Department of Mathematics and Statistics

University of Helsinki

Descriptive Complexity of Boolean and Algebraic Complexity Classes

Juha Kontinen

25.2.2026

Motivation

Descriptive Complexity

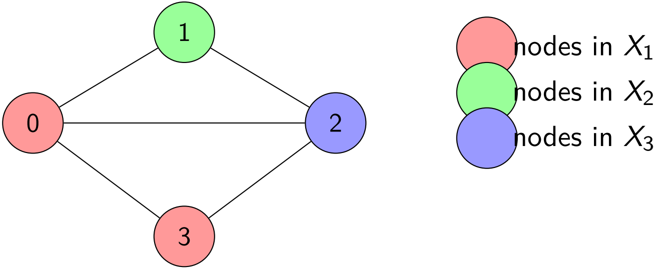
- Computational resources such as space, time, non-determinism can be related to the expressivity of logical languages over finite structures.
- The birth of the area was marked by Fagin's theorem characterizing NP in terms of existential second-order logic [Fag74].

Algebraic Computation

- Study problems not suitable for Boolean models
- Use algebraic results to illuminate classical complexity
- Semirings
  - More versatile than fields or rings
  - Captures very natural structures, e.g. $\mathbb{N}$, $\mathbb{B}$
  - Semiring Provenance [GKT07]

Fagin's theorem exemplified

Let $G = (\{0, \ldots, n-1\}, E)$ be a finite graph. The problem whether G is three-colorable asks if the vertices of G can be partitioned (colored with three colors) into X_1, X_2, X_3 s.t. there exists no edges between the vertices in X_i, for $1 \leq i \leq 3$.



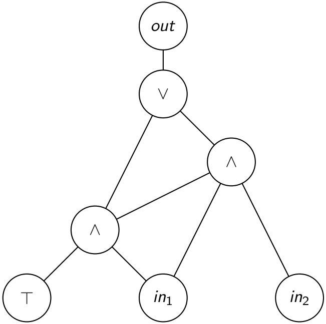
Fagin's theorem exemplified

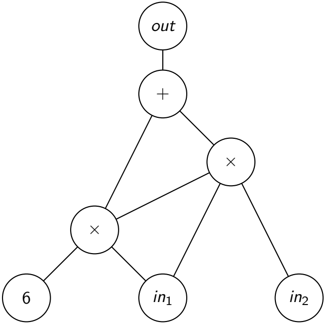
- Denote by $3\mathrm{COL}$ the class of finite three-colorable graphs.
- The computational problem: given G, determine if $G \in 3\mathrm{COL}$, is NP-complete.
- In logic, we can show that $G \in 3\mathrm{COL}$ iff $G \models \phi$, where

$$\phi := \exists X_1 X_2 X_3 \forall x_1 \forall x_2 (\theta \wedge (E(x_1, x_2) \rightarrow \vee_{i \neq j}(X_i(x_1) \wedge X_j(x_2)))),$$

where θ expresses that X_i's form a partition of the domain of G.

Boolean vs. arithmetic circuits





Circuit evaluation

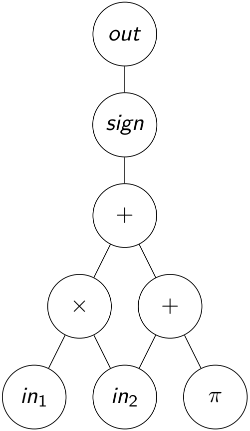
Circuits over basis B

- Directed Acyclic Graph with node types:
  - Input (fan-in 0)
  - Constant (fan-in 0)
  - $f \in B$ (fan-in ≥ 0)
  - Output (fan-in 1)

Circuit evaluation

Circuits over basis B

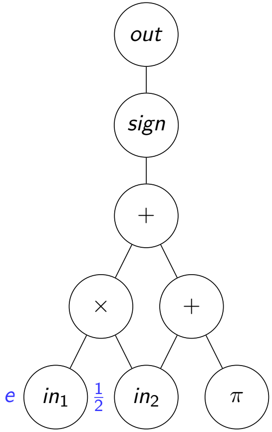
- Directed Acyclic Graph with node types:
  - Input (fan-in 0)
  - Constant (fan-in 0)
  - $f \in B$ (fan-in ≥ 0)
    - $+$, $\times$, *sign*, *zero*
  - Output (fan-in 1)



