

Indecision: finitely generated, finitely related clones (finite degree clones are undecidable)

Matthew Moore

The University of Kansas
Department of Electrical Engineering and Computer Science

March 22, 2019

Indecision: finitely generated, finitely related clones

- 1 Clones
- 2 The finite degree problem
- 3 The encoding of computation
- 4 Non-halting implies infinite degree
- 5 Halting implies finite degree
- 6 Conclusion

Indecision: finitely generated, finitely related clones

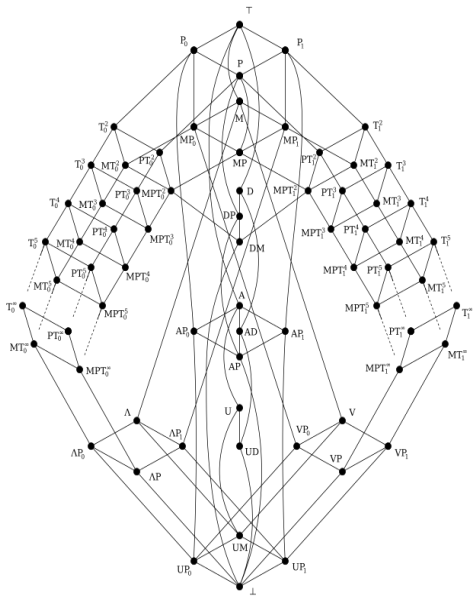
- 1 Clones
- 2 The finite degree problem
- 3 The encoding of computation
- 4 Non-halting implies infinite degree
- 5 Halting implies finite degree
- 6 Conclusion

A **clone** is a set of finitary operations closed under

- composition,
- variable identification,
- variable permutation,
- introduction of extraneous variables.

Emil Post in 1941 famously classified all Boolean clones.

Over (≥ 3) -element domains structure is quite complicated.



Clones are infinite. How can they be an input to an algorithm?

A clone on finite domain A can be **finitely specified** in essentially 2 ways.

First way: Given \mathcal{F} , a finite set of operations of A , define $\text{Clo}(\mathcal{F}) =$ “the smallest clone containing \mathcal{F} ”.

- A with \mathcal{F} forms a algebra, $\mathbb{A} = \langle A; \mathcal{F} \rangle$. Define $\text{Clo}(\mathbb{A}) = \text{Clo}(\mathcal{F})$.
- A **relation** of \mathbb{A} is a subpower $R \subseteq A^n$ closed under \mathcal{F} (hence $\text{Clo}(\mathcal{F})$)
- Define $\text{Rel}_n(\mathbb{A}) = \text{Rel}_n(\mathcal{F}) =$ “all $(\leq n)$ -ary relations of \mathbb{A} ”.
- Define $\text{Rel}(\mathbb{A}) = \text{Rel}(\mathcal{F}) = \bigcup_{n < \infty} \text{Rel}_n(\mathbb{A})$

These are the **finitely generated** clones

Second way: Given \mathcal{R} , a finite set of subpowers of A , define $\text{Pol}(\mathcal{R}) =$ “the set of all operations of A preserving all subpowers in \mathcal{R} ”.

These are the **finitely related/finite degree** clones.

$$\text{Rel}(\mathcal{F}) = \{R \subseteq A^n \mid R \text{ is preserved by all operations in } \mathcal{F}\}$$

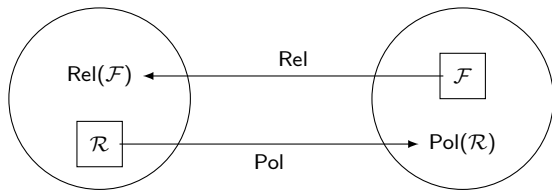
$$\text{Pol}(\mathcal{R}) = \{f : A^n \rightarrow A \mid f \text{ preserves all subpowers in } \mathcal{R}\}$$

These two operators form a **Galois connection**.

$$\mathcal{R} \subseteq \text{Rel}(\mathcal{F})$$



$$\mathcal{F} \subseteq \text{Pol}(\mathcal{R})$$



Every Galois connection defines two closure operators. Here, they are

$$\text{Clo} = \text{Pol} \circ \text{Rel} \quad \text{and} \quad \text{RClo} = \text{Rel} \circ \text{Pol}.$$

If $\mathbb{R} \in \text{RClo}(\mathcal{S})$, then we say “ \mathcal{S} entails \mathbb{R} ” and write $\mathcal{S} \models \mathbb{R}$

If $f \in \text{Pol}(\mathcal{S})$, then we say “ \mathcal{S} entails f ” and write $\mathcal{S} \models f$.

