

Alternating Automatic Register Machines

Ziyuan Gao^{1(\boxtimes)}, Sanjay Jain^{2(\boxtimes)}, Zeyong Li^{3(\boxtimes)}, Ammar Fathin Sabili^{2(\boxtimes)}, and Frank Stephan^{1,2(\boxtimes)}

 ¹ Department of Mathematics, National University of Singapore, 10 Lower Kent Ridge Road, S17, Singapore 119076, Republic of Singapore matgaoz@nus.edu.sg
² School of Computing, National University of Singapore, 13 Computing Drive, COM1, Singapore 117417, Republic of Singapore

{sanjay,ammar,fstephan}@comp.nus.edu.sg

³ Centre for Quantum Technologies, National University of Singapore, Block S15, 3 Science Drive 2, Singapore 117543, Singapore

li.zeyong@u.nus.edu

Abstract. This paper introduces and studies a new model of computation called an Alternating Automatic Register Machine (AARM). An AARM possesses the basic features of a conventional register machine and an alternating Turing machine, but can carry out computations using bounded automatic relations in a single step. One finding is that an AARM can recognise some NP-complete problems, including CNF-SAT (using a particular coding), in $\log^* n + \mathcal{O}(1)$ steps. On the other hand, if all problems in P can be solved by an AARM in $\mathcal{O}(\log^* n)$ rounds, then $P \subset PSPACE$.

Furthermore, we study an even more computationally powerful machine, called a Polynomial-Size Padded Alternating Automatic Register Machine (PAARM), which allows the input to be padded with a polynomial-size string. It is shown that the polynomial hierarchy can be characterised as the languages that are recognised by a PAARM in $\log^* n + \mathcal{O}(1)$ steps. These results illustrate the power of alternation when combined with computations involving automatic relations, and uncover a finer gradation between known complexity classes.

Keywords: Theory of computation \cdot Computational complexity \cdot Automatic relation \cdot Register machine \cdot Nondeterministic complexity \cdot Alternating complexity \cdot Measures of computation time

1 Introduction

Automatic structures generalise the notion of regularity for languages to other mathematical objects such as functions, relations and groups, and were

Z. Gao (as RF) and S. Jain (as Co-PI), F. Stephan (as PI) have been supported by the Singapore Ministry of Education Academic Research Fund grant MOE2019-T2-2-121/R146-000-304-112. Furthermore, S. Jain is supported in part by NUS grants C252-000-087-001 and E-252-00-0021-01. Further support is acknowledged for the NUS tier 1 grants AcRF R146-000-337-114 (F. Stephan as PI) and R252-000-C17-114 (F. Stephan as PI).

discovered independently by Hodgson [10,11]. Khoussainov and Nerode [14] as well as Blumensath and Grädel [1,2]. One of the original motivations for studying automaticity in general structures came from computable structure theory, in particular the problem of classifying the isomorphism types of computable structures and identifying isomorphism invariants. In computer science, automatic structures arise in the area of infinite state model checking; for example, Regular Model Checking, a symbolic framework for modelling and verifying infinite-state systems, can be expressed in Existential Second-Order Logic over automatic structures [17]. Although finite-state transducers are a somewhat more popular extension of ordinary finite-state automata for defining relations between sets of strings, there are several advantages of working with automatic relations, including the following: (1) in general, automatic relations enjoy better decidability properties than finite-state transducers; for example, equivalence between ordinary automata is decidable while this is not so for finite-state transducers; (2) automatic relations are closed under first-order definability [11,13,14] while finite-state transducers are not closed under certain simple operations such as intersection and complementation.

In this paper, we introduce a new model of computation, called an *Alternat*ing Automatic Register Machine (AARM), that is analogous to an alternating Turing machine but may incorporate *bounded* automatic relations¹ into each computation step. The main motivation is to try to discover new interesting complexity classes defined via machines where automatic relations are taken as primitive steps, and use them to understand relationships between fundamental complexity classes such as P, PSPACE and NP. More powerful computational models are often obtained by giving the computing device more workspace or by allowing non-deterministic or *alternating* computations, where alternation is a well-known generalisation of non-determinism. We take up both approaches in this work, extending the notion of alternation to automatic relation computations. An AARM is similar to a conventional register machine in that it consists of a register R containing a string over a fixed alphabet at any point in time, and the contents of R may be updated in response to *instructions*. One novel feature of an AARM is that the contents of the register can be non-deterministically updated using an automatic relation. Specifically, an instruction J is an automatic relation. Executing the instruction, when the content of the register R is r, means that the contents of R is updated to any x in $\{x:(x,r)\in J\}$; if there is no such x, then the program halts. Each AARM contains two finite classes, denoted here as A and B, of instructions; during a computation, instructions are selected alternately from A and B and executed.