Circuit evaluation

Circuits over basis B

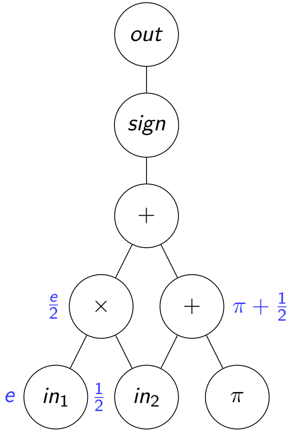
- Directed Acyclic Graph with node types:
  - Input (fan-in 0)
  - Constant (fan-in 0)
  - $f \in B$ (fan-in ≥ 0)
    - $+$, $\times$, *sign*, *zero*
  - Output (fan-in 1)



Circuit evaluation

Circuits over basis B

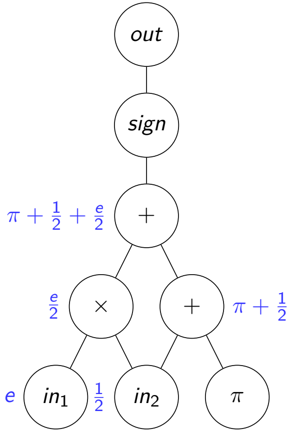
- Directed Acyclic Graph with node types:
  - Input (fan-in 0)
  - Constant (fan-in 0)
  - $f \in B$ (fan-in ≥ 0)
    - $+$, $\times$, *sign*, *zero*
  - Output (fan-in 1)



Circuit evaluation

Circuits over basis B

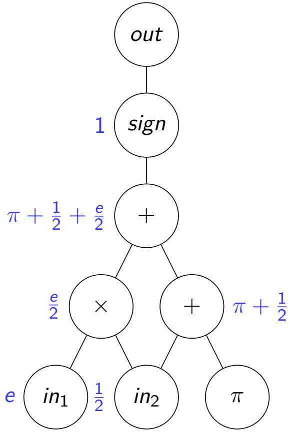
- Directed Acyclic Graph with node types:
  - Input (fan-in 0)
  - Constant (fan-in 0)
  - $f \in B$ (fan-in ≥ 0)
    - $+$, $\times$, *sign*, *zero*
  - Output (fan-in 1)



Circuit evaluation

Circuits over basis B

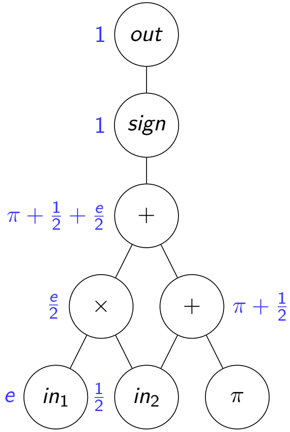
- Directed Acyclic Graph with node types:
  - Input (fan-in 0)
  - Constant (fan-in 0)
  - $f \in B$ (fan-in ≥ 0)
    - $+$, $\times$, *sign*, *zero*
  - Output (fan-in 1)



Circuit evaluation

Circuits over basis B

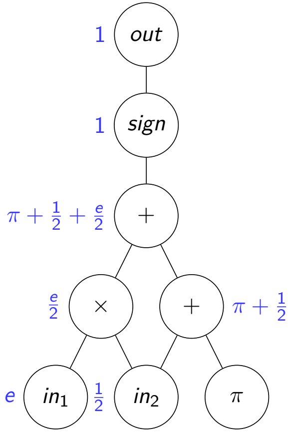
- Directed Acyclic Graph with node types:
  - Input (fan-in 0)
  - Constant (fan-in 0)
  - $f \in B$ (fan-in ≥ 0)
    - $+$, $\times$, *sign*, *zero*
  - Output (fan-in 1)



Circuit evaluation

Circuits over basis B

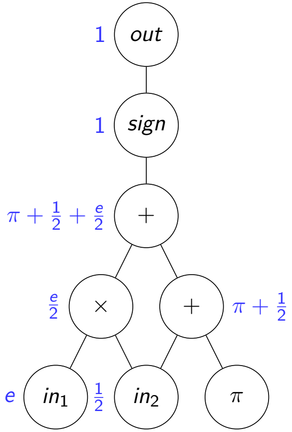
- Directed Acyclic Graph with node types:
  - Input (fan-in 0)
  - Constant (fan-in 0)
  - $f \in B$ (fan-in ≥ 0)
    - $+$, $\times$, *sign*, *zero*
  - Output (fan-in 1)
- *size*: number of gates
  - 8
- *depth*: longest path from input to output
  - 4