Indecision: finitely generated, finitely related clones

- 1 Clones
- 2 The finite degree problem
- 3 The encoding of computation
- 4 Non-halting implies infinite degree
- 5 Halting implies finite degree
- 6 Conclusion

For a set of relations \mathcal{S} , define

$$\text{deg}(\mathcal{S}) = \sup \{ \text{arity}(\mathbb{R}) \mid \mathbb{R} \in \mathcal{S} \}.$$

For a clone \mathcal{C} , define

$$\text{deg}(\mathcal{C}) = \inf \{ \text{deg}(\mathcal{S}) \mid \text{Pol}(\mathcal{S}) = \mathcal{C} \}.$$

For an algebra \mathbb{A} , define

$$\text{deg}(\mathbb{A}) = \text{deg}(\text{Clo}(\mathbb{A})).$$

The Finite Degree Problem

Input: \mathcal{F} , a finite set of operations on a finite domain.

Output: whether $\text{deg}(\text{Clo}(\mathcal{F})) < \infty$.

(Seems to originate in the 70s with the study of lattices of clones over more than 2 element domains.)

The Finite Degree Problem

Input: \mathcal{F} , a finite set of operations on a finite domain.

Output: whether $\deg(\text{Clo}(F)) < \infty$.

Given a Minsky machine \mathcal{M} , we encode it into a finite algebra $\mathbb{A}(\mathcal{M})$.

Theorem

The following are equivalent.

- \mathcal{M} halts,
- $\deg(\mathbb{A}(\mathcal{M})) < \infty$ (i.e. $\mathbb{A}(\mathcal{M})$ is finitely related),

Similar approaches have proved the following are undecidable:

- finite residual bound (McKenzie)
- finite axiomatizability/Tarski's problem (McKenzie)
- existence of a term op. that is NU on all but 2 elements (Maroti)
- DPSC, leading to another solution to Tarski's problem (M)
- profiniteness (Nurakunov and Stronkowski)

Indecision: finitely generated, finitely related clones

- 1 Clones
- 2 The finite degree problem
- 3 The encoding of computation**
- 4 Non-halting implies infinite degree
- 5 Halting implies finite degree
- 6 Conclusion

A Minsky machine has...

- states $0, 1, \dots, N$ (1 is the starting state, 0 is the halting state),
- registers A and B that have integer values ≥ 0 ,
- instructions of the form (i, R, j) , meaning “in state i , increase register R by 1 and enter j ”.
- instructions of the form (i, R, j, k) , meaning “in state i , if R is 0 enter j , otherwise decrease R by 1 and enter k ”.

In this talk, \mathcal{M} is some fixed Minsky machine.

Let \mathcal{M} have instructions

(1,B,3,2), (2,A,1), (3,A,4), (4,A,0).

Start the machine with register contents $A = 3$, $B = 2$.

Step	State	A	B	Step	State	A	B
0	(1,	3,	2)	4	(1,	5,	0)
1	(2,	3,	1)	5	(3,	5,	0)
2	(1,	4,	1)	6	(4,	6,	0)
3	(2,	4,	0)	7	(0,	7,	0)

\mathcal{M} computes $A + B + 2$ and stores the result in A .

A **configuration** (i, α, β) represents each stage of computation.

Consider \mathcal{M} as a function, and write

$$\mathcal{M}(i, \alpha, \beta) = (j, \alpha', \beta') \quad \text{or} \quad \mathcal{M}^n(i, \alpha, \beta) = (j, \alpha', \beta')$$

(single step of computation or multiple).

The **capacity** of \mathcal{M} is the max sum of the registers.