To further explain how a computation of an AARM is carried out, we first recall the notion of an *alternating Turing machine* as formulated by Chandra, Kozen and Stockmeyer [5]. As mentioned earlier, alternation is a generalisation

¹ Here an update relation is *bounded* if there is a constant such that each possible output is at most that constant longer than the longest input parameter; see Sect. 2. Since we only consider bounded automatic relations in this paper, such relations will occasionally be called "automatic relations".

of non-determinism, and it is useful for understanding the relationships between various complexity classes such as those in the polynomial hierarchy (PH). The computation of an alternating Turing machine can be viewed as a game in which two players – Anke and Boris – make moves (not necessarily strictly alternating) beginning in the start configuration of the machine with a given input w [8]. Anke and Boris move alternating with each having specific win configurations. A language L is in AAL[f(n)] if there is an AARM such that, for each input x, one player can force a win in f(|x|) many steps. Then x is in L if Anke can force the win. In general, we are for natural choices of f interested in the class AAL[f(n) + O(1)] and our results indicate that $f(n) = \log^* n$ is an important choice allowing interesting results; smaller functions f only lead to the class of regular languages. Furthermore, we found that the picture becomes much more interesting by allowing only such automatic relations which permit a player to choose between finitely many options. We call such automatic relations bounded and for each bounded automatic relation R there is a constant c such that R(x, y)can only be satisfied if $|y| \leq |x| + c$; here y is the value chosen by the player in dependence of a register content x. We also introduce and study Polynomial-Size Padded Bounded Alternating Automatic Register Machines (PAARMs), which allow a polynomial-size padding to the input of an AARM.

The idea of defining computing devices capable of performing single-step operations that are more sophisticated than the basic operations of Turing machines is not new. For example, Floyd and Knuth [7] studied addition machines, which are finite register machines that can carry out addition, subtraction and comparison as primitive steps. Unlimited register machines, introduced by Shepherdson and Sturgis [18], can copy the number in a register to any register in a single step. Bordihn, Fernau, Holzer, Manca and Martín-Vide [3] investigated another kind of language generating device called an *iterated sequential* transducer, whose complexity is usually measured by its number of states (or state complexity). More recently, Kutrib, Malcher, Mereghetti and Palano [15] proposed a variant of an iterated sequential transducer that performs lengthpreserving transductions on left-to-right sweeps. Automatic relations are more expressive than arithmetic operations such as addition or subtraction, and yet they are not too complex in that even one-tape linear-time Turing machines are computationally more powerful; for instance, the function that erases all leading 0's in any given binary word can be computed by a one-tape Turing machine in linear time but it is not automatic [20]. Despite the computational limits of automatic relations, we show in Theorem 6 below that the NP-complete Boolean satisfiability problem can be recognised by an AARM in $\log^* n + \mathcal{O}(1)$ steps, where n is the length of the formula. The results not only show a proofof-concept for the use of automatic relations in models of computation, but also shed new light on the relationships between known complexity classes.

For an extended version of this paper that presents examples and additional basic results on AARMs and PAARMs, please refer to [9].

2 Preliminaries

Let Σ denote a finite alphabet. We consider set operations including union (\cup) , concatenation (·), Kleene star (*), intersection (\cap) and complement (\neg). Let Σ^* denote the set of all strings over Σ . A *language* is a set of strings. Let the empty string be denoted by ε . For a string $w \in \Sigma^*$, let |w| denote the length of w and $w = w_1 w_2 \dots w_{|w|}$ where $w_i \in \Sigma$ denotes the *i*-th symbol of w. Fix a special symbol # not in Σ . Let $x, y \in \Sigma^*$ such that $x = x_1 x_2 \dots x_m$ and $y = y_1 y_2 \dots y_n$. Let $x' = x'_1 x'_2 \dots x'_r$ and $y' = y'_1 y'_2 \dots y'_r$ where $r = \max(m, n), x'_i = x_i$ if $i \le m$ else #, and $y'_i = y_i$ if $i \leq n$ else #. Then, the convolution of x and y is a string over $(\Sigma \cup \{\#\}) \times (\Sigma \cup \{\#\})$, defined as $conv(x, y) = (x'_1, y'_1)(x'_2, y'_2) \dots (x'_r, y'_r)$. A relation $J \subseteq X \times Y$ is *automatic* if the set $\{conv(x, y) : (x, y) \in J\}$ is regular, where the alphabet is $(\Sigma \cup \{\#\}) \times (\Sigma \cup \{\#\})$. Likewise, a function $f: X \to Y$ is automatic if the relation $\{(x, y) : x \in domain(f) \land y = f(x)\}$ is automatic [21]. An automatic relation J is bounded if \exists constant c such that $\forall (x, y) \in$ $J, \operatorname{abs}(|y| - |x|) \leq c$. On the other hand, an unbounded automatic relation has no such restriction. The problem of determining satisfiability of any given Boolean formula in conjunctive normal form will be denoted by CNF-SAT. Automatic functions and relations have a particularly nice feature as shown in the following theorem.