Circuit evaluation

Circuits over basis B

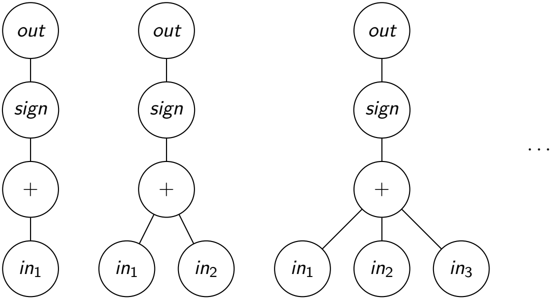
- Directed Acyclic Graph with node types:
  - Input (fan-in 0)
  - Constant (fan-in 0)
  - $f \in B$ (fan-in ≥ 0)
    - $+$, $\times$, *sign*, *zero*
  - Output (fan-in 1)
- *size*: number of gates
  - 8
- *depth*: longest path from input to output
  - 4
- Non-uniform!



Circuit families and uniformity

A very uniform circuit family

- Sequences $\mathcal{C} = (C_1, C_2, \ldots)$ of circuits where C_i has i input gates



AC^0 and TC^0

Definition

AC^0 and TC^0 refer to the classes of languages (sets of finite binary strings) recognized by $\mathrm{DLOGTIME}$-uniform families $(C_n)_{n\in\mathbb{N}}$ of constant depth polynomial-size circuits.

- For AC^0, the circuit C_n may have NOT and unbounded fan-in AND and OR gates.
- For TC^0, also unbounded fan-in MAJORITY gates are allowed, which output 1 iff at least half of the inputs are 1.
- $\mathrm{DLOGTIME}$-uniformity: $(C_n)_{n\in\mathbb{N}}$, as a family of directed acyclic graphs, can be recognized in time $O(\log(n))$.

First-order logic

FO-formulas

- The formulas of FO over vocabulary $\sigma = \{R_1, \ldots, R_n\}$ are defined as

$$\varphi ::= x = y \mid R_i(\vec{x}) \mid \varphi \wedge \varphi \mid \neg\varphi \mid \exists x\varphi$$

- The connective $\vee$ and quantifier $\forall$ can viewed as shorthands
- over ordered models (with arithmetic) we also have atomic formulas $x \leq y$ ($x + y = z$ and $x \times y = z$)

Generalized quantifiers

Definition

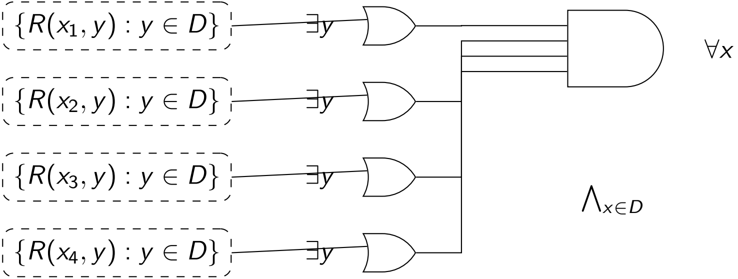
Let $S \subseteq \mathbb{N}$. The quantifiers C_S, Maj and I are defined by:

$$\begin{aligned}
\mathfrak{M} &\models \mathrm{C}_S\, x\, (\psi(x)) && \text{iff} \quad |\psi^{\mathfrak{M}}| \in S, \\
\mathfrak{M} &\models \mathrm{Maj}\ x\, (\psi(x)) && \text{iff} \quad |\psi^{\mathfrak{M}}| > |\mathfrak{M}|/2, \\
\mathfrak{M} &\models \mathrm{I}\ xy\, (\psi(x), \phi(y)) && \text{iff} \quad |\psi^{\mathfrak{M}}| = |\phi^{\mathfrak{M}}|.
\end{aligned}$$

These quantifiers can be added to first-order logic to obtain, e.g.,the logic FO(Maj).

