The Hartmanis-Stearns problem and some weaker results

Sipho Kemkes

Supervisor: Wieb Bosma

January 24, 2024

Overview

- The papers
- Hartmanis and Stearns' results
- Proven results
- Morphisms and the second result
- The other results and their proof

The papers

- Boris Adamczewski, Julien Cassaigne and Marion le Gonidec. *"On the computational complexity of algebraic numbers: the Hartmanis-Stearns problem revisited".* Transactions of the American Mathematical Society 373(5), 2016.

The papers

- Boris Adamczewski, Julien Cassaigne and Marion le Gonidec. *"On the computational complexity of algebraic numbers: the Hartmanis-Stearns problem revisited".* Transactions of the American Mathematical Society 373(5), 2016.
- J. Hartmanis and R.E. Stearns. *"On the computational complexity of algorithms".* Transactions of the American Mathematical Society, 117, 1965.

Hartmanis and Stearns' results

Theorem 10

All rational numbers are computable in linear time.

Hartmanis and Stearns’ results

Theorem 10

All rational numbers are computable in linear time.

Theorem 11

All algebraic numbers are computable in quadratic time.

Hartmanis and Stearns' results

Theorem 10

All rational numbers are computable in linear time.

Theorem 11

All algebraic numbers are computable in quadratic time.

Theorem 12

There are transcendental numbers that are computable in linear time.

The Hartmanis-Stearns problem

The Hartmanis-Stearns problem

Do there exist irrational algebraic numbers for which the first n binary digits can be computed in $O(n)$ operations by a multitape deterministic Turing machine?

Proven results

- Enumerators versus transducers

Proven results

- Enumerators versus transducers

Cobham's first claim

The base-b expansion of an algebraic irrational number cannot be generated by a uniform morphism or, equivalently, by a finite automaton.

Proven results

- Enumerators versus transducers

Cobham's first claim

The base-b expansion of an algebraic irrational number cannot be generated by a uniform morphism or, equivalently, by a finite automaton.

Cobham's second claim

The base-b expansion of an algebraic irrational number cannot be generated by a morphism with exponential growth.

Proven results

- Enumerators versus transducers

Cobham's first claim

The base-b expansion of an algebraic irrational number cannot be generated by a uniform morphism or, equivalently, by a finite automaton.

Cobham's second claim

The base-b expansion of an algebraic irrational number cannot be generated by a morphism with exponential growth.

Theorem 1.3

The base-b expansion of an algebraic irrational number cannot be generated by a deterministic pushdown automaton

Morphims

- A map $A \to A^*$ extended to a map $\sigma : A^* \to A^*$ is a morphism.

Morphims

- A map $A \to A^*$ extended to a map $\sigma : A^* \to A^*$ is a morphism.
- The incidence matrix of σ is M_σ. To define it, order the elements of A as $A = \{a_1, a_2, \ldots, a_d\}$. Then M_σ is defined by $(M_\sigma)_{i,j} = |\sigma(a_j)|_{a_i}$

Morphims

- A map $A \to A^*$ extended to a map $\sigma : A^* \to A^*$ is a morphism.
- The incidence matrix of σ is M_σ. To define it, order the elements of A as $A = \{a_1, a_2, \ldots, a_d\}$. Then M_σ is defined by $(M_\sigma)_{i,j} = |\sigma(a_j)|_{a_i}$
- A morphism has exponential growth if the spectral radius of M_σ is bigger than one.

Proposition ABL

Diophantine exponent

Let ρ be a real number. Then

$dio(\alpha) := \sup_\rho\{\rho \mid \exists U, V$ s.t. UV^β prefix of α and $\frac{|UV^\beta|}{|UV|} \geq \rho\}$

Proposition ABL

Diophantine exponent

Let ρ be a real number. Then

$dio(\alpha) := \sup_\rho\{\rho \mid \exists U, V \text{ s.t. } UV^\beta \text{ prefix of } \alpha \text{ and } \frac{|UV^\beta|}{|UV|} \geq \rho\}$

Proposition ABL

Let ξ be a real number with $\xi_b := 0.a1a2\ldots.$ Suppose that $dio(\alpha) > 1$ where $\alpha := a1a2$. Then ξ is either rational or transcendental.