The algebra $\mathbb{A}(\mathcal{M})$ has set

$$A(\mathcal{M}) = \{ \langle i, 0 \rangle, \langle i, A \rangle, \langle i, B \rangle, \langle i, \bullet \rangle, \langle i, \times \rangle \mid i \text{ a state of } \mathcal{M} \}$$

The algebra is $\mathbb{A}(\mathcal{M}) = \langle A(\mathcal{M}) ; \wedge, M, M', I, H, N_0, S, N_\bullet, P \rangle$.

$$M(x, y) = \begin{cases} \langle j, R \rangle & \text{if } (i, R, j) \in \mathcal{M}, \\ & x = \langle i, \bullet \rangle, y = \langle i, 0 \rangle; \\ \langle j, 0 \rangle & \text{if } (i, R, k, j) \in \mathcal{M}, \\ & x = \langle i, \bullet \rangle, y = \langle i, R \rangle; \\ \langle j, c \rangle & \text{if } [(i, R, j) \text{ or } (i, R, k, j) \in \mathcal{M}], \\ & x = y = \langle i, c \rangle; \\ \langle j, c \rangle & \text{if } y = \langle i, c \rangle, M(y, x) = \langle j, d \rangle, \\ & d \neq \times, \text{ by above rules;} \\ \langle j, \times \rangle & \text{otherwise}^* \end{cases} \quad M'(x) = \begin{cases} \langle k, c \rangle & \text{if } (i, R, k, j) \in \mathcal{M}, \\ & x = \langle i, c \rangle, c \neq R; \\ \langle k, \times \rangle & \text{otherwise}^* \end{cases}$$

- M encodes addition and subtraction operations.
- M' encodes testing for 0 in a register.
- $M(x, y) \neq \langle *, \times \rangle$ implies $x = y$ modulo a single coordinate transposition.

$$M(x, y) = \begin{cases} \langle j, R \rangle & \text{if } (i, R, j) \in \mathcal{M}, \\ & x = \langle i, \bullet \rangle, y = \langle i, 0 \rangle; \\ \langle j, 0 \rangle & \text{if } (i, R, k, j) \in \mathcal{M}, \\ & x = \langle i, \bullet \rangle, y = \langle i, R \rangle; \\ \langle j, c \rangle & \text{if } [(i, R, j) \text{ or } (i, R, k, j) \in \mathcal{M}], \\ & x = y = \langle i, c \rangle; \\ \langle j, c \rangle & \text{if } y = \langle i, c \rangle, M(y, x) = \langle j, d \rangle, \\ & d \neq x, \text{ by above rules;} \\ \dots & \dots \end{cases}, \quad M'(x) = \begin{cases} \langle k, c \rangle & \text{if } (i, R, k, j) \in \mathcal{M}, \\ & x = \langle i, c \rangle, c \neq R; \\ \dots & \dots \end{cases}$$

Let $\mathcal{M} = \{(1, B, 3, 2), (2, A, 1), (3, A, 4), (4, A, 0)\}$. ($A + B + 2$ from before)

$1: M \begin{pmatrix} \langle 1, \bullet \rangle, \langle 1, B \rangle \\ \langle 1, 0 \rangle, \langle 1, 0 \rangle \\ \langle 1, 0 \rangle, \langle 1, 0 \rangle \\ \langle 1, B \rangle, \langle 1, \bullet \rangle \end{pmatrix} = \begin{pmatrix} \langle 2, 0 \rangle \\ \langle 2, 0 \rangle \\ \langle 2, 0 \rangle \\ \langle 2, \bullet \rangle \end{pmatrix}$	$4: M \begin{pmatrix} \langle 3, \bullet \rangle, \langle 3, 0 \rangle \\ \langle 3, 0 \rangle, \langle 3, \bullet \rangle \\ \langle 3, 0 \rangle, \langle 3, 0 \rangle \\ \langle 3, A \rangle, \langle 3, A \rangle \end{pmatrix} = \begin{pmatrix} \langle 4, A \rangle \\ \langle 4, \bullet \rangle \\ \langle 4, 0 \rangle \\ \langle 4, A \rangle \end{pmatrix}$		Step	State	A	B
			0	1	0	1
			1	2	0	0
			2	1	1	0
			3	3	1	0
$2: M \begin{pmatrix} \langle 2, 0 \rangle, \langle 2, \bullet \rangle \\ \langle 2, 0 \rangle, \langle 2, 0 \rangle \\ \langle 2, 0 \rangle, \langle 2, 0 \rangle \\ \langle 2, \bullet \rangle, \langle 2, 0 \rangle \end{pmatrix} = \begin{pmatrix} \langle 1, \bullet \rangle \\ \langle 1, 0 \rangle \\ \langle 1, 0 \rangle \\ \langle 1, A \rangle \end{pmatrix}$	$5: M \begin{pmatrix} \langle 4, A \rangle, \langle 4, A \rangle \\ \langle 4, \bullet \rangle, \langle 4, 0 \rangle \\ \langle 4, 0 \rangle, \langle 4, \bullet \rangle \\ \langle 4, A \rangle, \langle 4, A \rangle \end{pmatrix} = \begin{pmatrix} \langle 0, A \rangle \\ \langle 0, A \rangle \\ \langle 0, \bullet \rangle \\ \langle 0, A \rangle \end{pmatrix}$		4	4	2	0
			5	0	3	0
$3: M' \begin{pmatrix} \langle 1, \bullet \rangle \\ \langle 1, 0 \rangle \\ \langle 1, 0 \rangle \\ \langle 1, A \rangle \end{pmatrix} = \begin{pmatrix} \langle 3, \bullet \rangle \\ \langle 3, 0 \rangle \\ \langle 3, 0 \rangle \\ \langle 3, A \rangle \end{pmatrix}$						

