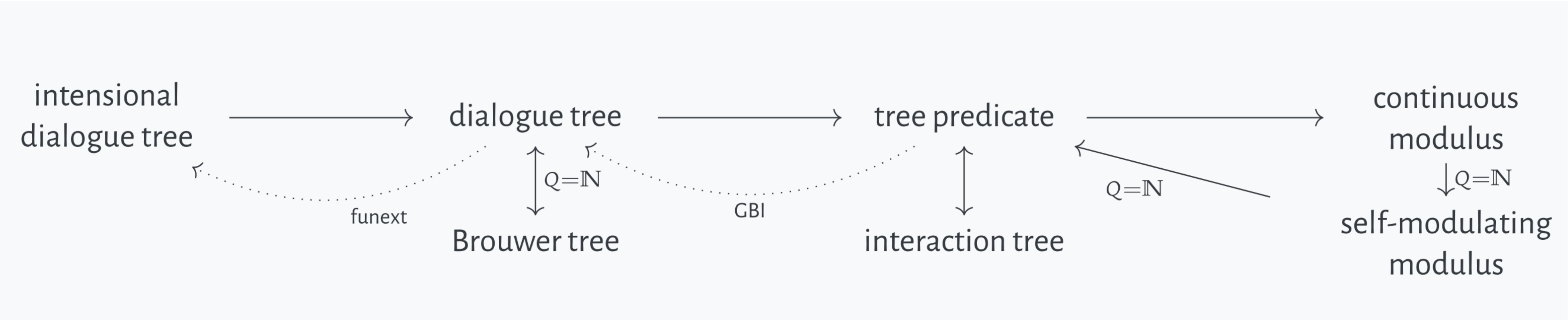
HoTT

Andrew W. Swan
"Oracle modalities"
arXiv preprint arXiv:2406.05818 (2024)

We explore some first connections between Turing reducibility and homotopy theory. This includes a synthetic proof that two Turing degrees are equal as soon as they induce isomorphic permutation groups on the natural numbers, making essential use of both Markov induction and the formulation of groups in HoTT as pointed, connected, 1-truncated types. We also give some simple non-topological examples of modalities in cubical assemblies based on these ideas, to illustrate what we expect higher dimensional analogues of the Turing degrees to look like.

Kreisel-Lacombe-Schönfield-Tseitin

Every function $(\mathbb{N} \to \mathbb{N}) \to \mathbb{N}$ is continuous.



jww Martin Baillon, Assia Mahboubi, Pierre-Marie Pédrot, Matthieu Piquerez

Incompleteness

Dominik Kirst and Benjamin Peters
"Gödel's Theorem Without Tears - Essential Incompleteness in Synthetic Computability"
CSL 2023.

Gödel published his groundbreaking first incompleteness theorem in 1931, stating that a large class of formal logics admits independent sentences which are neither provable nor refutable. This result, in conjunction with his second incompleteness theorem, established the impossibility of concluding Hilbert's program, which pursued a possible path towards a single formal system unifying all of mathematics. Using a technical trick to refine Gödel's original proof, the incompleteness result was strengthened further by Rosser in 1936 regarding the conditions imposed on the formal systems. [...]

The Coq Library of Undecidability Proofs

Synthetic undecidability
Analytic definition

$$\mathcal{U}p := \neg\exists f.\ \mu\text{-recursive } f \land \ldots$$

Lemma (Analytic)

There is no μ-recursive enumerator for the complement of the halting problem.

Theorem (Analytic)

Given a μ-recursive decider for p, there is a μ-recursive enumerator for the complement of the halting problem:

$$\mathcal{D}p \to \mathcal{E}(\overline{\mathsf{Halt}_{\mathsf{TM}}})$$

Synthetic undecidability
Analytic definition

$$\mathcal{U}p := \neg\exists f.\ \mu\text{-recursive } f \land \ldots$$

Lemma (Synthetic)

There is no enumerator for the complement of the halting problem, assuming CT.

Theorem (Synthetic)

Given a decider for p, there is an enumerator for the complement of the halting problem:

$$\mathcal{D}p \to \mathcal{E}(\overline{\mathsf{Halt}_{\mathsf{TM}}})$$

Synthetic undecidability

Analytic definition

$$\mathcal{U}p := \neg\exists f.\ \mu\text{-recursive } f \land \ldots$$

Lemma (Synthetic)

There is no enumerator for the complement of the halting problem, assuming CT.

