Finite Degree Clones Are Undecidable

Matthew Moore

The University of Kansas Department of Electrical Engineering and Computer Science

May 20, 2019

Matthew Moore (KU)

Finite Degree Clones Are Undecidable

2019-05-20 1 / 32

- 1 Clones and The Finite Degree Problem
- **2** The Encoding of Computation
- 3 Non-halting Implies Infinite Degree
- **4** Halting Implies Finite Degree
- **5** Conclusion and Open Problems

1 Clones and The Finite Degree Problem

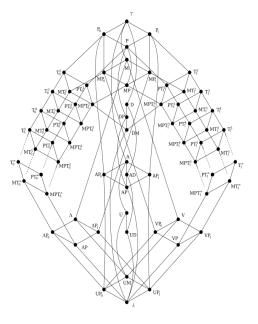
- 2 The Encoding of Computation
- On-halting Implies Infinite Degree
- **4** Halting Implies Finite Degree
- **5** Conclusion and Open Problems

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 (\geq 3)-element domains structure is quite complicated.



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

A clone on <u>finite</u> domain A can be **finitely specified** in essentially 2 ways.

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

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

These are the **finitely generated** clones.

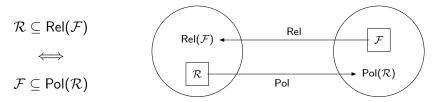
Second way: Given \mathcal{R} , a finite set of subpowers of A, define $Pol(\mathcal{R}) =$ "the set of all operations of A preserving all subpowers in \mathcal{R} ".

These are the finitely related/finite degree clones.

٠

 $\mathsf{Rel}(\mathcal{F}) = \left\{ R \subseteq A^n \mid R \text{ is preserved by all operations in } \mathcal{F} \right\}$ $\mathsf{Pol}(\mathcal{R}) = \left\{ f : A^n \to A \mid f \text{ preserves all subpowers in } \mathcal{R} \right\}$

These two operators form a Galois connection.



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

 $Clo = Pol \circ Rel$ and $RClo = Rel \circ Pol$.

If $\mathbb{R} \in \mathsf{RClo}(\mathcal{S})$, then we say " \mathcal{S} entails \mathbb{R} " and write $\mathcal{S} \models \mathbb{R}$.

If $f \in Pol(S)$, then we say "S entails f" and write $S \models f$.

٠

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

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

For a clone \mathcal{C} , define

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

For an algebra \mathbb{A} , define

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

The Finite Degree Problem

Input: finite algebra $\mathbb{A} = \langle A; f_1, \dots, f_n \rangle$ generating clone \mathcal{C} Output: whether deg $(\mathcal{C}) < \infty$

(seems to originate in the 70s with the study of lattices of clones over domains of more than 2 elements)

Matthew Moore (KU)

.

The Finite Degree Problem

Input: finite algebra $\mathbb{A} = \langle A; f_1, \dots, f_n \rangle$ generating clone COutput: whether deg $(C) < \infty$

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

Theorem

The following are equivalent.

- *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)
- certain omitting types (McKenzie, Wood)
- 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)

1 Clones and The Finite Degree Problem

2 The Encoding of Computation

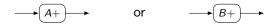
S Non-halting Implies Infinite Degree

Halting Implies Finite Degree

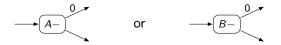
5 Conclusion and Open Problems

A Minsky machine has

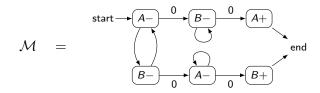
- registers A and B that have integer values ≥ 0 ,
- instructions to add 1 to a register,

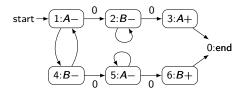


• instructions to test if a register is 0 and otherwise subtract 1 from it.



We can represent a Minsky machine as a finite flow graph.





Step	State	Α	В
0	(1,	2,	3)
1	(4,	1,	3)
2	(1,	1,	2)
3	(4,	0,	2)
4	(1,	0,	1)
5	(2,	0,	1)
6	(2,	0,	0)
7	(3,	0,	0)
8	(0,	1,	0)

How to represent intermediate computations?

- Assign a **state** to each node.
- A configuration (i, α, β) represents each stage of computation.
- Consider $\mathcal M$ as a function, and write

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

(single step of computation or multiple).

• On (α, β) , \mathcal{M} halts with registers (1,0) if $\alpha \leq \beta$ and (0,1) otherwise.

