

Languages given by Finite Automata over the Unary Alphabet

Gordon Hoi¹, Sanjay Jain², Frank Stephan^{2,3} and Christopher Tan³

- 1 School of Informatics and IT, Temasek Polytechnic, 21 Tampines Ave 1, Singapore 529757, Republic of Singapore, hoickg@gmail.com.
- 2 School of Computing, National University of Singapore, 13 Computing Drive, Block COM1, Singapore 117417, Republic of Singapore, sanjay@comp.nus.edu.sg; S. Jain was supported in part by the Singapore Ministry of Education Academic Research Fund Tier 2 grant MOE2019-T2-2-121 / R146-000-304-112 as well as NUS Provost Chair grant C252-000-087-001.
- 3 Department of Mathematics, National University of Singapore, 10 Lower Kent Ridge Road, Block S17, Singapore 119076, Republic of Singapore, fstephan@comp.nus.edu.sg and e0774066@u.nus.edu; F. Stephan was supported in part by the Singapore Ministry of Education Academic Research Fund Tier 2 grant MOE2019-T2-2-121 / R146-000-304-112.

Abstract

This paper studies the complexity of operations with finite automata and the complexity of their decision problems when the alphabet is unary.

(1) This paper improves the upper bound of the equality problem of unary nondeterministic automata from an exponential in the second root to an exponential in the third root of the number of states. This almost matches a known lower bound based on the exponential time hypothesis by Fernau and Krebs.

(2) It is established that the standard regular operations of union, intersection, complementation and Kleene star cause either only a polynomial or a quasipolynomial blow-up. Concatenation of two n -state ufas, in worst case, causes a blow-up from n to a function with an exponent of sixth root of n . Decision problems of finite formulas using regular operations and comparing languages given by n -state unambiguous automata, in worst case, require an exponential-type of time under the Exponential Time hypothesis and this complexity goes down to quasipolynomial time in the case that the concatenation of languages is not used in the formula. Merely comparing two languages given by n -state ufas in Chrobak Normal Form is in LOGSPACE.

(3) Starting from this research, membership of the infinite word given by a unary alphabet language in a fixed regular language of infinite words is shown to be as difficult as constructing the dfa of that language from the given automaton.

Keywords and phrases Nondeterministic and Unambiguous Finite Automata; Unary Alphabet; Universality Problem; Regular Operations with Languages; Automata Sizes; Computational Complexity of Operations; Membership in Regular ω -languages

1 Introduction

This paper investigates the complexity and size-constraints related to languages over the unary alphabet – this is assumed everywhere throughout the paper – when these languages are given by a nondeterministic finite automaton with a special emphasis on the case where this nfa is unambiguous; unambiguous nondeterministic finite automata (ufas) have many good algorithmic properties, even under regular operations with the languages, as long as no concatenation is involved. Here a bound of type $2^{\Theta(n)}$ is called exponential and a bound

of type $2^{n^{\Theta(1)}}$ is called exponential-type. If p is a non-constant polynomial in logarithms and iterated logarithms, then the class of bounds of the form $n^{\Theta(p(\log n, \log \log n, \log \log \log n, \dots))}$ for any p as above is called quasipolynomial. In an expression of the form $2^{\alpha(n)}$, the function $\alpha(n)$ is called the exponent of the function. Note that, under the Exponential Time Hypothesis, all NP-complete problems have an exponential-type complexity and solving k SAT for $k \geq 3$ has an exponential complexity. For several important cases, the exponential of an exponential-type function is determined up to a logarithmic or sublogarithmic expression in the exponent.

Unambiguous finite automata found much attention in recent research with a **lower quasipolynomial lower bound for the blow-up of the size at complementation by Raskin at ICALP 2018** and a better lower bound for complementation of form $n^{\Omega(\log n)}$ for the case of the binary alphabet (results on larger alphabets are only mentioned for comparison purposes) by Göös, Kiefer and Yuan [7].

Fernau and Krebs [6] proved that under the assumption of the Exponential Time Hypothesis (ETH), one needs at least $2^{\Omega(n^{1/3})}$ time to check whether an nfa with n states over the unary alphabet accepts all strings; they coded three-colourability of graphs for this problem. Tan [17] provides an alternative proof using a coding of three-occurences 3SAT; the ETH implies that one cannot solve this problem in $2^{o(m)}$ time where m is the number of variables. This is a special case of comparing languages and Fernau and Krebs [6] pointed to the $n^{O(n^{1/2})}$ algorithm which converts unary nfes into dfes to compare two unary nfes of up to n states. The present work provides a faster algorithm for this task and the exponent of the computation time of this algorithm matches the exponent of the lower bound of Fernau and Krebs up to a factor $O((\log n)^{1/3})$.

Recall that for an unambiguous nondeterministic finite automata (ufa), every word outside the language has zero accepting runs and every word inside the language has exactly one accepting run. Prior research had established that the intersection of two n -state ufes can be represented by an $O(n^2)$ ufa and that, over the binary alphabet, the complexity of the Kleene star of an n -state ufa can be recognised by an $O(n^2)$ ufa [5, 9, 13, 15]. But the size-increase of the other regular operations (complement, union, concatenation) remained open; it was however known that disjoint union has linear complexity. The present work shows that complementation has at most the quasipolynomial size blow-up $n^{\log n + O(1)}$ and thus the same holds for the union; furthermore, the concatenation is much worse and requires exponential-type size-increase where the exponent is at least $\Omega(n^{1/6})$. Raskin's [16] showed a lower bound $(n^{\log \log \log n})^{\Omega(1)}$ for unary complementation and thus the quasipolynomial upper bound cannot be improved to polynomial.

Furthermore, it is not efficient to compare ufes with respect to inclusion of the generated languages by constructing complementation of the second automaton and then taking intersection and checking for emptiness. This is due to a further result shows that one can directly compare n -state ufes with respect to equality or inclusion in polynomial time. If the ufes are in Chrobak Normal Form, the comparison can even be carried out in LOGSPACE - the transformation into this normal form is a polynomial time algorithm which does not increase the number of states for ufes.

Finally algorithmic properties with respect to the ω -word $L(0)L(1)L(2)\dots$ of a language L where $L(k)$ is 1 if the word of length k is in the language L and $L(k)$ is 0 if this word is not in the language L are investigated. If L is given by a dfa, membership tests for a fixed regular ω -language can be decided in polynomial time; for ufes and nfes there is a known trivial upper bound obtained by converting these automata into nfes; this upper bound has, up to logarithmic factors, the exponent $n^{1/2}$ for nfes and $n^{1/3}$ for ufes. The result of the

present work is that these upper bounds can be matched by conditional lower bounds up to a logarithmic factor of the exponent assuming the exponential time hypothesis.

The following table summarises the results for ufas and compares to previously known results. Here $c(n) = n^{\log n + O(1)}$ and results with a theorem plus number are proven in the present work. Lower bounds on size imply lower bounds on Computations; for concatenation a better lower bound is found (assuming ETH). In the first part of the table the bounds on the size are given and in the second part the bounds on the computation time for finding ufas with the desired property or determining the truth of a formula. The third part of the table summarises the results of the other parts of the paper. Here ufa-word and nfa-word are the ω -words defined when viewing the characteristic function of the recognised language as an ω -word.

Operation	Lower Bound	Source	Upper Bound	Source
Intersection	$n^2 - n$	Holzer and Kultrib [8]	n^2	Holzer and Kultrib [8]
Complement	$n^{(\log \log \log n)^{\Omega(1)}}$	Raskin [16]	$c(n)$	Theorem 2
Disjoint union	$2n - 4$	–	$2n$	Jirásková and Okhotin [13]
Union	–	–	$n + n \cdot c(n)$	Corollary 9
Symmetric difference	–	–	$2n \cdot c(n)$	Theorem 2
Kleene Star	$(n - 1)^2 + 1$	Čevorová [3]	$(n - 1)^2 + 1$	Čevorová [3]
Concatenation	$2^{\Omega(n^{1/6})}$	Theorem 7	$2^{O((n \log^2 n)^{1/3})}$	Okhotin [14]
Finite Formula	$\text{ETH} \Rightarrow 2^{\Omega(n^{1/3})}$	Theorem 11	$2^{O((n \log^2 n)^{1/3})}$	Okhotin [14]
Space for Universality	–	–	$O(\log n)$	Theorem 4
Time for Universality (both for Chrobak NF)	–	–	$O(n \log^2 n)$	Theorem 4
Time for Comparison	–	–	Polynomial Time	Corollary 5
Time for Concatenation	$\text{ETH} \Rightarrow 2^{\Omega(n^{1/4})}$	Theorem 12	$2^{O((n \log^2 n)^{1/3})}$	Okhotin [14]
Time for Complement	$n^{(\log \log \log n)^{\Omega(1)}}$	Raskin [16]	$n^{O(\log n)}$	Theorem 2
Time for Formulas	$\text{ETH} \Rightarrow 2^{\Omega(n^{1/3})}$	Theorem 11	$2^{O((n \log^2 n)^{1/3})}$	Okhotin [14]
Time for Formulas Without Concatenation	quasipolynomial	Raskin [16]	quasipolynomial	Remark 6
Time for nfa Comparison	$2^{\Omega(n^{1/3})}$	Krebs and Fernau [6]	$2^{O((n \log n)^{1/3})}$	Theorem 1
Nfa-word in ω -language	$2^{\Omega((n \log \log n / \log n)^{1/2})}$	Theorem 14	$2^{O((n \log n)^{1/2})}$	dfa-conversion
Ufa-word in ω -language	$2^{\Omega((n \log n)^{1/3})}$	Remark 16	$2^{O((n \log^2 n)^{1/3})}$	dfa-conversion