Cobham's second claim

Proposition 4.3

Let α be an infinite sequence that can be generated by a morphism with exponential growth. Then $dio(\alpha) > 1$.

Cobham's second claim

Proposition 4.3

Let α be an infinite sequence that can be generated by a morphism with exponential growth. Then $dio(\alpha) > 1$.

Cobham's second claim

The base-b expansion of an algebraic irrational number cannot be generated by a morphism with exponential growth.

Cobham's second claim

Proposition 4.3

Let α be an infinite sequence that can be generated by a morphism with exponential growth. Then $dio(\alpha) > 1$.

Cobham's second claim

The base-b expansion of an algebraic irrational number cannot be generated by a morphism with exponential growth.

- Proof: combine Propositions ABL and 4.3.

Pushdown automata

- Last in first out stack

Pushdown automata

- Last in first out stack
- Deterministic

Pushdown automata

- Last in first out stack
- Deterministic
- Transducer

Pushdown automata

- Last in first out stack
- Deterministic
- Transducer
- $\epsilon -$moves

Pushdown automata

- Last in first out stack
- Deterministic
- Transducer
- $\epsilon-$moves
- Configurations

Pushdown automata

- Last in first out stack
- Deterministic
- Transducer
- $\epsilon-$moves
- Configurations(-equivalence)

Proposition 4.6

Proposition 4.6

Let ξ be a real number generated by a k-pushdown automaton. If there exist two distinct positive integers n and n' such that $C(n) \sim C(n')$, then ξ is either rational or transcendental.

Proposition 4.6 (Proof)

- Proof: Let ξ be a real number and let $n < n'$ be positive integers such that $C(n) \sim C(n')$. Let $\alpha := (a_i)_{i \geq 1}$ be the output of the pushdown automaton that generates ξ such that $\xi_k = 0.a_1 a_2 \ldots$. Then by definition $a_{[w_n w]_k} = a_{[w_{n'} w]_k}$ for all $w \in \Sigma_k^*$.

Proposition 4.6 (Proof)

- Proof: Let ξ be a real number and let $n < n'$ be positive integers such that $C(n) \sim C(n')$. Let $\alpha := (a_i)_{i \geq 1}$ be the output of the pushdown automaton that generates ξ such that $\xi_k = 0.a_1 a_2 \dots$. Then by definition $a_{[w_n w]_k} = a_{[w_{n'} w]_k}$ for all $w \in \Sigma_k^*$.
- Now for a positive integer l we get $a_{k^l n+i} = a_{k^l n'+i}$ for all $i \in [0, k^l - 1]$.

Proposition 4.6 (Proof)

- Proof: Let ξ be a real number and let $n < n'$ be positive integers such that $C(n) \sim C(n')$. Let $\alpha := (a_i)_{i \geq 1}$ be the output of the pushdown automaton that generates ξ such that $\xi_k = 0.a_1 a_2 \ldots$. Then by definition $a_{[w_n w]_k} = a_{[w_{n'} w]_k}$ for all $w \in \Sigma_k^*$.
- Now for a positive integer l we get $a_{k^l n+i} = a_{k^l n'+i}$ for all $i \in [0, k^l - 1]$.
- Now take $U = a_1 a_2 \ldots a_{k^l n-1}$ and $V = ak^l nak^l n + 1 \ldots a_{k^l n'-1}$. Then $UV^{1+\frac{1}{n'-n}}$ is a prefix of α. We also get $\frac{|UV^{1+\frac{1}{n'-n}}|}{|UV|} = 1 + \frac{1}{n'-1/k^l} \geq 1 + \frac{1}{n'}$.