The encoding of computation

- let $\mathbb{A}(\mathcal{M})$ be the algebra we intend to build
- configurations (i, α, β) \iff special elements of $A(\mathcal{M})^n$
- term operations should simulate the action of $\mathcal M$ (need placemarker, •)
- computation on configurations ++++ subalgebra generation

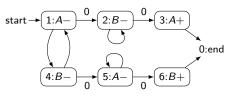
$$\mathbb{A}(\mathcal{M}) \text{ has universe...} \quad A(\mathcal{M}) = \Big\{ \left. \left< i, c \right> \mid i \text{ a state of } \mathcal{M}, \ c \in \{A, B, 0, \bullet, \times\} \Big\} \Big\}$$

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

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

The encoding of computation

- term operations should simulate the action of $\ensuremath{\mathcal{M}}$
- computation on configurations



Design considerations

•
$$M(r, s) = t$$
 if and only if...
• $r, s \in \operatorname{conf}(i, \alpha, \beta)$
• $r \neq s$
• $t \in \operatorname{conf}(\mathcal{M}(i, \alpha, \beta))$
via some $(R+)$ or $(R-)$

• otherwise introduce \times into the output t

Term operations

subalgebra generation

• M(x,y) for (R+) or (R-)

•
$$M'(x)$$
 for $(R-) \xrightarrow{0} \longrightarrow$

•
$$M'(r) = t$$
 if and only if...
• $r \in \operatorname{conf}(i, \alpha, \beta)$
• $t \in \operatorname{conf}(\mathcal{M}(i, \alpha, \beta))$
via some $(R-) \xrightarrow{0}$

Can we actually define M and M' with these features?

$$\mathcal{M}(x,y) = \begin{cases} \langle j, R \rangle & \text{if } x = \langle i, \bullet \rangle, \ y = \langle i, 0 \rangle, \ \overbrace{i:R+} \longrightarrow \overbrace{j:*}, \\ \langle j, 0 \rangle & \text{if } x = \langle i, \bullet \rangle, \ y = \langle i, R \rangle, \ \overbrace{i:R-} \longrightarrow \overbrace{j:*}, \\ \langle j, \bullet \rangle & \text{if } x = \langle i, 0 \rangle, \ y = \langle i, \bullet \rangle, \ \overbrace{i:R+} \longrightarrow \overbrace{j:*}, \\ \langle j, \bullet \rangle & \text{if } x = \langle i, R \rangle, \ y = \langle i, \bullet \rangle, \ \overbrace{i:R-} \longrightarrow \overbrace{j:*}, \\ \langle j, c \rangle & \text{if } x = y = \langle i, c \rangle, \ \overbrace{i:R+} \longrightarrow \overbrace{j:*} \text{ or } \overbrace{i:R-} \longrightarrow \overbrace{j:*}, \\ \langle j, \times \rangle & \text{else if } x = \langle i, c \rangle, \ y = \langle i, d \rangle, \ \overbrace{i:R+} \longrightarrow \overbrace{j:*} \text{ or } \overbrace{i:R-} \longrightarrow \overbrace{j:*}, \\ \langle i, \times \rangle & \text{otherwise, where } y = \langle i, c \rangle. \end{cases}$$

$$M'(x) = \begin{cases} \langle k, c \rangle & \text{if } x = \langle i, c \rangle, \ \overline{(i:R+)} \xrightarrow{0} \overline{(k:*)}, \ c \neq R, \\ \langle k, \times \rangle & \text{else if } x = \langle i, R \rangle, \ \overline{(i:R+)} \xrightarrow{0} \overline{(k:*)}, \\ \langle i, \times \rangle & \text{otherwise, where } x = \langle i, c \rangle. \end{cases}$$

Let's see an example computation...

.

$$\operatorname{start} \rightarrow \underbrace{1:A}_{(1,0)} \circ \underbrace{2:B}_{(2,0)} \circ \underbrace{3:A}_{(3,0)} \circ \underbrace{0:end}_{(4,0)} \circ \underbrace{1:A}_{(4,0)} \circ \underbrace{1:A}_{(4,0)} \circ \underbrace{1:A}_{(4,0)} \circ \underbrace{1:A}_{(4,0)} \circ \underbrace{1:A}_{(4,0)} \circ \underbrace{1:A}_{(1,A), (1,A)} \circ \underbrace{1:A}$$

Matthew Moore (KU)

.

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

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

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

Questions

- What if *R* doesn't contain these kinds of elements?
- What if R contains elements that aren't "computational"? (multiple •'s or non-constant states)

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

The **capacity** of a computation $\mathcal{M}^k(i, \alpha, \beta) = (j, \alpha', \beta')$ is the max sum of the registers.