2 The Nondeterministic Finite Automata Comparison Algorithm

The upper bound of the next result matches the lower bound $2^{\Omega(n^{1/3})}$ of the timebound from the universality problem of unary nfes given by Fernau and Krebs [6] up to a factor $O((\log n)^{1/3})$ when comparing the logarithms of the run time corresponding bounds. Here the universality problem is the problem to check whether the finite automaton generates all the words over the given alphabet (which is unary in this paper).

► **Theorem 1.** *Given two nondeterministic finite automata over the unary alphabet and letting n denote the maximum number of their states, one can decide whether the first nfa*

computes a subset of the second nfa in deterministic time $O(c^{(n \log n)^{1/3}})$ for a suitable constant $c > 1$. This timebound also applies directly to the comparison algorithm for equality and the algorithm for checking universality (all strings in the language).

Proof. Let n denote the maximum number of states of the two automata. One can transform the nondeterministic finite automata into Chrobak Normal Form [4] where it consists of a “stem” of up to n^2 states followed by parallel cycles which, together, use up to n states. Note that one can assume that the two stems have the same length, as each stem can be made one longer by moving the entry point into each cycle by one state and adding one state at the end of the stem which is accepting iff one of the nodes at the prior entry points was accepting; this is done repeatedly until the stems have the same length, at most $O(n^2)$ times. The comparison of the behaviour on the stems of equal length before entering the cycles can just be done by comparing the acceptance mode of the states of the same distance from the start.

For comparing two nfes in such a normal form, the comparison of the cycle part is therefore the difficult part. For the following, one ignores the stems and considers the special case where the nfa just consists of disjoint cycles, each of them having one start state and the only nondeterminism is the choice of the start state, that is, the cycle to be used.

So assume that such cycles are given. Now let P be the set of all primes p below n such that either (a) $p < (n \log n)^{1/3}$ or (b) the condition (a) fails and there is a further prime $q \geq (n \log n)^{1/3}$ for which some cycle in one of the two nfes has a length divisible by $p \cdot q$. By the prime number theorem, those primes entering P by condition (a) are at most $O((n/\log^2 n)^{1/3})$ many and those entering by condition (b) obey the same bound, as there can be at most $2(n/\log^2 n)^{1/3}$ cycles having at least the length $(n \log n)^{2/3}$ in the two automata — this bound follows from the fact that the product of two primes not obeying condition (a) is at least the length $(n \log n)^{2/3}$ and that all cycles in each automaton are disjoint and the number of cycles of such a length in each automaton can therefore not be larger than $n/(n \log n)^{2/3}$. Let Q be the set of all primes up to n which are not in P . Let r be the product of all primes $p \in P$ raised to the largest power k such that $p^k \leq n$. The number r is in $O(n^{c' \cdot (n/\log^2 n)^{1/3}})$ for some c' and thus $2^{c' \cdot (n \log n)^{1/3}}$ when replacing n by $2^{\log n}$ and applying a simple mathematical rearrangement. This expression is equal to $c^{(n \log n)^{1/3}}$ for some $c > 1$.

Now one constructs for the two given nfes the comparison normal forms of size $r \cdot n$ as follows:

For each $q \in Q$ one constructs a cycle of length $r \cdot q^2$ such that the state s in this cycle is accepting iff there is a cycle of length p in the original automaton where p divides $r \cdot q^2$ and when going in that cycle s steps (or just $s \bmod p$ steps) the corresponding state is accepting. The comparison normal form can be constructed in time $r \cdot \text{Poly}(n)$ time by constructing each cycle separately in both automata and compare it with all cycles of length p where p divides $r \cdot q^2$.

Now the first automaton recognises a subset of the set recognised by the second automaton iff for all $s < r$ one of the following two options holds:

(A) There is a $q \in Q$ such that in the second normalised automaton, all states of the form $s + t \cdot r$ in the cycle of length $r \cdot q^2$ are accepting;

(B) For every $q \in Q$ and for all states of the form $s + t \cdot r$, if this state in the cycle of length $r \cdot q^2$ is accepting in the normalised form of the first automaton then it is also accepting in the corresponding cycle of the normalised form of the second automaton.

This condition can be checked in time $r \cdot \text{Poly}(n)$: There are r possible values of s and for each such s , one has to check only $O(n^3)$ states, namely for each $q \in Q$ all states of the

form $s + t \cdot r$ where $t \in \{0, 1, \dots, q^2 - 1\}$; note that $q^2 \leq n^2$.

For correctness, one first shows that (A) and (B) are sufficient conditions. Let s be given. If (A) is satisfied, then the second automaton accepts all strings of length $s + t \cdot r$ whatever t is, as for the given q , all these strings are accepted by the cycle of length $r \cdot q^2$ when looking at states reached from the origin in $s + t \cdot r$ steps.

If (B) is satisfied and the first nfa accepts after $s + t \cdot r$ steps then there is a $q \in Q$ such that the cycle of length $r \cdot q^2$ has an accepting state at position $s + t \cdot r$ (modulo $r \cdot q^2$). From the condition it followed that the second automaton has an accepting state at the same position in the corresponding cycle and therefore also accepts the corresponding string.

One still needs also to see the converse. So assume that the following condition (C) holds: For every $q \in Q$ there exists a t_q such that the state at position $s + t_q \cdot r$ is rejecting in the cycle of length $r \cdot q^2$ in the second automaton and furthermore, for one q , the state at position $s + t_q \cdot r$ is accepting in the cycle of length $r \cdot q^2$ in the first automaton. So (C) is true iff both (A) and (B) fail. Now there is a step number s' such that, after going each cycle s' steps, the cycle is at position $s + t_q \cdot r$ for the cycle of length $r \cdot q^2$ for each $q \in Q$. It follows that the first automaton accepts a string of length s' while the second automaton rejects it. \blacktriangleleft

Holzer and Kutrib [9, Theorem 15] write that for every n -state nfa there is an equivalent $O((n \log n)^{1/2})$ state afa (alternating finite automaton) recognising the same language; in the case that this translation is efficient, the conditional lower bound of Fernau and Krebs [6] of $2^{\Omega(n^{1/3})}$ for deciding universality or equivalence of n -state nfes using a unary alphabet would translate into a $2^{\Omega((n/\log n)^{2/3})}$ lower bound for the same task for afas using a unary alphabet.

3 Unambiguous Finite Automata and their Algorithmic Properties

An unambiguous automaton (ufa) satisfies that for every input word, there is either exactly one accepting run or none. On one hand, these are more complicated to handle than non-deterministic finite automata so that the union of n n -state automata cannot be done with n^2 states; on the other hand, they still, at least for unary alphabets, have good algorithmic properties with respect to regular operations (union, intersection, complementation, formation of Kleene star) and comparison (subset and equality).

It is well known that, for the unary alphabet, the intersection of two ufes can be carried out by the usual product construction for nfes, as that construction preserves the property to be an ufa in the case that both input automata are an ufa, thus the size increase is $O(n^2)$ for forming the intersection of two n -state ufes.

Göös, Kiefer and Yuan [7] showed that there is a family of languages L_n over the binary alphabet recognised by an n -state ufa such that the size of the smallest nfes recognising the complement grows at least with $n^{\Omega((\log n)/\text{polylog}(\log n))}$. This lower bound also trivially applies to ufes. For complementation of ufes over the unary alphabet, a smaller bound might be possible: So far, Raskin [16] showed that the complementation of a unary ufa increases the states from n to some superpolynomial function in the worst case; this result is based on a lower bound of the form $n^{(\log \log \log n)^q}$ where q is some positive rational constant. Thus it is impossible to carry out the complementation with polynomial size-increase; however, the next results shows that one can do this with quasipolynomial size-increase.