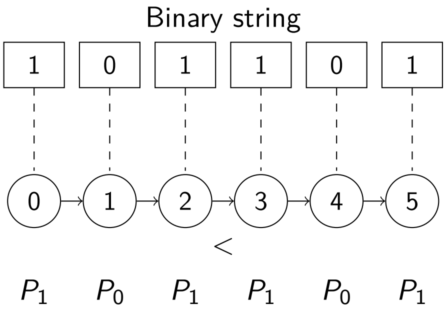
From FO-formulas to uniform constant-depth circuits

$\forall x \, \exists y \, R(x, y)$ over $D = \{1, \ldots, n\}$



$\bigvee_{y \in D} R(x, y)$ (computed for each x)

Binary strings as word models



Word model $(\{0, \ldots, n-1\}, <, P_0, P_1)$

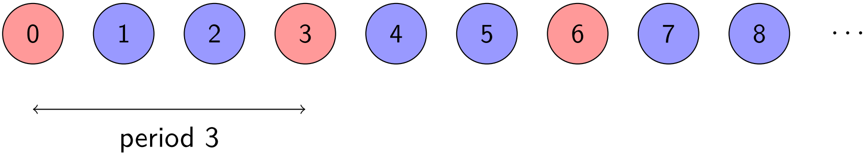
Circuit complexity and first-order logic

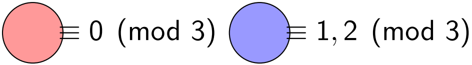
- Many circuit complexity classes have been logically characterized in terms of varying sets of arithmetic relations and generalized quantifiers [BIS90]. In particular:
- DLOGTIME-uniform $\mathrm{AC}^0 \equiv \mathsf{FO}_{\{\leq,+,\times\}}$
- DLOGTIME-uniform $\mathrm{TC}^0 \equiv \mathsf{FO}_{\{\leq,+,\times\}}(\mathsf{Maj}) \equiv \mathsf{FO}_{\{\leq,+,\times\}}(\mathsf{I})$, where Maj is the majority quantifier and I the Härtig quantifier (equicardinality).
- We know that **Parity** is not in AC^0 but it is not known if $\mathrm{TC}^0 \subsetneq \mathrm{NP}$.
- It is also known that $\mathrm{TC}^0 > \mathsf{FO}_{\{\leq\}}(\mathsf{Maj})$.

Cardinality quantifiers over ordered structures

- Cardinality quantifiers C_S are the simplest kind of unary quantifiers and their definability theory is well understood over unordered structures.
- Over ordered structures cardinality quantifiers can be classified into two cases: the equicardinality quantifier I can be defined in $\mathsf{FO}_{\{\leq\}}(\mathsf{C}_s)$ iff S is sufficiently **non-periodic** [Luo04].
- For example, if $S = \{2^n \mid n \in \mathbb{N}\}$ or $S = \mathrm{rg}(P)$, where $P\colon \mathbb{N} \to \mathbb{N}$ is a polynomial function with nonnegative integer coefficients of degree at least two, then I can be expressed in $\mathsf{FO}_{\{\leq\}}(\mathsf{C}_S)$. Note that $+$ can be easily defined with I over ordered structures.

Periodicity exemplified





The set S consisting of blue/red elements is periodic

Characterizing TC^0 in terms of cardinality quantifiers

A warm-up result

Theorem ([HKL25])

Let $P\colon \mathbb{N} \to \mathbb{N}$ *be a polynomial function with coefficients in* $\mathbb{N}$ *and* $\deg(P) = k \geq 2$*, and* $S = \mathrm{rg}(P)$*. Then*

$$\mathsf{FO}_{\{\leq\}}(\mathsf{C}_S) \equiv \mathrm{TC}^0 \ .$$

Proof.