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

We consider the halting problem on **0** register input: config = (1, 0, 0). Let $\mathbb{S}_m = Sg_{\mathbb{A}(\mathcal{M})^m} (conf(1, 0, 0))$.

Theorem (The Coding Theorem)

• If $\mathcal{M}^n(1,0,0) = (k, \alpha, \beta)$ has capacity < m then $conf(k, \alpha, \beta) \subseteq S_m$.

 If conf(k, α, β) ⊆ S_m and M does not halt with capacity < m then Mⁿ(1,0,0) = (k, α, β) for some n and has capacity < m.

Corollary

The following are equivalent.

- *M* halts with capacity < m,
- \mathbb{S}_m is halting (i.e. contains $conf(0, \alpha, \beta)$),
- every computational $\mathbb{R} \leq \mathbb{A}(\mathcal{M})^\ell$ with capacity $\geq m$ is halting.

Theorem (The Coding Theorem)

- If Mⁿ(1,0,0) = (k, α, β) has capacity < m then conf(k, α, β) ⊆ S_m.
- If conf(k, α, β) ⊆ S_m and M does not halt with capacity < m then Mⁿ(1,0,0) = (k, α, β) for some n and has capacity < m.

Framework for proving the hardness of algebraic properties

- Start out with $\mathbb{A}(\mathcal{M}) = \langle \mathcal{A}(\mathcal{M}) ; \mathcal{M}, \mathcal{M}' \rangle$.
- Add operations so that the property is recognizable in Rel(A(M))
 (ideally in the (S_m)_{m∈N}).
- Use a computer to verify necessary computations.
- Use software development techniques: write unit tests, rapidly iterate the operation definitions.

This allows us to give a more unified construction for the previously mentioned undecidability results in Universal Algebra.

1 Clones and The Finite Degree Problem

The Encoding of Computation

S Non-halting Implies Infinite Degree

Halting Implies Finite Degree

5 Conclusion and Open Problems

Observe

$$deg(\mathcal{C}) = \infty \quad \text{if and only if} \quad \forall n \ \text{Rel}_n(\mathcal{C}) \not\models \text{Rel}(\mathcal{C})$$
$$\text{if and only if} \quad \forall n \ \exists \mathbb{R} \ \text{Rel}_n(\mathcal{C}) \not\models \mathbb{R}$$

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

Two operations involved

- semilattice operation \land locally flat: $a \land b \neq \langle *, \times \rangle$ iff a = b
- "initialization" operation I(x, y)returns any configuration to conf(1, 0, 0)

At this point $\mathbb{A}(\mathcal{M}) = \langle A(\mathcal{M}) ; M, M', \wedge, I \rangle$.

 $\operatorname{Rel}_n(\mathcal{C}) \models \mathbb{R}$ if and only if \mathbb{R} can be built from $\operatorname{Rel}_n(\mathcal{C})$ using

- 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)

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

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

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

Lemma

Suppose that

$$ext{conf}(1,0,0) \subseteq \pi igg(igcap_{i \in I} \mu_i \Big(\prod_{j \in J_i} \mathbb{R}_{ij} \Big) igg) = \mathbb{S} \leq \mathbb{A}(\mathcal{M})^m$$

where π is a projection, the μ_i are permutations, and the \mathbb{R}_{ij} are a finite collection of members of $\operatorname{Rel}_n(\mathbb{A}(\mathcal{M}))$, 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 $m < \deg(\mathbb{A}(\mathcal{M}))$.
- If \mathcal{M} does not halt then $\mathbb{A}(\mathcal{M})$ is not finitely related.

Proof: Suppose that deg($\mathbb{A}(\mathcal{M})$) $\leq m$. This implies in particular that $\operatorname{Rel}_m(\mathbb{A}(\mathcal{M})) \models \mathbb{S}_{m+1}$. 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.

- 1 Clones and The Finite Degree Problem
- 2 The Encoding of Computation
- Son-halting Implies Infinite Degree
- 4 Halting Implies Finite Degree
- **5** Conclusion and Open Problems