This confirms a weak version of a conjecture of Colcombet [5] that complementation of ufes can be done with a polynomial blow-up. Though Raskin results refutes that, when replacing “polynomial” by “quasipolynomial” the conjecture would hold in the unary case.

For larger alphabets, the lower bounds are below the upper bounds given here, but the construction does not seem to generalise to larger alphabets, as it utilises quite some facts which only hold for unary ufas. The theorem is first stated for the case of a periodic ufa, as there the proof is clearer, afterwards it is indicated how to obtain it for the general case.

► **Theorem 2.** *A ufa with up to n states has a complement with $n^{\log(n)+O(1)}$ states which can be computed in quasipolynomial time from the original automaton.*

The proof will use the following straight-forward lemma.

► **Lemma 3.** *Consider a ufa in Chrobak Normal Form (consisting only of cycles without the stem part).*

(a) *Suppose a cycle with states s_0, s_1, \dots, s_{p-1} (with the transition from s_i to s_{i+1} on the unary input, where $i+1$ is taken mod p), is converted to a cycle with states $s'_0, s'_1, \dots, s'_{k \cdot p - 1}$, (with the transition from s'_i to s'_{i+1} on the unary input, where $i+1$ is taken mod $p \cdot k$), with $s'_{r+p \cdot c}$, for $c < p$, being an accepting state iff s_r is an accepting state in the original cycle. Then the new automaton is still a ufa accepting the same set of strings.*

(b) *Consider a cycle with states s_0, s_1, \dots, s_{p-1} , and (with the transition from s_i to s_{i+1} on the unary input, where $i+1$ is taken mod p).*

Suppose one converts the cycles into q cycles, with the j -th cycle ($j < q$) having states s_i^j , $i < p$, where s_i is not accepting then none of s_i^j is accepting, and if s_i is accepting then exactly one of s_i^j , $j < q$ is accepting. Then the new automaton is still a ufa and accepts the same set of strings as the original automaton.

(c) *Converse of (b) above: that is, two cycles with same number of states can be combined into one cycle.*

(d) *If a cycle with no accepting states is removed, it does not change the language accepted by the ufa.*

Proof. Jiang, McDowell and Ravikumar [11] – see also [14] – proved that one can transform, in polynomial time, an ufa over the unary alphabet into an ufa in Chrobak normal form without a size-increase, so the new ufa has still n states. Note that for the complement of an ufa in Chrobak Normal Form, one swaps acceptance / rejection for the states on the stem and then, for the parallel cycles, they form a periodic ufa concatenated to a single string language. Thus complementing the periodic ufa is the main work and it is assumed, without loss of generality, that the stem does not exist, so every cycle has some start state and the only amount of non-determinism is the choice of the start state. For each input word, there is exactly one cycle which goes either into an accept or reject state while all other cycles are into a state which does not signal any decision; swapping accept and reject states then allows to complement the so obtained ufa.

For ease of notation, in a cycle with p states s_0, s_1, \dots, s_{p-1} (with the transition from s_i to s_{i+1} on the unary input, where $i+1$ is taken mod p), one can call the state s_i , the i -th state of the cycle (with 0-th state being the starting state of the cycle).

Intuitively, the original ufa will be transformed into a new ufa using Lemma 3. The new ufa will have some blue states (denoting the accepting states for the language accepted by the original ufa) and some states green (denoting the accepting states for the complement of the language accepted by the original ufa). The blue states will only be formed by considering the accepting states of the original automaton, or due to the transformations as done by Lemma 3. The green states will be introduced during this construction when it is safe to do so (that is, whenever the automaton reaches that state after processing a unary string, the string will be in the complement of the language). Thus, it will always be the case (after a

modification step) that the blue/green states being considered as accepting states keeps the automaton as a ufa, with blue nodes accepting exactly the original language accepted by the ufa and the green nodes accepting a subset of the complement. The final ufa will have the green states accepting exactly the complement.

It is convenient to view the progress in the construction as a tree. At any step, the leaves of the tree represent cycles of the automaton, and the current automaton is the union of cycles at the leaves. A modification may be done during the construction by introducing children to some leaves based on Lemma 3 and converting some states into green.

Each leaf is associated with some cycles of the ufa as mentioned above along with the parameters (p, r, A) , where p is a number, $r < p$, and A is a set of numbers $\{q_1, q_2, \dots, q_m\}$, such that there are m cycles associated with the leaf have lengths $p \cdot q_i$ respectively.

The following invariants will be satisfied:

- (I1) For a leaf L with parameters (p, r, A) : only $(r + p \cdot c)$ -th states, for some c , in the cycles associated with leaf L can be of colour blue (accepting) or green (accepting for the complement).
- (I2) For two distinct leaves with parameters (p, r, A) and (p', r', A') , there can be no natural numbers ℓ with the property that $\ell \bmod p = r$ and $\ell \bmod p' = r'$.

Thus, in short, the different leaves are “independent” automata: if at the end of a string a blue/green state is reached in a cycle of one leaf then blue/green state cannot be reached at the end of the same string in a cycle of another different leaf.

- (I3) Furthermore, for every number ℓ there will be a leaf with parameters (p, r, A) such that $\ell \bmod p = r$.

At the start of the construction, the tree has only one node, with parameters $(1, 0, A)$, where A contains the lengths of all the cycles in the original ufa, and the cycles associated with the node are all the cycles in the original ufa.

At any stage, one modifies a leaf L with parameters (p, r, A) in the tree using the following steps:

1. Merge any cycles with same length at the leaf L (along with updating parameter A correspondingly). This is fine by Lemma 3(c), and preserves the invariants.
2. If there are no blue or green nodes in a cycle associated with the leaf L , then delete that cycle (if this leaves no cycles associated with the leaf L , then introduce a cycle of size p , with no blue/green states), along with updating parameter A correspondingly.
3. If leaf L now has only one associated cycle, then for the parameter (p, r, \cdot) associated with the leaf L , if $(r + p \cdot c)$ -th node of the cycle (for any c) is not coloured, then it is coloured green. Note that this is safe based on invariant (I2). This node will not have any children in the future.
4. If there are still more than one cycles associated with the leaf L , then suppose $A = \{q_1, q_2, \dots, q_m\}$. Note that by the automaton being a ufa, and each of the cycles having at least one blue state, it follows using (I1) that each pair of numbers in A have gcd greater than 1 (thus in particular each $q_i > 1$).
 - a. Now convert the cycles of length $p \cdot q_i$, $i > 1$ associated with the leaf to a cycle of length $p \cdot q_1 \cdot q_i / \gcd(q_1, q_i)$ based on Lemma 3(a), and update A correspondingly.
 - b. Make q_1 children of the node, with parameters $(p \cdot q_1, r + j \cdot p, A)$, with $j < q_1$. Cycles associated with the new children are defined as follows:
Each cycle C of length $p \cdot q_1 \cdot s$ associated with L is converted into q_1 cycles of length $p \cdot q_1 \cdot s$ where the j -th cycle (with $j < q_1$) has the i -th state blue/green iff i -th state of C is blue/green and $i \bmod (p \cdot q_1) = r + j \cdot p$. Otherwise the state is uncoloured.

This j -th cycle is associated with the child with parameter $(p \cdot q_1, r + j \cdot p, A)$. The parameter A is appropriately computed for each child based on the children associated with it.

Based on Lemma 3 (b), the above transformation preserves the properties/invariants.

Note that all the above steps do not change the invariants, and keep the new automaton still an nfa accepting (using blue states) the same set of strings as the earlier automaton. If green state is introduced, then it is consistent due to invariant (I2).

Now, note that after steps 4.1 and 4.2 are executed, the values in A (before step 4.1) are divided by at least 2 each (by $\gcd(q_1, q_i)$ for the number corresponding to old q_i). Thus, the number of levels in the tree can be at most $\log n$, where n is the length of the longest cycle at the beginning.

It follows that the parameter p associated with any leaf can be at most $n \cdot \frac{n}{2} \cdot \frac{n}{4} \dots$, which is bounded by $n^{0.5 \log n + O(1)}$.

The computation time at each node is polynomial in the size of the cycles and n .

Thus, the whole computation takes time $O(n^{O(\log n)})$. There are at most $n^{0.5 \log n + O(1)}$ cycles of length up to $n^{0.5 \log n + O(1)}$, as for each length, the cycles could be combined. Thus the overall number of states is at most $n^{\log n + O(1)}$, the upper bound is just the square of the length of the longest cycle.