Easy special case: $P = x^2$. Let $\mathrm{Sq} = \{n^2 \mid n \in \mathbb{N}\}$ and consider C_{Sq}. Now, I is definable in $\mathsf{FO}_{\leq}(\mathsf{C}_{\mathrm{Sq}})$ and $+$ is definable in $\mathsf{FO}_{\leq}(\mathsf{I})$. On the other hand, $\times$ is already definable in $\mathsf{FO}_{\{\leq,+,\mathrm{Sq}\}}$. It follows that

$$\mathsf{FO}_{\{\leq\}}(\mathsf{C}_{\mathrm{Sq}}) \equiv \mathsf{FO}_{\{\leq,+,\times\}}(\mathsf{I}, \mathsf{C}_{\mathrm{Sq}}) \equiv \mathrm{TC}^0.$$

□

Characterizing TC^0 in terms of cardinality quantifiers

Theorem ([HKL25])

Let $S \subseteq \mathbb{N}$ be ***pseudoloose****. Then*

$$\mathsf{FO}_{\{\leq\}}(\mathsf{C}_S) \geq \mathrm{TC}^0.$$

Note: there are uncountably many pseudoloose sets, e.g., $S = \{\lfloor x^r \rfloor \mid x \in \mathbb{N}\}$ is pseudoloose for any real $r > 1$.

Semirings

A **semiring** is a set K equipped with two operations $+$ and $\times$ and two elements 0 and 1 such that

- $(K, +, 0)$ is a commutative monoid
- $(K, \times, 1)$ is a monoid
- $\times$ is distributive w.r.t. $+$
- 0 is absorbing

K is **commutative**, if $(K, \times, 1)$ is commutative.

Examples

- $\mathbb{N}$, $\mathbb{R}$, $\mathbb{R}_{\geq 0}$, $\mathbb{C}$, $\mathbb{B}$, $\mathbb{Z}$
- Tropical semiring $(\mathbb{R} \cup \{\infty\}, \min, +, \infty, 0)$
- Łukasiewicz semiring $([0, 1], \max, \min(0, x + y - 1), 0, 1)$

Semirings and K-relations

- A K-**relation** is a relation over a (finite) domain A whose tuples are annotated with elements of K.
- This general notion subsumes many familiar structures: for instance, probability distributions arise when $K = \mathbb{R}_{\geq 0}$, while multisets correspond to $K = \mathbb{N}$. In this way, K-relations provide a uniform abstraction for reasoning across a wide range of computational contexts.

Figure: K-relations over domain $A = \{a, b\}$ and attributes $\{x, y\}$.

$K = \mathbb{B}$

x	y	
a	a	1
a	b	1
b	a	0
b	b	0

$K = \mathbb{N}$

x	y	
a	a	2
a	b	0
b	a	0
b	b	5

$K = \mathbb{R}_{\geq 0}$

x	y	
a	a	1/4
a	b	3/4
b	a	0
b	b	0

Semiring provenance in database theory

- Database queries under:
  - Standard semantics: what are the query answers?
  - Semiring semantics: how to get the query answers?
- Operates on K-relations,
- Queries propagate the annotations of input tuples to the query results, indicating how each answer was derived,
- Different semirings can also be used to measure the level of confidence or cost of evaluation for query answers.

Semiring semantics of first-order logic

- Orginates from the work in semiring provenance in databases [GT17]. Similar logics have been considered in the **weighted-automata** context (see, e.g., [Bad+24]).
- Fix a semiring $K = (K, +, \cdot, 0, 1)$, a finite domain A and a vocabulary τ.
- The semiring interpretation for FO[τ]-formulas is defined via a K-interpretation π assigning K-values to all τ-atomic and negated atomic facts (e.g, $R(\vec{a})$ and $a_1 = a_2$ for $R \in \tau$) over elements of A.

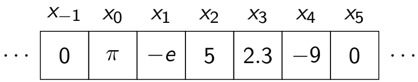
The mapping π can be then extended to compound formulas using the rules:

$$\pi(\phi \vee \psi) = \pi\phi + \pi\psi \qquad \pi(\phi \wedge \psi) = \pi\phi \cdot \pi\psi$$
$$\pi\forall x\phi = \prod_{a\in A} \pi\phi(a/x) \qquad \pi\exists x\phi = \sum_{a\in A} \pi\phi(a/x)$$

What can we say about the computational properties of FO under the semiring semantics

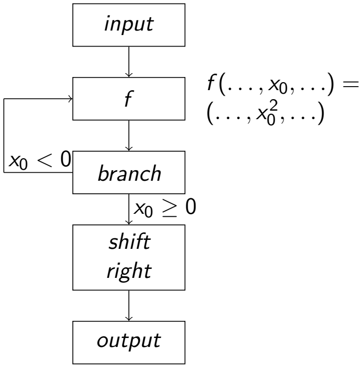
- Goal was to explore the complexity aspects of logics under the semiring semantics.
- There are several descriptive complexity results for algebraic computations using FO and its extensions in the metafinite and weighted logic context (see, e.g., [GM95; Bad+24]).
- We use (a slight extension of) FO to characterize constant-depth arithmetic circuits (as defined before) and NP_K (NP over BSS-machines for K) by a suitable version of existential second-order logic.