Theorem 1 ([11,14]). Every function or relation which is first-order definable from a finite number of automatic functions and relations is automatic, and the corresponding automaton can be effectively computed from the given automata.

3 Alternating Automatic Register Machines

An Alternating Automatic Register Machine (AARM) consists of a register R and two finite sets A and B of *instructions*. A and B are not necessarily disjoint. Formally, we denote an AARM by M and represent it as a quadruple (Γ, Σ, A, B) . (An equivalent model may allow for multiple registers.) At any point in time, the register contains a string, possibly empty, over a fixed alphabet Γ called the register alphabet. The current string in R is denoted by r. Initially, R contains an input string over Σ , an *input alphabet* with $\Sigma \subseteq \Gamma$. Strings over Σ will sometimes be called *words*. The contents of the register may be changed in response to an instruction. An instruction $J \subseteq \Gamma^* \times \Gamma^*$ is a bounded automatic relation; this changes the contents of R to some x such that $(x,r) \in J$ (if such an x exists). The instructions in A and B are labelled I_1, I_2, \ldots , (in no particular order and not necessarily distinct). A configuration is a triple (ℓ, w, r) , where I_{ℓ} is the current instruction's label and $w, r \in \Gamma^*$. Instructions are generally nondeterministic, that is, there may be more than one way in which the string in R is changed from a given configuration in response to an instruction. A *com*putation history of an AARM with input w for any $w \in \Sigma^*$ is a finite or infinite sequence c_1, c_2, c_3, \ldots of configurations such that the following conditions hold. Let $c_i = (\ell_i, w_i, r_i)$ for all *i*.

- $-r_1 = w$. We call c_1 the *initial configuration* of the computation history.
- For all $i, (w_i, r_i) \in I_{\ell_i}$. This means that I_{ℓ_i} can be carried out using the current register contents, changing the contents of R to w_i .
- Instructions executed at odd terms of the sequence belong to A, while those executed at even terms belong to B:

$$I_{\ell_i} \in \begin{cases} A \text{ if } i \text{ is odd}; \\ B \text{ if } i \text{ is even.} \end{cases}$$

- If c_{i+1} is defined, then $r_{i+1} = w_i$. In other words, the contents of R are (nondeterministically) updated according to the instruction and register contents of the previous configuration.
- Suppose *i* is odd (resp. even) and $c_i = (I_{\ell_i}, w_i, r_i)$ is defined. If there is some $I_{\ell} \in B$ (resp. $I_{\ell} \in A$) with $\{x : (x, w_i) \in I_{\ell}\}$ nonempty, then c_{i+1} is defined. In other words, the computation continues so long as it is possible to execute an instruction from the appropriate set, either A or B, at the current term.

We interpret a computation history of an AARM as a sequential game between two players, Anke and Boris, where Anke moves during odd turns and Boris moves during even turns. During Anke's turn, she must pick some instruction Jfrom A such that $\{x: (x,r) \in J\}$ is nonempty and select some $w \in \{x: (x,r) \in J\}$ J; if no such instruction exists, then the game terminates. The contents of R are then changed to w at the start of the next turn. The moving rules for Boris are defined analogously, except that he must pick instructions only from B. Anke wins if the game terminates after a finite number of turns and she is the last player to execute an instruction; in other words, Boris is no longer able to carry out an instruction in B and the *length* of the game (or computation history), measured by the total number of turns up to and including the last turn, is odd. Boris wins the game if Anke does not win (this includes the case that Anke does not make any move). The AARM *accepts* a word w if Anke can move in such a way that she will always win a game with an initial configuration (ℓ, v, w) for some $I_{\ell} \in A$ and $v \in \Gamma^*$, regardless of how Boris moves. To state this acceptance condition more formally, one could define Anke's and Boris' strategies to be functions \mathcal{A} and \mathcal{B} respectively with $\mathcal{A} : (\mathbb{N} \times \Gamma^* \times \Gamma^*)^* \times \Gamma^* \mapsto \mathcal{A} \times \Gamma^*$ and $\mathcal{B}: (\mathbb{N} \times \Gamma^* \times \Gamma^*)^* \times \Gamma^* \mapsto B \times \Gamma^*$, which map each segment of a computation history together with the current contents of R to a pair specifying an instruction as well as the new contents of R at the start of the next round according to the moving rules given earlier. The AARM accepts w if there is an \mathcal{A} such that for every \mathcal{B} , there is a finite computation history $\langle c_1, \ldots, c_{2n+1} \rangle$ where

- $-c_i = (\ell_i, w_i, r_i)$ for each i,
- $-r_1=w,$
- $\mathcal{A}((\langle c_i : i < 2j+1 \rangle, r_{2j+1})) = (I_{\ell_{2j+1}}, w_{2j+1}) \text{ for each } j \in \{0, \dots, n\},\$
- $\mathcal{B}((\langle c_i : i < 2k \rangle, r_{2k})) = (I_{\ell_{2k}}, w_{2k}) \text{ for each } k \in \{1, \dots, n\};$
- there is no move for B in c_{2n+1} , that is no instruction in B contains a pair of the form (\cdot, w_{2n+1}) .