As each step of the algorithm preserves the invariants and the changes in the cycles are done only based on Lemma 3, it follows that the final automaton is an ufa with respect to either blue or green states being accepting. Blue accepting states preserve the language accepted by the original automaton. Green accepting states are introduced only in step 3, in which case clearly green states are consistent with accepting strings of the complement of the language. As the eventual leaves can have only one cycle, it follows that each leaf with parameters (p, r, \cdot) decides for all strings of length equivalent to $r \bmod p$. Furthermore, as root covers all lengths and each splitting into children covers the lengths covered by parent, all lengths are covered by some leaf. It follows that the final ufa decides the language. ◀

► **Theorem 4.** (a) *One can decide in LOGSPACE whether an ufa in Chrobak Normal Form accepts all words. Without the LOGSPACE constraint, the running time can be estimated as quasilinear, that is, of the form $O(n \log^2(n))$.*

(b) *Furthermore, one can decide in LOGSPACE whether an nfa U_1 in Chrobak Normal Form accepts a subset of the language accepted by another ufa U_2 in Chrobak Normal Form.*

Proof. (a) First check if the states of the stem are all accepting, which can clearly be done in LOGSPACE by automata walkthrough - pointers needed $O(\log n)$ memory to track positions in the ufa. Then one walks through each cycle and counts the number i_k of accepting states and the length j_k of the cycle. Now the ufa accepts all words, that is, is universal iff $\sum_k i_k / j_k = 1$. We initially show how to do this without being careful about space, but later show how the computation can be modified to be done in LOGSPACE.

As the computation with rational numbers might be prone to rounding, one first normalises to one common denominator, namely $p = \prod_k j_k$ and furthermore computes $s = \sum_k i_k \cdot \prod_{h \neq k} j_h$. Now the above equality $\sum_k i_k / j_k = 1$ holds iff $s = p$.

The values of s and p can be computed iteratively by the following algorithm, note that there are at most n cycles and each time a cycle is processed, the corresponding values i_k and j_k can be established by an automata walk-through.

So the loop is as follows:

1. Initialise $s = 0$ and $p = 1$;

2. For each k do begin find i_k and j_k ; update $s = (s \cdot j_k) + i_k \cdot p$; $p = p \cdot j_k$ endfor;
3. if $s = p$ then accept else reject.

In this algorithm, only the variables p and s need more space than $O(\log n)$; the other variables are all pointers or numbers between 0 and n which can be stored in $O(\log n)$ space.

The values of s and p are at most $n^{2(n^{1/2})}$, as there are, when one assumes that lengths of cycles in Chrobak normal form are different, at most $2n^{1/2}$ cycles, as the sum of their lengths is at most n and half of them are larger than $n^{1/2}$. Thus, instead of computing the above algorithm once with exact numbers, one computes in time $O(n \log n)$ the first $5 \cdot n^{1/2} + 2$ primes out of which 80% are above $n^{1/2}$ so that their product is above the maximum values s and p can take — note that this part has even the better bound $O((n^{1/2} \log^8(n)))$, if one uses the algorithm of Agrawal, Kayal and Saxena [1, 12] for the primality test; the bound includes that the primes to be found are all bounded by a constant times $n^{1/2} \log n$, using the prime number theorem. As their product is larger than the upper bound $n^{1+2(n^{1/2})}$ of s and p , one then accepts iff all computations modulo each such prime q result in $s = p$ modulo q ; this condition is, by the Chinese remainder theorem, equivalent to $s = p$ without taking any remainders. So the modified algorithm would be this.

1. Let $q = 2$; $\ell = 1$;
2. Initialise $s = 0$ and $p = 1$ (both are kept modulo q)
3. For each k do begin find i_k and j_k by transversal of the corresponding cycle; update (both computations modulo q) $s = (s \cdot j_k) + (i_k \cdot p)$; $p = p \cdot j_k$ endfor;
4. if $s \neq p$ (modulo q) then reject;
5. Let $\ell = \ell + 1$ and replace q by the next prime using a fast primality test and exhaustive search;
6. If $\ell < 5n^{1/2} + 2$ (or an easier to compute upper bound linear in this expression like $2^{0.5 \log n + 4}$ assuming that the binary system is used and $\log n$ is the number of binary digits of n) then goto step 2.

The automata transversal of each of these $O(n^{1/2})$ loops needs at most time $O(n \log n)$ as one transverses each of the cycles of the ufa to determine the corresponding i_k and j_k , the cycles are disjoint and have together at most n states. So the overall running time is $O(n^{3/2} \log n)$. If one would use more space, about $O(n^{1/2} \log n)$, then one can avoid the repeated computation of i_k, j_k by automata walk-throughs and gets the upper bound on the computation time of $O(n \log^2(n))$.

For the space usage, the computations modulo q need only $O(\log q)$ space which is then $O(\log n)$ space, as the first $5n^{1/2} + 2$ primes q and the storage of variables modulo q is all of $O(\log n)$. Primality tests can be done in $O(\log n)$ space for the usual way of doing is – checking all divisors up to the root – or with slightly more space when doing more advanced algorithms.

(b) First note that basically the same idea as in (a) can be used to check if a ufa accepts all unary strings in sets vw^* for some v, w of length up to $2n$ can be done as above with a slight modification of the ufa walk-throughs. For this one partitions the words accepted by U_1 into two groups:

- (i) A finite set X_1 of strings of length at most n (where n is the size of the ufa) and
- (ii) A set X_2 consisting of subsets of the form vw^* , where v, w are unary strings with $n < |v| \leq 2n$ and $|w| \leq n$.

The strings in group (ii) above are from the cycles in U_1 , by considering each accepting state in a cycle separately, and taking $|v|$ as the length of the smallest string leading to the state and $|w|$ as the length of the corresponding cycle.

Strings in group (i) can easily be checked using a walkthrough of U_2 , where if there is a branching into the cycles, one can do a depth first search.

For strings in group (ii), each set of form vw^* , where $n < \text{leg}|v| \leq 2n$ and $|w| \leq n$, is checked separately. As $|v| >$ the length of the stem part of U_2 , one can first modify the cycle part of U_2 to always start in a state which is reached after $|v|$ steps, and ignore the stem part. This would basically mean that we need to check if w^* is accepted in the modified U_2 (denote this modified U_2 as U'_2). For space constraints, note that we do not need to write down U'_2 , but just need to know the length by which the starting state of each cycle is shifted (which is the difference between $|v|$ and the length of the stem part of U_2). Now, for checking whether w^* is accepted by U'_2 , consider a further modified U''_2 formed as follows: for each cycle C in U'_2 with length r and states s_0, s_1, \dots, s_{r-1} (s_0 being starting state, and transitions on unary input being from s_i to s_{i+1} , where $i+1$ is taken mod r) consider a cycle C' in U''_2 with states $s'_0, s'_1, \dots, s'_{r-1}$ (s'_0 being starting state, and transitions on unary input being from s'_i to s'_{i+1} , where $i+1$ is taken mod r) where s'_i is an accepting state iff $s_{|v|+i \cdot |w| \bmod r}$ was an accepting state in C . This new ufa U''_2 also has at most n states, the new length of each cycle is still the same as the lengths of the old cycles and the number of cycles do not increase. Now, similar to part (a), one just needs to check if U''_2 is accepting all unary strings. Here again note that one doesn't need to write down U''_2 fully, but just needs to check, for each cycle, its length and the number of accepting states, which can be done in LOGSPACE. ◀

As converting an ufa into Chrobak Normal Form goes in polynomial time without increasing the size and as logarithmic space computations are in polynomial time, one directly gets the following corollary.

► **Corollary 5.** *One can decide the universality problem and the inclusion problem for two n -state ufes in polynomial time.*

► **Remark 6.** For an ufa (of size n) for a language L over the unary alphabet, the language L^* can be recognised even by a dfa of quadratic size in n [3].

Thus if one allows in regular languages Kleene star, Kleene plus and the Boolean set-theoretic operations (but no concatenation), then the output of constant-size expressions, with parameters being given by languages accepted by n -state ufes, can be recognised by ufes of quasipolynomial size. Furthermore, constant-sized quantifier-free formula with same type of parameters and comparing such subexpressions by $=$, \subseteq and \neq can be evaluated in quasipolynomial time.