Blum Shub Smale Machines

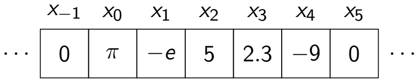


BSS machines / K-machines

- Unbounded tape of K-registers
- Associated graph with node types:
  - Input
  - Output
  - Computation
  - Branch
  - Shift
- $\mathrm{FTIME}_R(f)$: Functions computed in time $\mathcal{O}(f)$

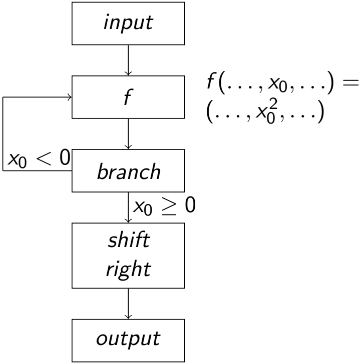


Blum Shub Smale Machines



BSS machines / K-machines

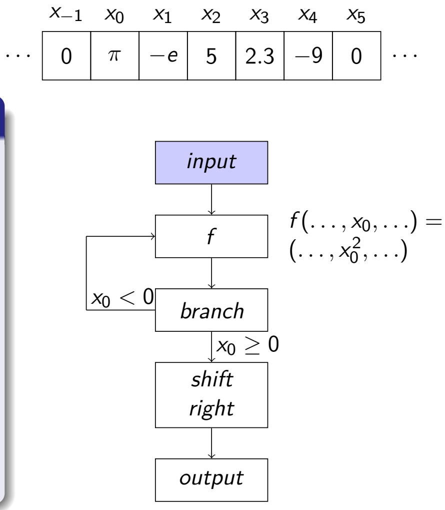
- Unbounded tape of K-registers
- Associated graph with node types:
  - Input
  - Output
  - Computation
  - Branch
  - Shift
- $\mathrm{FTIME}_R(f)$: Functions computed in time $\mathcal{O}(f)$



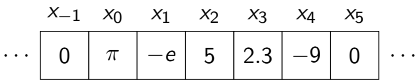
Blum Shub Smale Machines

BSS machines / K-machines

- Unbounded tape of K-registers
- Associated graph with node types:
  - Input
  - Output
  - Computation
  - Branch
  - Shift
- $\mathrm{FTIME}_R(f)$: Functions computed in time $\mathcal{O}(f)$

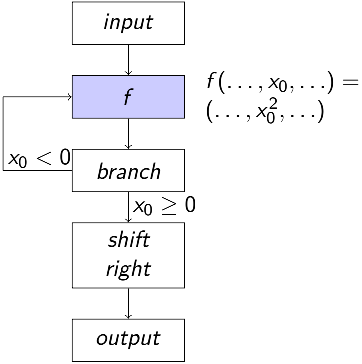


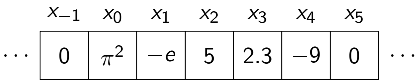
Blum Shub Smale Machines



BSS machines / K-machines

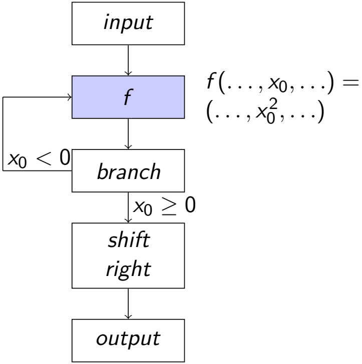
- Unbounded tape of K-registers
- Associated graph with node types:
  - Input
  - Output
  - Computation
  - Branch
  - Shift
- $\mathrm{FTIME}_R(f)$: Functions computed in time $\mathcal{O}(f)$