Takeaways: on a relation $\mathbb{R} \leq \mathbb{A}(\mathcal{M})^n$...

- certain elements of R encode configurations of \mathcal{M} ,
- M and M' encode the action of \mathcal{M} in the presence of certain elements of R .

Questions

- What if R doesn't contain these kinds of elements?
- What if R contains elements that aren't "computational": multiple \bullet 's or non-constant states.

Given configuration (k, α, β) , in $\mathbb{A}(\mathcal{M})^n$ define

$$c(k, \alpha, \beta) = \bigcup_{p \in P_n} \left\{ p \left(\langle k, \bullet \rangle, \underbrace{\langle k, A \rangle, \dots, \langle k, A \rangle}_{\alpha}, \underbrace{\langle k, B \rangle, \dots, \langle k, B \rangle}_{\beta}, \underbrace{\langle k, 0 \rangle, \dots, \langle k, 0 \rangle}_{n-\alpha-\beta-1} \right) \right\}$$

Call \mathbb{R} **computational** if it doesn't contain any elements with 2 \bullet 's or non-constant state.

The **capacity** of computational \mathbb{R} is (number of coordinates with \bullet) -1 .

Let $S_m = \text{Sg}_{\mathbb{A}(\mathcal{M})^m}(c(1, 0, 0))$.

Theorem (The Coding Theorem)

- If $\mathcal{M}^n(1, 0, 0) = (k, \alpha, \beta)$ and this computation has capacity $m - 1$, then $c(k, \alpha, \beta) \subseteq S_m$.
- If $c(k, \alpha, \beta) \subseteq S_m$ and \mathcal{M} does not halt with capacity $m - 1$ then for some n we have $\mathcal{M}^n(1, 0, 0) = (k, \alpha, \beta)$ and this computation has capacity $m - 1$.

Corollary

The following are equivalent.

- \mathcal{M} halts with capacity $m - 1$,
- S_m is halting,
- every computational $\mathbb{R} \leq \mathbb{A}(\mathcal{M})^\ell$ with capacity $m - 1$ is halting.

Indecision: finitely generated, finitely related clones

- 1 Clones
- 2 The finite degree problem
- 3 The encoding of computation
- 4 Non-halting implies infinite degree**
- 5 Halting implies finite degree
- 6 Conclusion

Observe

$\deg(\mathcal{C}) = \infty$ if and only if $\text{Rel}_n(\mathcal{C}) \not\equiv \text{Rel}(\mathcal{C})$ for all n
if and only if $\text{Rel}_n(\mathcal{C}) \not\equiv \mathbb{R}$ for all n and some \mathbb{R}

Idea: to show that $\deg(\mathbb{A}(\mathcal{M})) = \infty$ when \mathcal{M} does not halt, we prove the last equivalence for $\mathcal{C} = \text{Clo}(\mathbb{A}(\mathcal{M}))$.

$\text{Rel}_n(\mathcal{C}) \models \mathbb{R}$ if and only if \mathbb{R} can be built from $\text{Rel}_n(\mathcal{C})$, in finitely many steps, by applying the following constructions:

- intersection of equal arity relations,
- (cartesian) product of finitely many relations,
- permutation of the coordinates of a relation, and
- projection of a relation onto a subset of coordinates.

Theorem (Zadori 1995)

$\text{Rel}_n(\mathbb{A}) \models \mathbb{S}$ if and only if

$$\mathbb{S} = \pi \left(\bigcap_{i \in I} \mu_i \left(\prod_{j \in J_i} \mathbb{R}_{ij} \right) \right)$$

for some $\mathbb{R}_{ij} \in \text{Rel}_n(\mathbb{A})$, some coordinate projection π , and some coordinate permutations μ_i .