► **Theorem 7.** *There is an exponential-type blow-up for ufa sizes when recognising the concatenation of unary languages; the concatenation of two languages given by n -state ufes requires, in the worst case, an ufa with $2^{\Omega(n^{1/6})}$ states.*

Proof. Let m be a numeric parameter and let p_1, \dots, p_k be the first $k = m/\log m$ primes of size at least m ; note that $m > k + 4$ for all sufficiently large m . These primes are within $\Theta(m)$ by the prime number theorem (which says that the h -th prime number is of size $\Theta(h \log h)$). Now the ufa U to be constructed contains k cycles C_ℓ of length $p_\ell \cdot (k + 3)$ for $\ell = 0, 1, \dots, k - 1$ and the cycle C_ℓ has, at positions $\ell + 2 + h \cdot (k + 3)$ for $h = 0, 1, \dots, p_\ell - 2$ an accepting state. There is one further cycle C' of length $k + 3$ which has accepting states at positions $0, 1, k + 2$. Let L denote the language recognised by this ufa. The lengths of k consecutive unary strings not being accepted by the above ufa are exactly at lengths $r \cdot (k + 3) + 2, \dots, r \cdot (k + 3) + k - 1$ where r is $p_\ell - 1$ modulo p_ℓ for $\ell = 0, 1, \dots, k - 1$, and this does not happen at any other lengths. Let H be the finite language which contains the

words of length $0, 1, \dots, k-2$ and no other words. Now $L \cdot H$ contains all words whose length does, for at least one ℓ , not have the remainder $k-1 + (k+3) \cdot (p_\ell - 1)$ modulo $(k+3) \cdot p_\ell$. The complement of $L \cdot H$ is a periodic language which contains exactly those words which have, for all ℓ , the remainder $k-1 + (k+3) \cdot (p_\ell - 1)$ modulo $(k+3) \cdot p_\ell$. So every nfa or ufa recognising this language needs cycles of length at least $(k+3) \cdot p_0 \cdot p_1 \cdot \dots \cdot p_{k-1}$. The length of this cycle is approximately $\Theta(m^k) \cdot (k+3)$ and any nfa or ufa recognising it needs at least the same number of states. Furthermore, the ufa U has n states with $n \in \Theta(m) \cdot \Theta(k^2) = \Theta(m^3 / \log^2 m)$. It follows that $n \cdot \Theta(\log^2(m)) = \Theta(m^3)$ and, using $\Theta(\log n) = \Theta(\log m)$ as n, m are polynomially related, that $\Theta(n \cdot \log^2(n)) = \Theta(m^3)$. So one can estimate $m \in \Theta((n \cdot \log^2 n)^{1/3})$. Now the concatenation of $L \cdot H$ has an ufa of size o to be determined and its complement, by the above, has an ufa of at least size $O(m)^{m/\log m}$. Using that the complement of an ufa of size h can be done in size $h^{\log o + O(1)}$, one has that the logarithm of the corresponding sizes satisfies this: $\log^2 o \geq (\log m + O(1)) \cdot m / \log m \geq m$ and $\log o \geq m^{1/2}$. Now the input ufa is of size n with $m \in \Theta((n \log^2 n)^{1/3})$ and thus one has that $\log o \in \Omega(n^{1/6})$. So the concatenation of languages given by n -state ufes can result in an ufa of size at least $2^{\Omega(n^{1/6})}$. ◀

► **Remark 8.** This result stands in contrast to the situation of nfes. It is well-known that the concatenation of two n -state nfes needs only $2n$ states. However, the above construction shows that forming the complement in the unary nfes then blows up from $2n$ states to $2^{\Omega(n^{1/6})}$ states, giving an exponential-type lower bound for this operation; a direct construction leading to the bound $2^{\Omega((n \log n)^{1/2})}$ is known [14]. Furthermore, Čeverova [3] showed that the concatenation of two unary dfes of size n can be realised by an dfa of size $O(n^2)$; actually, he gives an explicit formula on the size of the stem and the cycle which depends only on the size of the stems and the cycles in the two input automata. Pighizzini's result allows for an implementation of the following concatenation algorithm [15]: Convert the two ufes into dfes and then apply the algorithm to make the concatenation of dfes; this gives the upper bound of $2^{O((n \log n)^{1/2})}$ for the size of the concatenation ufa, thus the exponent of the size is up to a constant the same as the exponent of the blow-up at the transformation of an n -state ufa to a dfa.

The following corollary summarises the costs of operations. It takes the following information into account.

Holzer and Kutrib [8] showed that the intersection of two ufes is just given by the n^2 state sized product automaton of the two n -state ufes which preserves the property of being ufes.

The bounds for the disjoint union are listed by Jirásková and Okhotin [13] and are obtained by the simple union of the two ufes (this might give multiple start states, which is allowed for ufes); note that as the languages are disjoint, on each word in the union, one can reach as accepting state only in one of the ufes and there, by assumption, the way into the accepting state is unique. For the general union of two languages L, H given by n -state ufes, consider the formula $L \cup (H - L)$ where $H - L$ is equal to the intersection of H and the complement of L .

The symmetric difference of two languages L, H is the disjoint union of $L - H$ and $H - L$, thus the corresponding formula applies.

For concatenation, the best known bound is that of Okhotin's conversion of an ufa into a dfa [14] and then the corresponding operations are done with the resulting dfa or dfes which are often polynomial, that is, increase the exponent only by a constant factor. The lower bound for the disjoint union is just the length of two even length cycles differing by

length 2; one cycle has the accepting states at the even positions and the other one at the odd positions.

Finite formulas refers to a formula with several input automata combining the input n -state ufas with regular operations to a new ufa.

► **Corollary 9.** *Given ufas with up to n states recognising the languages L, H and let $c(n)$ satisfying $c(n) \in n^{\log n + O(1)}$ be the bound on the size of an ufa from Theorem 2 which is recognising the complement $c(L)$ of L . For the standard regular operations on languages over the unary alphabet, one obtains the following bounds.*

Operation	Lower Bound	Source	Upper Bound	Source
Intersection	$n^2 - n$	Holzer and Kultrīb [8]	n^2	Holzer and Kultrīb [8]
Complement	$n^{(\log \log \log n)^{\Omega(1)}}$	Raskin [16]	$c(n)$	Theorem 2
Disjoint union	$2n - 4$	see above	$2n$	Jirásková and Okhotin [13]
Union $L \cup H$	–	–	$n + n \cdot c(n)$	$L \cup (c(L) \cap H)$
Symmetric difference	–	–	$2n \cdot c(n)$	Theorem 2
Kleene Star	$(n - 1)^2 + 1$	Čevorová [3]	$(n - 1)^2 + 1$	Čevorová [3]
Concatenation	$2^{\Omega(n^{1/6})}$	Theorem 7	$2^{O((n \log^2 n)^{1/3})}$	Okhotin [14]
Finite Formula	$ETH \Rightarrow 2^{\Omega(n^{1/3})}$	Theorem 11	$2^{O((n \log^2 n)^{1/3})}$	Okhotin [14]

In summary: All standard regular operations except concatenation have polynomial or quasipolynomial size-increase but concatenation has exponential-type size-increase.

One might ask whether one can evaluate constant-sized formulas using as inputs unary languages given by n -state ufas in a way which avoids the exponential-type blow-up in the evaluation, which the usage of concatenation brings with it. The answer is “no” as the following theorem shows. In the following, H, I, J are sets of words given by n -state nfas and K is a finite language.

► **Remark 10.** For the next result, one needs the following fact about the Exponential Time Hypothesis. Impagliazzo, Paturi and Zane [10] list only a constant ℓ for how often each variable occurs, however, one can replace each variable by ℓ copies and then each copy occurs once; however, now one has to add ℓ 2SAT-clauses per variable which code a circular implication between the truth-values of the ℓ copies replacing the original variable. Thus one has ℓn variables and total of (upto) ℓn clauses with 3-literals each and (upto) ℓn clauses with 2-literals each. If the original instances required, in the worst case, time c^n , the new instances require, in the worst case, time $(c^{1/\ell})^{\ell n}$ where ℓn is the new number of variables.

Note that one can obtain the same three-occur result also for some other NP-complete variants of 3SAT. For example, for X3SAT where a clause is true iff exactly one literal is true. To obtain such a formula, one takes the three-occur 3SAT instance obeying the Exponential Time Hypothesis with n variables for some n and requiring time c^n for some $c > 1$ to be solved and for each clause with three literals x_1, x_2, x_3 , one replaces this clause by four X3SAT clauses with 6 new variables $y_1, y_2, y_3, z_1, z_2, z_3$ which satisfy $y_1 + y_2 + y_3 = 1$ and $y_k + \neg x_k + z_k = 1$ representing the implication $y_k \rightarrow x_k$ for $k = 1, 2, 3$; the z_1, z_2, z_3 occur all exactly once. So if the new X3SAT-instance is satisfied then the original 3SAT instance is satisfied due to one of the y_k being true and thus implying that the literal x_k is true; on the other hand, one can easily compute from a satisfying assignment of the original 3SAT instance one of the new X3SAT instance. This gives a further dilution and the constant c

from the runtime bound of the original three-occur 3SAT instance for n variables (where without loss of generality all clauses have at least two literals) would be transformed to $(c^{1/10})10n$ due to there being at most $3n/2$ clauses (as each clause has at least two literals, and each variable appearing at most thrice) and 6 new variables being added per clause resulting in a total of $(1 + 6 \cdot 3/2) \cdot n$ variables in the translated instance. Now each y_k occurs in two clauses, each z_k in one clause and each original variable in up to three clauses which now code that an y -variable implies the corresponding literal for the three occurrences of that variable – the y -variables are then one for each such occurrence. However, these variants are not needed in the present work.