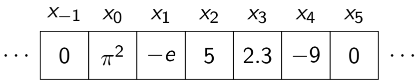


BSS machines / K-machines

- Unbounded tape of K-registers
- Associated graph with node types:
  - Input
  - Output
  - Computation
  - Branch
  - Shift
- $\mathrm{FTIME}_R(f)$: Functions computed in time $\mathcal{O}(f)$

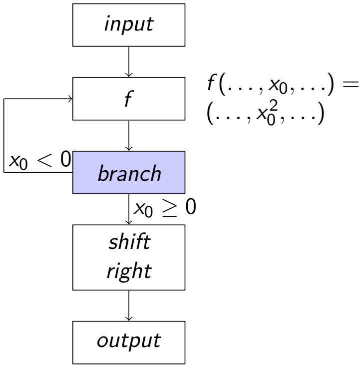


Blum Shub Smale Machines

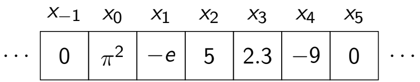


BSS machines / K-machines

- Unbounded tape of K-registers
- Associated graph with node types:
  - Input
  - Output
  - Computation
  - Branch
  - Shift
- $\mathrm{FTIME}_R(f)$: Functions computed in time $\mathcal{O}(f)$

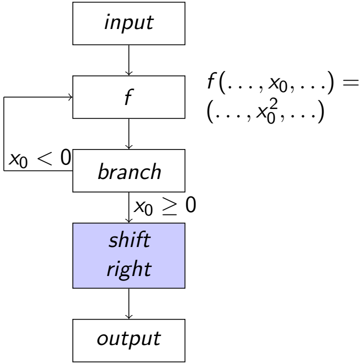


Blum Shub Smale Machines

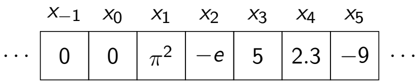


BSS machines / K-machines

- Unbounded tape of K-registers
- Associated graph with node types:
  - Input
  - Output
  - Computation
  - Branch
  - Shift
- $\mathrm{FTIME}_R(f)$: Functions computed in time $\mathcal{O}(f)$

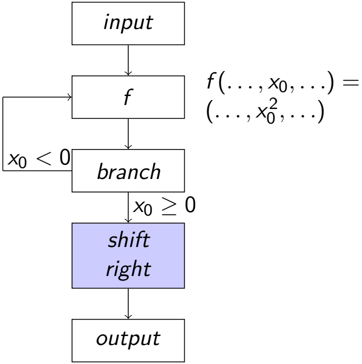


Blum Shub Smale Machines

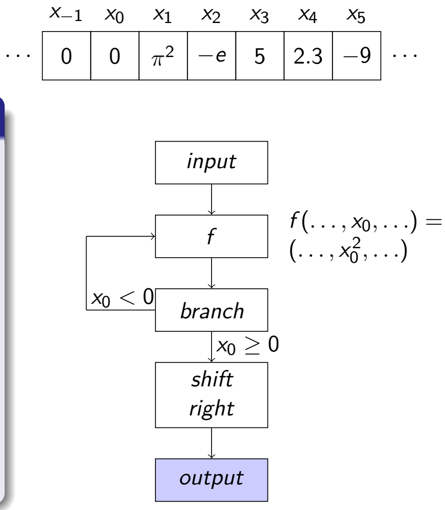


BSS machines / K-machines

- Unbounded tape of K-registers
- Associated graph with node types:
  - Input
  - Output
  - Computation
  - Branch
  - Shift
- $\mathrm{FTIME}_R(f)$: Functions computed in time $\mathcal{O}(f)$



Blum Shub Smale Machines



BSS machines / K-machines

- Unbounded tape of K-registers
- Associated graph with node types:
  - Input
  - Output
  - Computation
  - Branch
  - Shift
- $\mathrm{FTIME}_R(f)$: Functions computed in time $\mathcal{O}(f)$

Our results

First-order logic and arithmetic circuits

We extend FO with the ability to compare the semiring values of subformulas ($\psi = \phi$ and $\psi \leq \phi$ if K is ordered).

Theorem ([Bar+25a])

$$\text{FO} = \mathrm{FAC}^0_K$$

- Here on the circuit side we assume gates for $+$ and $\cdot$ of K and the same binary comparison gates ($=$ and possibly $\leq$) as on the logic side.
- The result is for non-uniform families of circuits so on the logic side we have to allow arbitrary built-in relations.