Proposition 4.6 (Proof)

- Proof: Let ξ be a real number and let $n < n'$ be positive integers such that $C(n) \sim C(n')$. Let $\alpha := (a_i)_{i \geq 1}$ be the output of the pushdown automaton that generates ξ such that $\xi_k = 0.a_1 a_2 \ldots$. Then by definition $a_{[w_n w]_k} = a_{[w_{n'} w]_k}$ for all $w \in \Sigma_k^*$.
- Now for a positive integer l we get $a_{k^l n+i} = a_{k^l n'+i}$ for all $i \in [0, k^l - 1]$.
- Now take $U = a_1 a_2 \ldots a_{k^l n-1}$ and $V = ak^l nak^l n + 1 \ldots a_{k^l n'-1}$. Then $UV^{1+\frac{1}{n'-n}}$ is a prefix of α. We also get $\frac{|UV^{1+\frac{1}{n'-n}}|}{|UV|} = 1 + \frac{1}{n'-1/k^l} \geq 1 + \frac{1}{n'}$.
- Now we have $dio(\alpha) \geq 1 + \frac{1}{n'} > 1$ and then proposition ABL gives that ξ is rational or transcendental.

Cobham's first claim

Cobham's first claim

The base-b expansion of an algebraic irrational number cannot be generated by a uniform morphism or, equivalently, by a finite automaton.

Proof: There is a finite amount of states and an infinite number of possible inputs, so the pigeonhole principle gives that there are two inputs that end up in the same state. Then Proposition 4.6 gives the result.

Theorem 1.3

Theorem 1.3

The base-b expansion of an algebraic irrational number cannot be generated by a deterministic pushdown automaton

Theorem 1.3

Theorem 1.3

The base-b expansion of an algebraic irrational number cannot be generated by a deterministic pushdown automaton

- Let ξ be a real number generated by a pushdown automaton. Let $S(w)$ denote the contents of the stack after reading input w. Then we have the stackheight $H(w) := |S(w)|$.

Theorem 1.3

Theorem 1.3

The base-b expansion of an algebraic irrational number cannot be generated by a deterministic pushdown automaton

- Let ξ be a real number generated by a pushdown automaton. Let $S(w)$ denote the contents of the stack after reading input w. Then we have the stackheight $H(w) := |S(w)|$.
- For all positive integers m we define $\mathcal{H}_m := \{w \in \mathbb{R}_k \mid H(w) \leq m\}$

Theorem 1.3

Theorem 1.3

The base-b expansion of an algebraic irrational number cannot be generated by a deterministic pushdown automaton

- Let ξ be a real number generated by a pushdown automaton. Let $S(w)$ denote the contents of the stack after reading input w. Then we have the stackheight $H(w) := |S(w)|$.
- For all positive integers m we define $\mathcal{H}_m := \{w \in \mathbb{R}_k \mid H(w) \leq m\}$
- Case 1: There is a m such that $\mathcal{H}_m$ is infinite. There is a finite amount of configurations with a stackheight of at most m, but we have an infinite amount of inputs, so the pigeonhole principle gives that there must be a $n \neq n'$ with $C(n) \sim C(n')$ and then we have proposition 4.6 again to give that

Proof of Theorem (continued)

- Case 2: all $\mathcal{H}_m$ are finite. We pick a $v_m \in \mathcal{H}_m$ with maximal length. Then because of $\mathcal{H}_m \subseteq \mathcal{H}_m + 1$, we have $|v_m| \leq |v_{m+1}|$. Furthermore we have $\mathcal{R}_k = \bigcup_{m=1}^{\infty} \mathcal{H}_k$ which implies that the set $\{v_m \mid m \geq 1\}$ is infinite.

