Affine automata verifiers

ALIYA KHADIEVA, University of Latvia, Latvia and Kazan Federal University, Russia
ABUZER YAKARYILMAZ, University of Latvia, Latvia

We initiate the study of the verification power of Affine finite automata (AfA) as a part of Arthur-Merlin (AM) proof systems. We show that every unary language is verified by a real-valued AfA verifier. Then, we focus on the verifiers restricted to have only integer-valued or rational-valued transitions. We observe that rational-valued verifiers can be simulated by integer-valued verifiers, and their protocols can be simulated in nondeterministic polynomial time. We show that this bound is tight by presenting an AfA verifier for NP-complete problem SUBSETSUM. We also show that AfAs can verify certain non-affine and non-stochastic unary languages.

CCS Concepts: • **Theory of computation → Formal languages and automata theory**.

Additional Key Words and Phrases: affine automata, interactive proof systems , Arthur-Merlin games, unary languages, subset-sum problem, NP.

ACM Reference Format:
Aliya Khadieva and Abuzer Yakaryılmaz. 2021. Affine automata verifiers. In *8th ACM Celebration of Women in Computing: womENcourage 2021, 22–24 September, 2021, Prague, Czech Republic.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

Affine finite automata (AfAs) are quantum-like generalization of probabilistic finite automata (PFAs) mimicking quantum interference and having the capability of "making measurement" based on ℓ_1-norm (called weighting). The computation of an AfA is linear, but the weighting operators may be non-linear.

AfAs was formally defined in [3], and it was shown that they are more powerful than PFAs and quantum finite automata (QFAs) in bounded error and unbounded error settings, but their nondeterministic version is equivalent to nondeterministic QFAs. Since then, AfAs and their different generalizations (e.g., OBDDs and using counters) have been investigated in a series of work [4–6].

We consider AfAs as part of Arthur-Merlin (AM) proof systems and investigate their verification power. We show that every unary language can be verified by a real-valued AfA verifier. Then, we focus on the verifiers with integer-valued or rational-valued transitions. We show how to simulate rational-valued verifiers by integer-valued ones and how to simulate their protocols in nondeterministic polynomial time. We present an AfA verifier for NP-complete problem SUBSETSUM. We also show that AfAs can verify certain non-affine and non-stochastic unary languages. In our protocols, we use similar verification strategies and encoding techniques previously used for two-way QFAs in [7, 8].

We define AM(AfA) as the class of languages verifiable by bounded-error Arthur-Merlin system having realtime affine finite verifiers. In [2], Arthur-Merlin systems with probabilistic finite automata verifier is defined as an automata having both nondeterministic and probabilistic states. We follow the same framework here. We indeed give the ability of making nondeterministic transitions to the model of a finite automaton with classical and affine states.

Manuscript submitted to ACM

The list of standard complexity classes mentioned in the paper:

REG	:	regular languages
L	:	logarithmic space
P	:	polynomial time
NP	:	nondeterministic polynomial time
SPACE(n)	:	linear space
PSPACE	:	polynomial space
NEXP	:	nondeterministic exponential space
ALL	:	all languages

On unary languages, for the real-valued verifiers, we show that AfAs and 2QCFAs have the same verification power, where 2QCFA is the two-way QFA model defined in [1]:

UALL = UAM(2QCFA) = UAM(AfA), where AfAs are realtime machines but 2QCFAs run in exponential expected time.

On unary languages, for the rational-valued verifiers, we know that

$$\mathsf{UREG} = \mathsf{UAM}_{\mathbb{Q}}(\mathsf{PFA}) \subseteq \begin{array}{l} \mathsf{UAM}_{\mathbb{Q}}(\mathsf{QFA}) \subseteq \mathsf{UAM}(\mathsf{QFA}) \\ \mathsf{UAM}_{\mathbb{Q}}(\mathsf{2PFA}) \subseteq \mathsf{UAM}(\mathsf{2PFA}) \end{array},$$

where it is open whether the inclusions are strict, and we show that $\mathsf{UPOLY(P)} \in \mathsf{UAM}_{\mathbb{Q}}(\mathsf{AfA})$ and so we have $\mathsf{UREG} \subsetneq \mathsf{UAM}_{\mathbb{Q}}(\mathsf{AfA})$.

On non-unary languages, for the rational-valued verifiers, we give an upper bound for $\mathsf{AM}_{\mathbb{Q}}(\mathsf{AfA})$, and so we have

$$\mathsf{AM}_{\mathbb{Q}}(\mathsf{AfA}) = \mathsf{AM}_{\mathbb{Z}}(\mathsf{AfA}) \subseteq \mathsf{NP} \cap \mathsf{SPACE}(n) \subsetneq \mathsf{AM}_{\mathbb{Q}}(\mathsf{2QCFA}),$$

where 2QCFAs run in double-exponential expected time. Our bound is tight since we show that $\mathsf{SUBSETSUM} \in \mathsf{AM}_{\mathbb{Z}}(\mathsf{AfA})$.

ACKNOWLEDGMENTS

Yakaryılmaz was partially supported by the ERDF project Nr. 1.1.1.5/19/A/005 “Quantum computers with constant memory”. A part of research is funded by the subsidy allocated to Kazan Federal University for the state assignment in the sphere of scientific activities, project No. 0671-2020-0065.

REFERENCES

[1] A.Ambainis and J. Watrous. 2002. Two–way finite automata with quantum and classical states. *Theoretical Computer Science* 287, 1 (2002), 299–311.

[2] Anne Condon, Lisa Hellerstein, Samuel Pottle, and Avi Wigderson. 1998. On the Power of Finite Automata with Both Nondeterministic and Probabilistic States. *SIAM J. Comput.* 27, 3 (1998), 739–762.

[3] A. Díaz-Caro and A. Yakaryılmaz. 2016. Affine computation and affine automaton. In *Computer Science — Theory and Applications (LNCS, Vol. 9691)*. Springer, 1–15. arXiv:1602.04732.

[4] Mika Hirvensalo, Etienne Moutot, and Abuzer Yakaryılmaz. 2017. On the Computational Power of Affine Automata. In *Language and Automata Theory and Applications (LNCS, Vol. 10168)*. Springer, 405–417.

[5] Marcos Villagra and Abuzer Yakaryılmaz. 2016. Language recognition power and succintness of affine automata. In *Unconventional Computation and Natural Computation (LNCS, Vol. 9726)*. Springer, 116–129.

[6] Marcos Villagra and Abuzer Yakaryılmaz. 2018. Language recognition power and succinctness of affine automata. *Natural Computing* 17, 2 (2018), 283–293.

[7] Abuzer Yakaryılmaz. 2013. Public qubits versus private coins. In *The Proceedings of Workshop on Quantum and Classical Complexity*. Univeristy of Latvia Press, 45–60. ECCC:TR12-130.

[8] Abuzer Yakaryılmaz and A. C. Cem Say. 2010. Succinctness of two-way probabilistic and quantum finite automata. *Discrete Mathematics and Theoretical Computer Science* 12, 2 (2010), 19–40.