Our results
NP over BSS-machines

We extend FO with existential quantification (essentially) over K-relations to obtain a variant of ESO.

Theorem ([Bar+25b])

$\mathrm{ESO} = \mathrm{NP}_K$

- Non-determinism for the BSS-machine is done by guessing a polynomial length string of K-values before the start of the deterministic computation.
- We also showed a version of Cook's Theorem and related the Boolean part of NP_K with the existential first-order theory of the semiring K.

Sources I

[Bad+24] Guillermo Badia, Manfred Droste, Carles Noguera, and Erik Paul. “Logical Characterizations of Weighted Complexity Classes”. In: **49th International Symposium on Mathematical Foundations of Computer Science (MFCS 2024)**. Ed. by Rastislav Královič and Antonín Kučera. Vol. 306. Leibniz International Proceedings in Informatics (LIPIcs). Dagstuhl, Germany: Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2024, 14:1–14:16. ISBN: 978-3-95977-335-5. DOI: 10.4230/LIPIcs.MFCS.2024.14. URL: https://drops.dagstuhl.de/entities/document/10.4230/LIPIcs.MFCS.2024.14 (cit. on pp. 29, 30).

Sources II

[Bar+25a] Timon Barlag, Nicolas Fröhlich, Teemu Hankala, Miika Hannula, Minna Hirvonen, Vivian Holzapfel, Juha Kontinen, Arne Meier, and Laura Strieker. "Logic and Computation Through the Lens of Semirings". In: **CoRR** abs/2502.12939 (2025) (cit. on p. 40).

[Bar+25b] Timon Barlag, Nicolas Fröhlich, Teemu Hankala, Miika Hannula, Minna Hirvonen, Vivian Holzapfel, Juha Kontinen, Arne Meier, and Laura Strieker. "Logical Approaches to Non-deterministic Polynomial Time over Semirings". In: **CoRR** abs/2509.26214 (2025) (cit. on p. 41).

[BIS90] D. A. Mix Barrington, N. Immerman, and H. Straubing. "On uniformity within NC^1". In: **Journal of Computer and System Sciences** 41 (1990), pp. 274–306 (cit. on p. 21).

Sources III

[Fag74] Ronald Fagin. "Generalized first-order spectra and polynomial-time recognizable sets". In: **Complexity of computation** 7 (1974), pp. 43–73 (cit. on p. 2).

[GKT07] Todd J. Green, Gregory Karvounarakis, and Val Tannen. "Provenance semirings". In: **Proceedings of the Twenty-Sixth ACM SIGACT-SIGMOD-SIGART Symposium on Principles of Database Systems, June 11-13, 2007, Beijing, China**. Ed. by Leonid Libkin. ACM, 2007, pp. 31–40. DOI: 10.1145/1265530.1265535. URL: https://doi.org/10.1145/1265530.1265535 (cit. on p. 2).

Sources IV

[GM95] Erich Grädel and Klaus Meer. "Descriptive complexity theory over the real numbers". In: **Proceedings of the Twenty-Seventh Annual ACM Symposium on Theory of Computing, 29 May-1 June 1995, Las Vegas, Nevada, USA**. Ed. by Frank Thomson Leighton and Allan Borodin. ACM, 1995, pp. 315–324. DOI: 10.1145/225058.225151. URL: https://doi.org/10.1145/225058.225151 (cit. on p. 30).

[GT17] Erich Grädel and Val Tannen. "Semiring Provenance for First-Order Model Checking". In: **CoRR** abs/1712.01980 (2017) (cit. on p. 29).

Sources V

[HKL25] Lauri Hella, Juha Kontinen, and Kerkko Luosto. "Regular Representations of Uniform TC0". In: **ACM Trans. Comput. Logic** 26.4 (Sept. 2025). ISSN: 1529-3785. DOI: 10.1145/3750044. URL: https://doi.org/10.1145/3750044 (cit. on pp. 24, 25).

[Luo04] Kerkko Luosto. "Equicardinality on Linear Orders". In: **Proc. 19th IEEE Symp. on Logic in Computer Science**. Turku, Finland, 2004, pp. 458–465 (cit. on p. 22).