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 $\operatorname{Rel}_k(\mathbb{A}(\mathcal{M})) \models \operatorname{Rel}_n(\mathbb{A}(\mathcal{M}))$ for all n.
- We proceed by induction on n.
- The base case of n = k is trivial.
- We thus endeavor to prove $\operatorname{Rel}_{n-1}(\mathbb{A}(\mathcal{M})) \models \mathbb{R}$ for $\mathbb{R} \in \operatorname{Rel}_n(\mathbb{A}(\mathcal{M}))$.
- Relations in Rel_n(A(M)) can be divided into 4 different kinds, so we proceed by cases.
- We add operations to handle entailment in each of the different cases: $N_{\bullet}(w, x, y, z)$, P(u, v, x, y), H(x, y), $N_0(x, y, z)$, S(x, y, z).
- $\mathbb{A}(\mathcal{M}) = \langle \mathcal{A}(\mathcal{M}) ; \mathcal{M}, \mathcal{M}', \wedge, \mathcal{I}, \mathcal{N}_{\bullet}, \mathcal{P}, \mathcal{H}, \mathcal{N}_{0}, \mathcal{S} \rangle$ (final version)

٠

$$\mathbb{A}(\mathcal{M}) = \left\langle \mathcal{A}(\mathcal{M}) ; \ \mathcal{M}, \mathcal{M}', \wedge, \mathcal{I}, \mathcal{N}_{\bullet}, \mathcal{P}, \mathcal{H}, \mathcal{N}_{0}, \mathcal{S} \right\rangle$$

Case ${\mathbb R}$ is non-computational

- There is an element with 2 •'s or with non-constant state.
- 2 •'s: operation N_• 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 $\operatorname{Rel}_{m-1}(\mathbb{A}(\mathcal{M})) \models \mathbb{R}$.

Case ${\mathbb R}$ is halting

- *R* contains an element of conf(0,0,0).
- Any element of conf(0,0,0) can be used with operations *I*, *H*, and *N*₀ to prove entailment.

Theorem

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

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])

D(ℝ) = "coordinates i such that ∃r ∈ R with r(i) = (j, •)"
 = "the • (dot) part of ℝ."

• $\mathcal{N}(\mathbb{R}) =$ "the inherently non-halting part of \mathbb{R} " ...

• $\pi_{\mathcal{N}(\mathbb{R})}(\mathbb{R})$ is non-halting,

 $\circ \text{ if } \mathcal{K} = \left| \mathcal{N}(\mathbb{R}) \cap \mathcal{D}(\mathbb{R}) \right| \text{ then } \mathbb{S}_{\mathcal{K}} \leq \mathbb{R}.$

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 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 $n \ge \kappa + 16$ and

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

Then $\operatorname{Rel}_{n-1}(\mathbb{A}(\mathcal{M})) \models \mathbb{R}$.

This completes the case analysis!

Theorem

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

- 1 Clones and The Finite Degree Problem
- 2 The Encoding of Computation
- On-halting Implies Infinite Degree
- Halting Implies Finite Degree
- **5** Conclusion and Open Problems

Theorem

The following are equivalent.

- *M* halts,
- $deg(\mathbb{A}(\mathcal{M})) < \infty$ (i.e. $\mathbb{A}(\mathcal{M})$ is finitely related),
- \mathcal{M} halts with capacity at least deg $(\mathbb{A}(\mathcal{M})) 16$.

Interesting observations

- There are infinitely many ${\cal M}$ with halting status independent of ZFC.
- Thus, there are infinitely many \mathcal{M} such that deg($\mathbb{A}(\mathcal{M})$) $< \infty$ is independent of ZFC.
- There are finite algebras A that whose finite-relatedness is independent of ZFC.

•
$$\mathsf{maxdeg}_{\sigma}(n) = \mathsf{sup} \left\{ \begin{array}{ll} \mathbb{A} \ \mathsf{deg}(\mathbb{A}) & | & \mathbb{A} \ \mathsf{has signature} \ \sigma, \\ \mathsf{deg}(\mathbb{A}) < \infty, \ \mathsf{and} \ |A| \leq n \end{array} \right\}$$

is not computable.

Problem

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

Problem

Given relations \mathcal{R} and operations \mathcal{F} , decide whether $Pol(\mathcal{R}) = Clo(\mathcal{F})$.

Natural Duality Problems

We can modify the definition of deg(·) to obtain a duality degree: deg_{∂}(·).

Problem (Finite Duality Degree)

Decide whether 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 deg $_{\partial}(\mathbb{A}(\mathcal{M})) < \infty$?

Problem

Given finite \mathbb{A} , decide whether \mathbb{A} admits a duality.

Matthew Moore (KU)

Finite Degree Clones Are Undecidable

Theorem

The following are equivalent.

- *M* halts,
- $deg(\mathbb{A}(\mathcal{M})) < \infty$ (i.e. $\mathbb{A}(\mathcal{M})$ is finitely related),
- *M* halts with capacity at least deg(*A*(*M*)) − 16.

Thank you for your attention.