Theorem (Synthetic)

Given a decider for p, there is an enumerator for the complement of the halting problem:

$$\mathcal{D}p \to \mathcal{E}(\overline{\mathsf{Halt}_{\mathsf{TM}}})$$

Synthetic undecidability

Analytic definition

$$\mathcal{U}p := \neg\exists f.\ \mu\text{-recursive } f \land \ldots$$

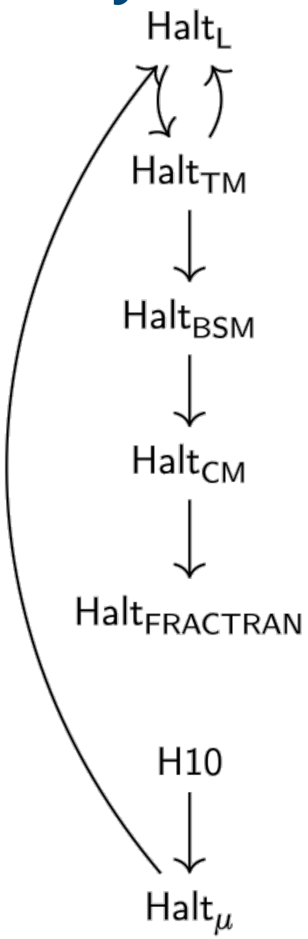
Lemma (Synthetic)

There is no enumerator for the complement of the halting problem, assuming CT.

Synthetic definition

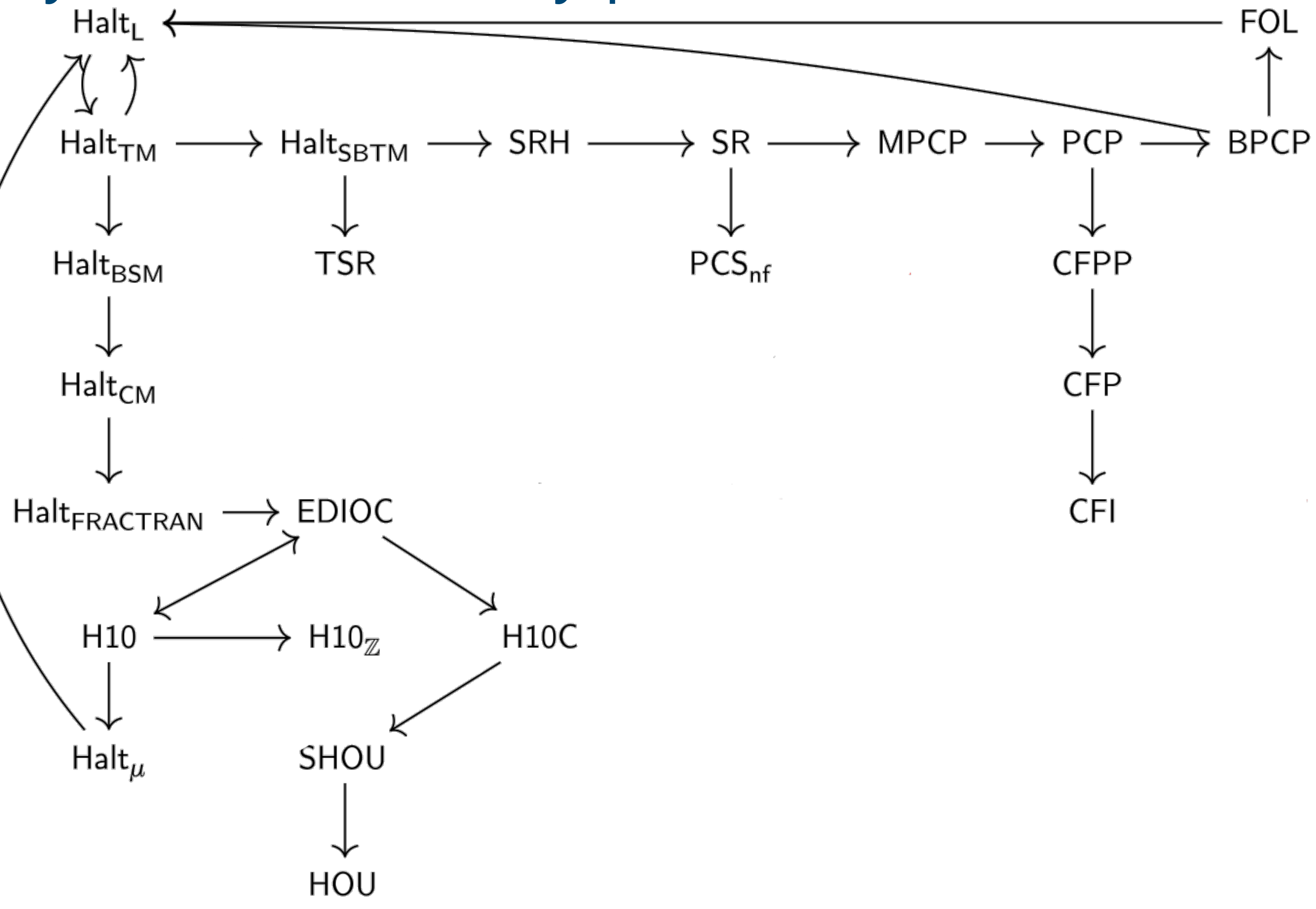
$$\mathcal{U}p := \mathcal{D}p \to \mathcal{E}(\overline{\mathsf{Halt}_{\mathsf{TM}}})$$