Lemma

Suppose that

$$c(1, 0, 0) \subseteq \pi \left(\bigcap_{i \in I} \mu_i \left(\prod_{j \in J_i} \mathbb{R}_{ij} \right) \right) = \mathbb{S} \leq \mathbb{A}(\mathcal{M})^m,$$

where π is a projection, the μ_i are permutations, and the \mathbb{R}_{ij} are a finite collection of members of $\text{Rel}_n(\mathbb{A}(\mathcal{M}))$, and $n < m$. Then \mathbb{S} is halting.

Theorem

The following hold for any Minsky machine \mathcal{M} .

- If \mathcal{M} does not halt with capacity m then $m < \text{deg}(\mathbb{A}(\mathcal{M}))$.
- If \mathcal{M} does not halt then $\mathbb{A}(\mathcal{M})$ is not finitely related.

Proof: Suppose that $\text{deg}(\mathbb{A}(\mathcal{M})) \leq m$. This implies in particular that $\text{Rel}_m(\mathbb{A}(\mathcal{M})) \models \mathbb{S}_{m+1}$. By Zadori's theorem, \mathbb{S}_{m+1} can be represented as in the Lemma above, so by that same Lemma it is halting. By the Coding Theorem, this implies that \mathcal{M} halts with capacity m , a contradiction. \cdot

Indecision: finitely generated, finitely related clones

- 1 Clones
- 2 The finite degree problem
- 3 The encoding of computation
- 4 Non-halting implies infinite degree
- 5 Halting implies finite degree**
- 6 Conclusion

Strategy

- The relations \mathbb{S}_m witnessed non-entailment when \mathcal{M} did not halt. When \mathcal{M} does halt, these relations eventually witness the halting.
- Show that for some suitably chosen k , we have $\text{Rel}_k(\mathbb{A}(\mathcal{M})) \models \text{Rel}_n(\mathbb{A}(\mathcal{M}))$ for all n .
- We proceed with induction on n .
- The base case of $n = k$ is trivial.
- We thus endeavor to prove $\text{Rel}_{n-1}(\mathbb{A}(\mathcal{M})) \models \mathbb{R}$ for $\mathbb{R} \in \text{Rel}_n(\mathbb{A}(\mathcal{M}))$.
- Relations in $\text{Rel}_n(\mathbb{A}(\mathcal{M}))$ can be divided into 4 different kinds, so we proceed by cases.
- Recall $\mathbb{A}(\mathcal{M}) = \langle A(\mathcal{M}) ; \wedge, M, M', I, H, N_0, S, N_\bullet, P \rangle$.
Different collections of operations handle entailment in each of the different cases.

$$\mathbb{A}(\mathcal{M}) = \langle A(\mathcal{M}) ; \wedge, M, M', I, H, N_0, S, N_\bullet, P \rangle$$

Case \mathbb{R} is non-computational

- There is an element with 2 \bullet 's or with non-constant state.
- 2 \bullet 's: operation N_\bullet handles entailment.
- Non-constant state: operation P handles entailment.

Theorem

If $m \geq 3$ and $\mathbb{R} \leq \mathbb{A}(\mathcal{M})^m$ is non-computational then $\text{Rel}_{m-1}(\mathbb{A}(\mathcal{M})) \models \mathbb{R}$.

Case \mathbb{R} is halting

- R contains $c(0, 0, 0)$.
- Any element of $c(0, 0, 0)$ can be used with operations I , H , and N_0 to prove entailment.

Theorem

If $m \geq 3$ and $\mathbb{R} \leq \mathbb{A}(\mathcal{M})^m$ is halting then $\text{Rel}_{m-1}(\mathbb{A}(\mathcal{M})) \models \mathbb{R}$.

We are left to examine computational non-halting $\mathbb{R} \leq \mathbb{A}(\mathcal{M})^n$.

Let's say that \mathcal{M} halts with capacity κ .

Two metrics: (both subsets of $[n]$)

- $\mathcal{D}(\mathbb{R}) =$ “coordinates i such that $r \in R$ with $r(i) = \langle j, \bullet \rangle$ ”
= “the \bullet (dot) part of \mathbb{R} .”
- $\mathcal{N}(\mathbb{R}) =$ “the inherently non-halting part of \mathbb{R} ” ...
 - $\pi_{\mathcal{N}(\mathbb{R})}(\mathbb{R})$ is non-halting,
 - If $K = |\mathcal{N}(\mathbb{R}) \cap \mathcal{D}(\mathbb{R})|$ then $S_K \leq \mathbb{R}$.