► **Theorem 11.** *Assuming ETH, it needs time $2^{\Omega(n^{1/3})}$ to evaluate the truth of the formula*

$$(L - (H_1 \cup H_2 \cup H_3 \cup H_4 \cup H_5)) \cdot K = L$$

where $H_1, H_2, H_3, H_4, H_5, K$ are given by n -state ufas and L is the set of all words.

Proof. As indicated in Remark 10, assume that each variable of a 3SAT instance occurs at most in one 3-literal clause and at most in two 2-literal clauses. Let m denote the number of variables of this modified problem; without loss of generality, $m/\log m$ and $m/3$ are natural numbers; $\log m$ is upbounded for this. The total number of clauses is bounded by $4m/3$ as each variable is in one 3-literal clause (shared with two other variables) and two 2-literal clauses. For ease of presentation, assume without loss of generality that there are exactly $4m/3$ clauses.

Partition the m variables into five sets such that no two variables of any clause appear in the same set. That is, colour each variable with colour $c = 1, 2, 3, 4, 5$ such that no two variables occurring in the same clause have the same colour.

Select $5m/\log m$ primes greater than $2m$, but still bounded by some constant times m (such primes exist by the prime number theorem). Suppose these primes are $p_{c,h}$, with $h = 0, 1, \dots, m/(\log m) - 1$ and $c = 1, 2, 3, 4, 5$. Divide the m variables into groups of $\log m$, and assign the variables of colour c in the h -th group to the prime $p_{c,h}$, for $h = 0, 1, \dots, m/(\log m) - 1$ and $c = 1, 2, 3, 4, 5$.

For each colour $c = 1, 2, 3, 4, 5$ construct a ufa for H_c as follows. For $h = 0, 1, \dots, m/(\log m) - 1$, create a cycle $C_{c,h}$ of length $(4m/3 + 1) \cdot p_{c,h}$. There are up to $p_{c,h}$ Boolean combinations of the truth-values of the variables assigned to $p_{c,h}$; for the ℓ -th such combination, for $k = 0, 1, \dots, 4m/3$, one makes the $[(4m/3 + 1) \cdot \ell + k + 1]$ -th state in $C_{c,h}$ accepting iff the ℓ -th combination of truth-values assigned to the variables assigned to $p_{c,h}$ makes the k -th clause true. As there is at most one variable in each clause which is coloured c , it follows that the above automaton for H_c has at most one accepting path for any unary word.

If there is an satisfying truth assignment to the variables, then let such a truth assignment be the $\ell_{c,h}$ -th for the variables assigned to $p_{c,h}$. Let r be such that $r \bmod p_{c,h} = \ell_{c,h}$, for $h = 0, 1, \dots, m/(\log m) - 1$ and $c = 1, 2, 3, 4, 5$. Now, for each $k < 4m/3$, for some c and h , $[(4m/3 + 1) \cdot \ell_{c,h} + k + 1]$ -th state in the cycle $C_{c,h}$ would be accepting. Thus, one has a sequence of $4m/3$ consecutive words in the language $H_1 \cup H_2 \cup H_3 \cup H_4 \cup H_5$ (starting with length which is $(4m/3 + 1) \cdot r + 1$ upto length $(4m/3 + 1) \cdot r + 4m/3$). However there is no sequence of $4m/3 + 1$ words in $H_1 \cup H_2 \cup H_3 \cup H_4 \cup H_5$ due to all cycles being in a rejecting state whenever the length of the word is a multiple of $4m/3 + 1$.

On the other hand, if there is a sequence of $4m/3$ consecutive words in the language $H_1 \cup H_2 \cup H_3 \cup H_4 \cup H_5$ it must be starting with some length $(4m/3 + 1) \cdot r + 1$ and ending at length $(4m/3 + 1) \cdot r + 4m/3 + 1$, for some r . But, then considering $\ell_{c,h} = r \bmod p_{c,h}$, it must be the case that for each $k < 4m/3$, for some c and h , $[(4m/3 + 1) \cdot \ell_{c,h} + k + 1]$ -th state in the cycle $C_{c,h}$ is accepting, and thus the 3SAT formula is satisfiable.

Now the complement of $H_1 \cup H_2 \cup H_3 \cup H_4 \cup H_5$ has a hole of $4m/3$ consecutive words iff the 3SAT formula is satisfiable. Let K contains all words of length strictly below $4m/3$ and no other words, an ufa with $4m/3+1$ states recognises K . Now $(L - (H_1 \cup H_2 \cup H_3 \cup H_4 \cup H_5)) \cdot K$ equals L iff there is no satisfying assignment of the 3SAT formula.

The size n of the five ufas for H_1, H_2, H_3, H_4, H_5 is $O(m^3/\log m)$ and $n \log n = \Theta(m^3)$, thus $m = \Theta((n \log n)^{1/3})$. It follows that checking the correctness of the given formula on seven n -state ufas requires at least time $2^{\Omega((n \log n)^{1/3})}$ under assumption of the Exponential Time Hypothesis. \blacktriangleleft

Note that Okhotin [14] provides an upper bound by converting the ufas into dfas and then carrying out the operations with dfas. These operations run in time polynomial in the size of the dfas constructed. While the size lower bound for concatenation of two n -state ufas is just $2^{\Omega(n^{1/6})}$, the following conditional bound on the computational complexity of finding an ufa for the concatenation is even higher: $2^{\Omega(n^{1/4})}$ when using the Exponential Time Hypothesis.

► Theorem 12. *Under the assumption of the Exponential Time Hypothesis, one needs at least $2^{\Omega(n^{1/4})}$ time to compute an ufa for the language of the concatenation of the languages of two given n -state ufas in worst case.*

Proof. Let m be an m -variable 3SAT instance with at most $3m$ clauses, where each variable occurs at most three times. Assume without loss of generality that $m \geq 4$ and $\log m$ is a whole number. Let the clauses be u_1, u_2, \dots, u_{3m} , and the variables be x_1, x_2, \dots, x_m . Let $r = \lfloor (\log m + 3)/3 \rfloor$. Intuitively, we will assign r clauses (and variables in these clauses) to each cycle in the ufa.

It follows from the prime number theorem that there is a constant c' independent of m such that the set P_m of primes between $8m$ and $c'm$ has at least cardinality $s = 3m/r$. Consider the primes p_1, p_2, \dots, p_s in P_m .

Now one assigns to each prime number p_i , the clauses $u_{(i-1)r+1}, u_{(i-1)r+2}, \dots, u_{i*r}$ and the variables appearing in them. As there are at most $3r = \log m + 3$ variables assigned to these clauses, the number of possible truth assignments to such variables is at most $8m < p_i$. Also, each variable might be in clauses assigned to at most three such primes.

The cycles in the ufa have length of the following form, where the start position of each cycle is at position 0 and the accepting states for each cycle is mentioned. Each cycle accesses only positions which have some fixed value modulo $5m+1$ (with no intersection on the positions), which maintains the ufa nature.

1. One cycle is of length $5m+1$, where exactly the state at the position 0 is accepting.
2. For each prime p_i , which has clauses $u_{(i-1)r+1}, u_{(i-1)r+2}, \dots, u_{i*r}$ assigned to it, make a cycle of length $(5m+1) \cdot p_i$. The cycle has accepting state at position $h + (5m+1)k$, for $h \in \{(i-1)r+1, (i-1)r+2, \dots, i*r\}$, if the clause u_h is not satisfied by the k -th possible truth-assignment to the variables (upto $3r = \log m + 3$) in the clauses assigned to p_i , or the number k is bigger than the number of possible truth assignments to the variables but less than p_i .
3. For each variable x_j consider primes $p_i, p_{i'}, p_{i''}$ with $p_i < p_{i'} < p_{i''}$ to which it is associated with. Note that only p_i is guaranteed to exist; the others might be absent in the case that all clauses involving x_j are coded in the same variable p_i . If p_i and $p_{i'}$ exist one has a cycle of length $p_i \cdot p_{i'} \cdot (5m+1)$ and the position $k \cdot (5m+1) + j + 3m$ is accepting provided that $(k \text{ modulo } p_i)$ -th possible truth assignment to variables associated with p_i and $(k \text{ modulo } p_{i'})$ -th possible truth assignment to variables associated with $p_{i'}$ give different truth assignment to x_j . Similarly, if $p_i, p_{i'}, p_{i''}$ all three exist, one has a cycle

of length $p_{i'} \cdot p_{i''} \cdot (5m + 1)$ and the position $k \cdot (5m + 1) + j + 3m$ is accepting provided that $(k \bmod p_{i'})$ -th possible truth assignment to variables associated with $p_{i'}$ and $(k \bmod p_{i''})$ -th possible truth assignment to variables associated with $p_{i''}$ give different truth assignment to x_j .