Proof of Theorem (continued)

- Case 2: all $\mathcal{H}_m$ are finite. We pick a $v_m \in \mathcal{H}_m$ with maximal length. Then because of $\mathcal{H}_m \subseteq \mathcal{H}_m + 1$, we have $|v_m| \leq |v_{m+1}|$. Furthermore we have $\mathcal{R}_k = \bigcup_{m=1}^{\infty} \mathcal{H}_k$ which implies that the set $\{v_m \mid m \geq 1\}$ is infinite.
- Because of this definition, we have $H(v_m) < H(v_m w)$ for all $w \in \Sigma^*$.

Proof of Theorem (continued)

- Case 2: all $\mathcal{H}_m$ are finite. We pick a $v_m \in \mathcal{H}_m$ with maximal length. Then because of $\mathcal{H}_m \subseteq \mathcal{H}_m + 1$, we have $|v_m| \leq |v_{m+1}|$. Furthermore we have $\mathcal{R}_k = \bigcup_{m=1}^{\infty} \mathcal{H}_k$ which implies that the set $\{v_m \mid m \geq 1\}$ is infinite.
- Because of this definition, we have $H(v_m) < H(v_m w)$ for all $w \in \Sigma^*$.
- Take m big enough so we have $|v_m| > |v_1|$ so we have $H(v_m) > 1$. For such m, we decompose $S(v_m)$ as $S(v_m) = X_m z_m$. This means that X_m is a prefix of $S(v_m w)$ for all $w \in \Sigma^*$.

Proof of Theorem (continued)

- Case 2: all $\mathcal{H}_m$ are finite. We pick a $v_m \in \mathcal{H}_m$ with maximal length. Then because of $\mathcal{H}_m \subseteq \mathcal{H}_m + 1$, we have $|v_m| \leq |v_{m+1}|$. Furthermore we have $\mathcal{R}_k = \bigcup_{m=1}^{\infty} \mathcal{H}_k$ which implies that the set $\{v_m \mid m \geq 1\}$ is infinite.
- Because of this definition, we have $H(v_m) < H(v_m w)$ for all $w \in \Sigma^*$.
- Take m big enough so we have $|v_m| > |v_1|$ so we have $H(v_m) > 1$. For such m, we decompose $S(v_m)$ as $S(v_m) = X_m z_m$. This means that X_m is a prefix of $S(v_m w)$ for all $w \in \Sigma^*$.
- This means that $(q_{v_m}, S(v_m)) \sim (q_{v_m}, z_m)$. Note that $(q_{v_m}, z_m) \in Q \times \Gamma$ which is a finite set, but $\{v_m \mid m \geq 1\}$ is an infinite set.

Proof of Theorem (continued)

- Case 2: all $\mathcal{H}_m$ are finite. We pick a $v_m \in \mathcal{H}_m$ with maximal length. Then because of $\mathcal{H}_m \subseteq \mathcal{H}_m + 1$, we have $|v_m| \leq |v_{m+1}|$. Furthermore we have $\mathcal{R}_k = \bigcup_{m=1}^{\infty} \mathcal{H}_k$ which implies that the set $\{v_m \mid m \geq 1\}$ is infinite.
- Because of this definition, we have $H(v_m) < H(v_m w)$ for all $w \in \Sigma^*$.
- Take m big enough so we have $|v_m| > |v_1|$ so we have $H(v_m) > 1$. For such m, we decompose $S(v_m)$ as $S(v_m) = X_m z_m$. This means that X_m is a prefix of $S(v_m w)$ for all $w \in \Sigma^*$.
- This means that $(q_{v_m}, S(v_m)) \sim (q_{v_m}, z_m)$. Note that $(q_{v_m}, z_m) \in Q \times \Gamma$ which is a finite set, but $\{v_m \mid m \geq 1\}$ is an infinite set.
- The pigeonhole principle gives that there must two $m \neq m'$ such that $(q_{v_m}, S(v_m)) \sim (q_{v_{m'}}, S(v_{m'}))$ and then proposition 4.6 gives that ξ is rational or transcendental.