The Coq library of undecidability proofs



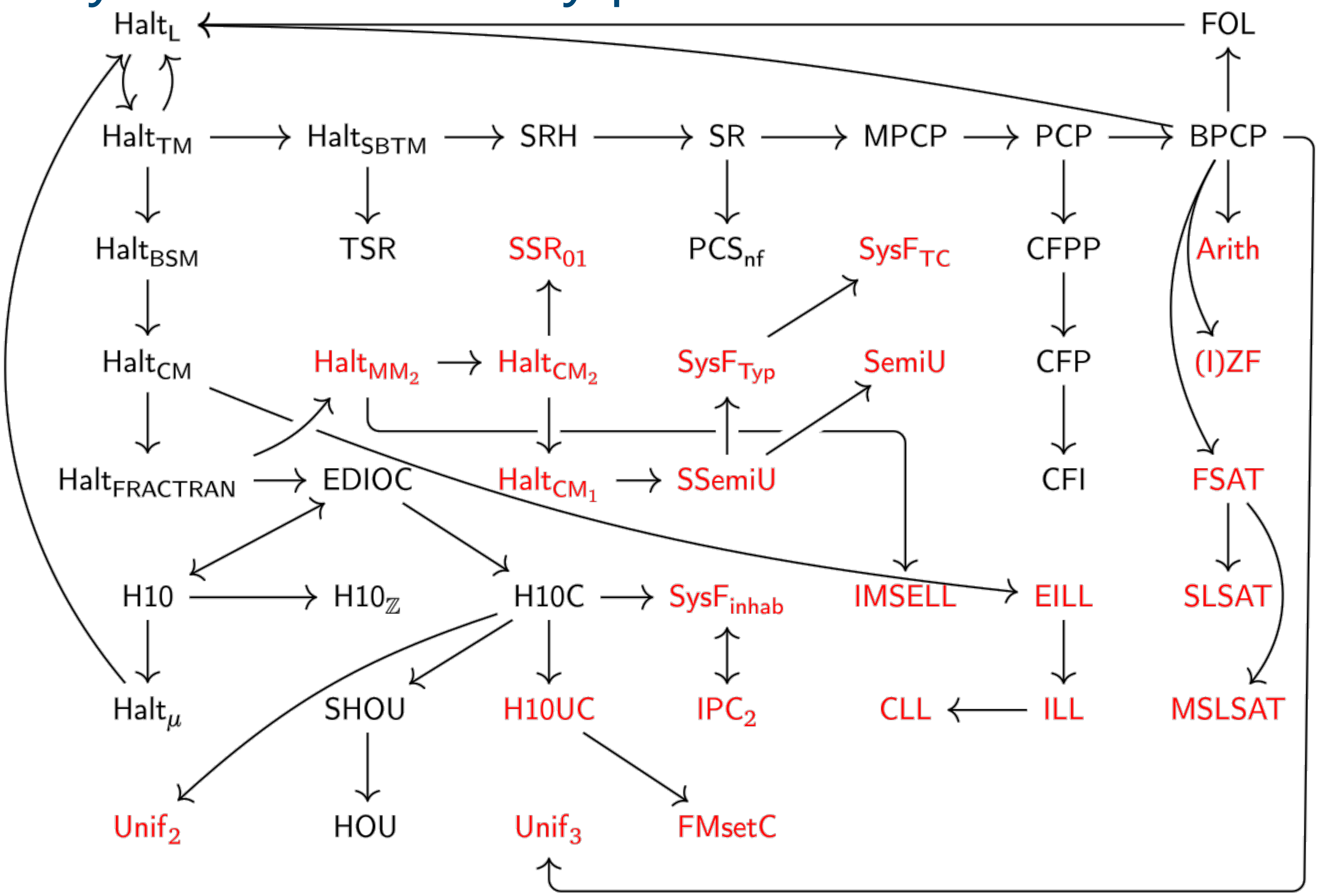
with Dominique Larchey-Wendling, Gert Smolka, Fabian Kunze, Max Wuttke …