Now all unary strings of length in multiples of $5m + 1$ are on the accepting state of the first cycle. Furthermore, given some ℓ , the unary strings of length of form $(5m + 1)\ell + 1, (5m + 1)\ell + 2, \dots, (5m + 1) + 5m$ are all rejecting iff $(\ell \bmod p_i)$ -th truth assignment for variables associated with p_i (for each i), defines a partial satisfying assignment by the cycle of the second type and, furthermore, for every variable x_j being assigned to two or three primes $p_i, p_{i'}, p_{i''}$, the $(\ell \bmod p_i)$ -th, $(\ell \bmod p_{i'})$ -th and $(\ell \bmod p_{i''})$ -th truth assignments to variables associated with $p_i, p_{i'}, p_{i''}$ respectively coincide in their assignment to x_j , so that there is no accepting state by a cycle of the third type activated at positions $(5m + 1)\ell + j + 3m$ and $(5m + 1)\ell + j + 4m$ in the two corresponding cycles. Thus an interval of length $5m$ without any word in the language occurs iff the coded 3SAT formula has a satisfying assignment. This allows to conclude that the concatenation of the so defined language L and the language of all words strictly shorter than $5m$ is universal, that is, contains all unary words, iff the coded 3SAT instance does not have a solution.

Now let $2^{F(n)}$ be the time to compute the ufa for the concatenation of the languages of two given n -state ufas; as the algorithm writes in each cycle at most one symbol of the output, the number of states in the ufa computed is also bounded by $2^{F(n)}$. Now by Theorem 4 and its corollary, one can decide in time $2^{O(F(n))}$ whether the so constructed ufa is universal, that is, contains all binary words.

The above constructed ufa coding the solvability of an m -variable 3SAT instance has up to $n = (5m + 1) \cdot (1 + ((9m)/(\log m + 3))c'm + 2m(cm')^2) \leq (9m)^2(cm')^2 \in O(m^4)$ states; this bound is obtained by counting the number of cycles created above and multiplying them with the cycle length and then taking upper bounds on the resulting expressions. As said, concatenating the language L of this ufa with the language of all words up to length $5m - 1$ results in a language which contains all unary words iff the corresponding 3SAT formula is not satisfiable. Thus one can decide in time $2^{O(F(n))}$ whether the coded three-occur 3SAT instance is satisfiable. By the assumption of the Exponential time hypothesis, $2^{\Omega(m)} \subseteq 2^{O(F(n))}$. Furthermore, $m \in \Omega(n^{1/4})$. Thus $2^{\Omega(n^{1/4})} \subseteq 2^{O(F(n))}$ and it follows that also $2^{F(n)}$ is a function in $2^{\Omega(n^{1/4})}$. This proves the given time bound. ◀

► **Remark 13.** This result also proves, that for deciding whether the concatenation of two languages given by n -state ufas is universal, the Exponential Time Hypothesis implies a $2^{\Omega(n^{1/4})}$ lower bound. The upper bound of this is slightly better than the dfa-conversion bound $2^{O((n \log^2 n)^{1/3})}$ of Okhotin [14]: Theorem 1 proves that the universality of an nfa can be checked in time $2^{O((n \log n)^{1/3})}$ and as the concatenation of two n -state ufas can be written as an $2n$ -state nfa, this upper bound also applies to checking the universality of the so obtained nfa.

4 Membership in Regular Languages of Infinite Words

For a finite alphabet, a finite word is a finite string over this alphabet; in the present work, the alphabet has exactly one member. The characteristic function of a language (set) L of finite words, can be viewed as the infinite word $L(0)L(1)\dots$; if the i -th word is in L then $L(i) = 1$ else $L(i) = 0$. Thus the characteristic function of the language L can be viewed as an ω -word and $L(0)L(1)\dots$ is the ω -word generated by the language L . An ω -language

is a set of ω -words and it is regular iff a nondeterministic Büchi automaton recognises the language.

Büchi [2] showed in particular that an ω -language is regular iff there exist finitely many regular languages $A_1, A_2, \dots, A_n, B_1, B_2, \dots, B_n$ such that B_1, B_2, \dots, B_n do not contain the empty word and the given ω -language equals $\bigcup_k A_k \cdot B_k^\infty$ where B_k^∞ is the set of infinite concatenations of members in B_k ; all elements of an ω -language are ω -words.

Now the question investigated is the following: Given a fixed ω -regular language, what is the complexity to check whether the ω -word generated by a unary n -state nfa is in this given ω -language. The lower bound of Fernau and Krebs [6] directly shows that this task requires, under the exponential time hypothesis, at least $2^{\Omega(n^{1/3})}$ deterministic time, where n is the number of states of the input nfa. An upper bound is obtained by converting the nfa to a dfa and then computing words v, w such that the ω -word generated by the language equals vw^ω . Then, one checks if is a k such that the $vw^\omega \in A_k \cdot B_k^\infty$; this can be done by constructing a deterministic Muller automaton for the given ω -language. For this, one first feeds the Muller automaton v and records the state after processing v . Then one feeds the Muller automaton each time with w and records the entry and exit states and which states were visited. After some time, the Muller automaton goes, when processing finitely many copies of w , through a loop and the states visited in this loops are the infinitely often visited states; from these one can compute the membership of vw^ω in $A_k \cdot B_k^\infty$. The complexity of this algorithm is $\text{Poly}(n) \cdot 2^{\Theta((n \log n)^{1/2})}$ —mainly by using the length bound on the period mentioned in the survey of Holzer and Kutrib [9] and other sources as well as stepwise simulating the nfa for each input, whether the next bit in the ω -word generated by the language accepted by the nfa is 0 or 1, in order to feed this bit into the Muller automaton until one has seen enough periods of w in order to determine the infinitely often visited states of the Muller automaton.

► **Theorem 14.** *Assuming the Exponential Time Hypothesis, checking whether an n -state nfa defines an ω -word in \mathcal{L} takes at least time $2^{\Omega((n \log \log n / \log n)^{1/2})}$.*

Proof. Impagliazzo, Paturi and Zane [10] showed that whenever the Exponential Time Hypothesis holds then this is witnessed by a sequence of 3SAT formulas which has linearly many clauses when measured by the number of variables. Such clauses will be coded up as follows in an nfa.

One codes an m variable, k clause 3SAT with $k \in O(m)$ using an nfa as follows. Suppose x_1, \dots, x_m are the variables used in the 3SAT formula, and C_1, \dots, C_k are the k clauses.

Let $r' = \lceil \log \log m \rceil$, $r = 2^{r'}$. Without loss of generality assume m is divisible by r' : otherwise we can increase m (upto doubling) to make this hold and add one literal clauses to the 3SAT formula using the new variables, without changing the big O complexity.

The nfa has disjoint cycles of different prime lengths p_1, p_2, \dots, p_t , where $t \in \Theta(m / \log \log m)$ and each of these prime numbers are at least $4(rk + 20)$ and in $\Theta(m \log m)$. Note that by the prime number theorem, as $k \in O(m)$, there are such different primes where the constant in the Θ also depends on the constant of the linear bound of k in m . So the overall size of the nfa is $\Theta(m^2 \log m / \log \log m)$. Intuitively, we will use a cycle of length p_i to handle the variables $x_{(i-1)r'+1} x_{(i-1)r'+2} \dots x_{(i-1)r'+r'}$.

For each prime length p_i , where $i = 1, 2, \dots, t$ as above, the cycle of length p_i codes $(1100000(10a_{i,\ell,h}0)_{h=1}^k 1000011)_{\ell=1}^r 1^{p_i-r(k+14)}$ where 1 denotes accepting state in the cycle and 0 denotes rejecting state in the cycle. Here $a_{i,\ell,h}$ is 1 if the truth assignment to $x_{(i-1)r'+1} x_{(i-1)r'+2} \dots x_{(i-1)r'+r'}$ being the ℓ -th binary string in $\{0, 1\}^{s'_i}$ makes the h -th clause C_h true, and 0 otherwise. Each item $(1100000(10a_{i,\ell,h}0)_{h=1}^k 1000011)$ is called a block and each block codes a possible truth assignment to the variables encoded by prime p_i : block corresponding to a value ℓ corresponds to the ℓ -th truth assignment to the variables $x_{(i-1)r'+1}$

$x_{(i-1)*r'+2} \dots x_{(i-1)*r'+r'}$, and the part $10a_{i,\ell,h}0$ corresponds to checking if the h -th clause is satisfied. Note that $r = 2^{r'}$ is the number of possible truth-assignments to these r' variables.