Case \mathbb{R} is computational and $|\mathcal{N}(\mathbb{R}) \cap \mathcal{D}(\mathbb{R})| > \kappa$

- $|\mathcal{N}(\mathbb{R}) \cap \mathcal{D}(\mathbb{R})| > \kappa$ then \mathbb{R} contains a halting subalgebra.
- it follows that \mathbb{R} halts!

We thus consider computational non-halting \mathbb{R} with $|\mathcal{N}(\mathbb{R}) \cap \mathcal{D}(\mathbb{R})| \leq \kappa$. ·

Case computational non-halting \mathbb{R} with $|\mathcal{N}(\mathbb{R}) \cap \mathcal{D}(\mathbb{R})| \leq \kappa$

Theorem

Assume that $n \geq \kappa + 16$ and

- $\mathbb{R} \leq \mathbb{A}(\mathcal{M})^n$ is computational non-halting,
- $|\mathcal{N}(\mathbb{R}) \cap \mathcal{D}(\mathbb{R})| \leq \kappa,$
- $\quad \quad \quad \vdots \quad \quad \quad$ (several technical hypotheses)

Then $\text{Rel}_n(\mathbb{A}(\mathcal{M})) \models \mathbb{R}$.

This completes the case analysis!

Theorem

If \mathcal{M} halts with capacity κ then $\text{deg}(\mathbb{A}(\mathcal{M})) \leq \kappa + 16$.

Indecision: finitely generated, finitely related clones

- 1 Clones
- 2 The finite degree problem
- 3 The encoding of computation
- 4 Non-halting implies infinite degree
- 5 Halting implies finite degree
- 6 Conclusion**

Theorem

The following are equivalent.

- \mathcal{M} halts,
- $\deg(\mathbb{A}(\mathcal{M})) < \infty$ (i.e. $\mathbb{A}(\mathcal{M})$ is finitely related),
- \mathcal{M} halts with capacity $\deg(\mathbb{A}(\mathcal{M}))$.

Interesting observations

- There are infinitely many \mathcal{M} and $n \in \mathbb{N}$ such that \mathcal{M} halts in $\leq n$ steps but this is not provable in ZFC.
- Thus, there are infinitely many \mathcal{M} and $n \in \mathbb{N}$ such that $\deg(\mathbb{A}(\mathcal{M})) \leq n$ is true but not provable in ZFC.
- There are finite algebras \mathbb{A} that are finitely related but for which a bound on $\deg(\mathbb{A})$ cannot be proven.

- $\text{maxdeg}_\sigma(n) = \sup \left\{ \deg(\mathbb{A}) \mid \begin{array}{l} \mathbb{A} \text{ has signature } \sigma, \\ \deg(\mathbb{A}) < \infty, \text{ and } |A| \leq n \end{array} \right\}$

not computable.

Problem (Finite Generation Problem)

Given relations \mathcal{R} , decide if $\mathcal{C} = \text{Pol}(\mathcal{R})$ is finitely generated. That is, whether $\mathcal{C} = \text{Clo}(\mathcal{F})$ for some finite set of operations \mathcal{F} .

The theory of Natural Dualities for algebras has a very similar notion of relational entailment.

We can modify the definition of $\text{deg}(\cdot)$ to obtain a duality degree: $\text{deg}_{\partial}(\cdot)$.

Problem (Finite Duality Degree)

Decide whether $\text{deg}_{\partial}(\mathbb{A}) < \infty$ for finite \mathbb{A} .

Duality entailment implies usual entailment, so we already have that $\mathbb{A}(\mathcal{M})$ is not finitely duality related when \mathcal{M} does not halt.

Problem

If \mathcal{M} halts, is $\text{deg}_{\partial}(\mathbb{A}(\mathcal{M})) < \infty$?

Theorem

The following are equivalent.

- \mathcal{M} halts,
- $\deg(\mathbb{A}(\mathcal{M})) < \infty$ (i.e. $\mathbb{A}(\mathcal{M})$ is finitely related),
- \mathcal{M} halts with capacity $\deg(\mathbb{A}(\mathcal{M}))$.

“Finite Degree Clones are Undecidable”

Thank you for your attention.