The Coq library of undecidability proofs

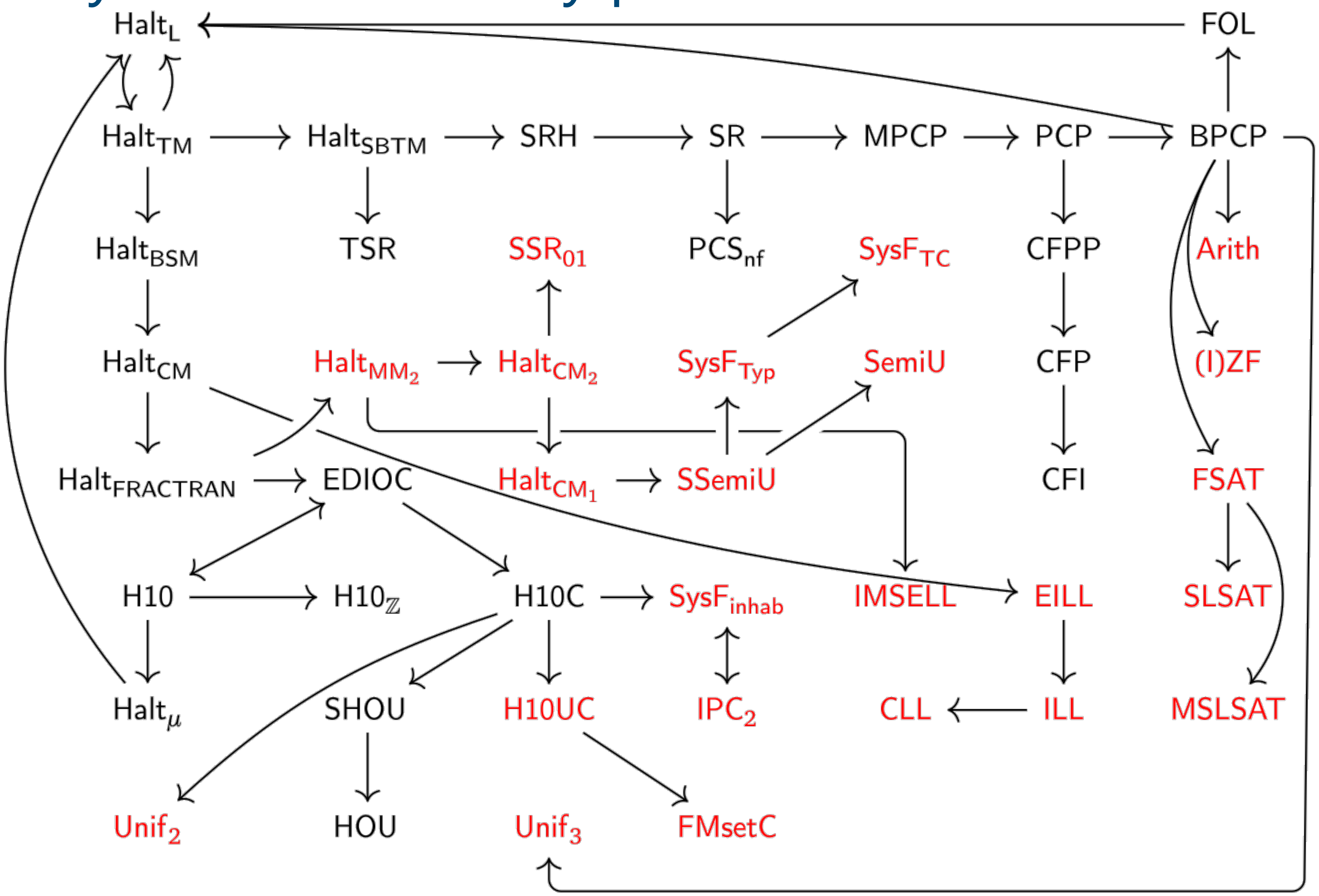


with … Edith Heiter, Dominik Kirst, Simon Spies, Dominik Wehr

The Coq library of undecidability proofs



The Coq library of undecidability proofs



~100k lines of code, 14 contributers

Models of computation

- Equivalence proofs for computability of relations $\mathbb{N}^k \to \mathbb{N} \to \mathbb{P}$
- Identification of the weak call-by-value λ-calculus as sweet spot
  - extraction framework doing automatic computability proofs
  - can be used to prove many-one equivalence between problems
  - can be used to prove that SCT is a consequence of CT
  - even works as a foundation for (analytic) complexity theory, see Fabian Kunze's work

Conclusion

- Machine-checked textbook proofs are feasible using synthetic approach, proofs can focus on mathematical essence.
- CIC allows these proofs to be classical and is an ideal ground for constructive reverse mathematics without choice.
- Lots of open questions regarding constructive status for even basic results.
- Machine-checked undecidability proofs from cutting-edge research are feasible, proofs can focus on inductive invariants.

Conclusion

- Machine-checked textbook proofs are feasible using synthetic approach, proofs can focus on mathematical essence.
- CIC allows these proofs to be classical and is an ideal ground for constructive reverse mathematics without choice.
- Lots of open questions regarding constructive status for even basic results.
- Machine-checked undecidability proofs from cutting-edge research are feasible, proofs can focus on inductive invariants.

Thank you!