Note that five consecutive zeros only occur at the beginning of a block and four consecutive zeros only occur at the end of a block.

Each cycle has a different prime length; thus, by the Chinese remainder theorem, for each possible truth assignment to the variables, there is a number s such that $s \bmod p_i$ is the starting position of the block where the corresponding variable values are used for evaluating which clauses are satisfied. Thus, if a truth assignment leads to the 3SAT formula being true, then for the language L recognised by the nfa, $L(s)L(s+1) \dots L(s+4k+13)$ would be $1100000(1010)^k1000011$ which is in $1100000(1010)^+1000011$. On the other hand, if $1100000(1010)^+1000011$ is a substring of $L(0)L(1) \dots$, then let $L(s)$ be the starting point for the substring $1100000(1010)^+1000011$ in $L(0)L(1) \dots$. Then, as 11000001 can happen only at start of a block of any cycle of the nfa and 1000011 only at the end of a block of any cycle of the nfa, we must have that $(1010)^+$ must be of the form $(1010)^k$. Thus, for some ℓ_i corresponding to each i , for each value of h in $\{1, 2, \dots, k\}$, for some i , $a_{i,\ell_i,h}$ is 1. Thus the 3SAT formula is satisfiable.

This proves the reduction of a 3SAT formula to the question whether the ω -word generated by the corresponding nfa is in the ω -language

$$\{0, 1\}^*1100000(1010)^+1000011\{0, 1\}^\infty.$$

Now $n \in \Theta(m^2 \log m / \log \log m)$ and therefore $\Theta(\log n) = \Theta(\log m)$; thus $m \in \Omega((n \log \log n / \log n)^{1/2})$ and, by the Exponential Time Hypothesis, determining the membership of the ω -language defined by an unary n -state nfa requires at least time $c^{(n \log \log n / \log n)^{1/2}}$ for some constant c . It follows that logarithms of the computation time of the upper and lower bounds match up to a factor in $O(\log n)$. \blacktriangleleft

► **Remark 15.** One can make a marker of the form 1100011000110001100011 at the beginning of the bits coded in each cycle – the primes have to be slightly larger for that – and this marker only occurs as a word in the subword of the ω -word iff all cycles are in the initial position; otherwise some overlap with a consecutive run of three 1s or the subword $10a010b01$ ($a, b \in \{0, 1\}$) inside the area of the above marker would occur which provides an additional 1 to go into the marker. Therefore (using an ω -automaton) one can recognise the beginning of intervals which code, for each combinations of variable assignments, one block which is of the form $1100000\{1010, 1000\}^+1000011$ and which has the subword 10001 iff the variable-assignment does not satisfy the given instance. Thus one can – modulo some fixed constant – count the number of solutions of the instance represented by the ω -word. Therefore the membership in the corresponding ω -language, which can be chosen as fixed, can check whether the correctly coded ω -words representing an m -variable k -clause 3SAT instance has, modulo a fixed natural number, a nonzero number of solutions. Such counting checks are not known to be in the polynomial hierarchy, thus the membership test for fixed ω -languages is represented by a complexity class possibly larger than **NP** or **PH**.

► **Remark 16.** The construction in Theorem 11 can be adjusted as follows. One combines all five ufas for H_1, H_2, H_3, H_4, H_5 such that the cycle length of $(4m/3 + 1) \cdot p_{c,h}$ is adjusted to $(20 + 8m) \cdot p_{c,h}$. Furthermore, one codes for each clause not one bit in five ufas, but six bits in one ufa, with the first bit being always 0 and the next five bits being 1 based on whether the corresponding coloured variable satisfies the clause (that is, if in the Theorem 11, H_i would have set the clause true), for the colours 1, 2, 3, 4, 5. The whole sequence of blocks is not preceded by one single 0 but by 1111110 . The sequence ends with 0111111000000 . These are 20 constant bits to be coded instead of one previously.

Now let $R = \{0\} \cdot (\{0, 1\}^5 - \{00000\})$ and consider the ω -language $\{0, 1\}^* \{111110\} \cdot R^* \cdot \{0111111000000\} \cdot \{0, 1\}^\omega$. This ω -language contains the ω -word of the translated instance iff the 3SAT formula has a satisfying assignment. In this ω -language, its defining formula just says that there is somewhere a pattern where the members of R just indicate that there is at least one literal per coded clause which makes the corresponding clause true and that there are no codes of unsatisfied clauses (which would be 000000) between the code for the start and the end of the instance; the blocks at the start and the end are chosen such that the end block has so many trailing zeroes that one cannot swap the start and end block in order to get something which is falsely interpreted as the code of a satisfied instance. Thus one can decide m -variable 3SAT if the corresponding ufa is in the language. The size of the ufa is $\Theta(m^3 / \log m)$ and thus the value m is $\Theta((n \log n)^{1/3})$. It follows that by the Exponential Time Hypothesis, one needs at least time $2^{\Omega((n \log n)^{1/3})}$ to check the membership of an ω -word given by an n -state ufa in a fixed ω -language in the worst case. The exponent in this conditional lower bound differs by a factor of $(\log n)^{1/3}$ from the upper bound obtained by converting the ufa into a dfa and then running the corresponding test.

References

- 1 Manindra Agrawal, Neeraj Kayal and Nitin Saxena. PRIMES is in P. *Annals of Mathematics*, 160:781–793, 2004.
- 2 J. Richard Büchi. On a decision method in restricted second order arithmetic. *Proceedings of the International Congress on Logic, Methodology and Philosophy of Science*, Stanford University Press, Stanford, California, 1960.
- 3 Kristína Čevorová. Kleene star on unary regular languages. *Descriptive Complexity of Formal Systems: Fifteenth International Workshop, DCFS 2013, London, Ontario, Canada, July 22–25, 2013. Proceedings. Springer LNCS 8031:277–288*, 2013.
- 4 Marek Chrobak. Finite automata and unary languages. *Theoretical Computer Science* 47:149–158, 1986.
- 5 Thomas Colcombet. Unambiguity in Automata Theory. *Seventeenth International Workshop on Descriptive Complexity of Formal Systems DCFS 2015, Springer LNCS 9118:3–18*, 2015.
- 6 Henning Fernau and Andreas Krebs. Problems on finite automata and the exponential time hypothesis. *Algorithms* 10.1:24, 2017.
- 7 Mika Göös, Stefan Kiefer and Weiqiang Yuan. Lower bounds for unambiguous automata via communication complexity. *Forty Ninth International Colloquium on Automata, Languages and Programming, ICALP 2022, July 4–8, 2022, Paris, France. LIPIcs 229:126:1–126:13*, 2022. See also the technical report on <http://www.arxiv.org/abs/2109.09155>, Version 2, 2022.
- 8 Markus Holzer and Martin Kutrib. Unary language operations and their nondeterministic state complexity. *International Conference on Developments in Language Theory. Springer LNCS 2540:162–172*, 2002.
- 9 Markus Holzer and Martin Kutrib. Descriptive and computational complexity of finite automata – a survey. *Information and Computation*, 209:456–470, 2011.
- 10 Russel Impagliazzo, Ramamohan Paturi and Francis Zane. Which problems have strongly exponential complexity? *Journal of Computer and System Sciences* 63.4:512–530, 2001.
- 11 Tao Jiang, Edward McDowell and Bala Ravikumar. The structure and complexity of minimal NFA’s over a unary alphabet. *International Journal of Foundations of Computer Science*, 2(2):163–182, 1991.
- 12 Hendrik W. Lenstra, Jr, and Carl B. Pomerance. Primality testing with Gaussian periods. *Journal of the European Mathematical Society* 21.4:1229–1269, 2019.

- 13 Galina Jirásková and Alexander Okhotin. State complexity of unambiguous operations on deterministic finite automata. *Twentieth Conference on Descriptive Complexity of Formal Systems*, Halifax, Canada, *Springer LNCS* 10952:188–199, 2018.
- 14 Alexander Okhotin. Unambiguous finite automata over a unary alphabet. *Information and Computation* 212:15–36, 2012
- 15 Giovanni Pighizzini. Unary language concatenation and its state complexity. *Implementation and Application of Automata: Fifth International Conference*, CIAA 2000, London, Ontario, Canada, 24–25 July 24 2000. Springer Berlin Heidelberg, *Springer LNCS* 2088:252–262, appeared 2001.
- 16 Michael Raskin. A superpolynomial lower bound for the size of non-deterministic complement of an unambiguous automaton. *Forty-fifth International Colloquium on Automata, Languages and Programming ICALP 2018, Leibniz International Proceedings in Informatics* 107:138.1–138.11, 2018.
- 17 Christopher Tan. *Characteristics and Computation of Minimal Automata*. Undergraduate Research Opportunity Programme in Science, National University of Singapore, Singapore 2022.