Here $\langle c_i : i < k \rangle$ denotes the sequence $\langle c_1, \ldots, c_{k-1} \rangle$, which is empty if $k \leq 1$. Such an \mathcal{A} is called a *winning strategy for Anke with respect to* (M, w). Given a winning strategy \mathcal{A} for Anke with respect to (M, w) and any strategy \mathcal{B} , the corresponding computation history of M with input w is unique and will be denoted by $\mathcal{H}(\mathcal{A}, \mathcal{B}, M, w)$. In most subsequent proofs, \mathcal{A} and \mathcal{B} will generally not be defined so formally. Set

$$L(M) := \{ w \in \Sigma^* : M \text{ accepts } w \};$$

one says that M recognises L(M). Note that a constant amount of extra state information can be stored in the register.

Definition 2 (Alternating Automatic Register Machine Complexity). Let $M = (\Gamma, \Sigma, A, B)$ be an AARM and let $t \in \mathbb{N}_0$. For each $w \in \Sigma^*$, M accepts w in time t if Anke has a winning strategy \mathcal{A} with respect to (M, w) such that for any strategy \mathcal{B} played by Boris, the length of $\mathcal{H}(\mathcal{A}, \mathcal{B}, M, w)$ is not more than t. (As defined earlier, $\mathcal{H}(\mathcal{A}, \mathcal{B}, M, w)$ is the computation history of M with input w when \mathcal{A} and \mathcal{B} are applied.) An AARM decides a language L in f(n) steps for a function f depending on the length n of the input if for all $x \in \{0,1\}^n$, both players can enforce that the game terminates within f(n) steps by playing optimally and one player has a winning strategy needing at most f(n) moves and $x \in L$ if Anke is the player with the winning strategy. AAL[f(n)] denotes the family of languages decided by AARMs that decide in time f(n).

It can be shown that AARMs recognise precisely the family of all recursively enumerable languages [9, Theorem 7], and that $AAL[\mathcal{O}(f(n))]$ is closed under the usual set-theoretic Boolean operations as well as the regular operations [9, Theorem 4].

We recall that an alternating Turing machine that decides in $\mathcal{O}(f(n))$ time can be simulated by a deterministic Turing machine using $\mathcal{O}(f(n))$ space. The following theorem gives a similar connection between the time complexity of AARMs and the space complexity of deterministic Turing machines.

Theorem 3. For any f such that $f(n) \ge n$, $AAL[\mathcal{O}(f(n))] \subseteq DSPACE[\mathcal{O}((n + f(n))f(n))] = DSPACE[\mathcal{O}(f(n)^2)].$

Proof. Given an AARM M, there is a constant c such that each register update by an automatic relation used to define an instruction of M increases the length of the register's contents by at most c. Thus, after $\mathcal{O}(f(n))$ steps, the length of the register's contents is $\mathcal{O}(n + f(n))$. As implied by [4, Theorem 2.4], each computation of an automatic relation with an input of length $\mathcal{O}(n + f(n))$ can be simulated by a nondeterministic Turing machine in $\mathcal{O}(n + f(n))$ steps; this machine can then be converted to a deterministic space $\mathcal{O}(n + f(n))$ Turing machine. If M accepts an input w, then there are $\mathcal{O}(f(n))$ register updates by automatic relations when Anke applies a winning strategy, and so there is a deterministic Turing machine simulating M's computation with input w using space $\mathcal{O}((n + f(n))f(n))$.

As a consequence, one obtains the following analogue of the equality between AP (classes of languages that are decided by alternating polynomial time Turing machines) and PSPACE.

Corollary 4. $\bigcup_k AAL[\mathcal{O}(n^k)] = PSPACE.$

Proof. The containment relation $AAL[\mathcal{O}(f(n))] \subseteq DSPACE[\mathcal{O}((n+f(n))f(n))]$ in Theorem 3 holds whether or not the condition $f(n) \ge n$ holds. Furthermore, the computation of an alternating Turing machine can be simulated using an AARM, where the transitions from existential (respectively, universal) states correspond to the instructions for Anke (respectively, Boris), and each computation step of the alternating Turing machine corresponds to a move by either player. Therefore PSPACE, which is equal to AP, is contained in $\bigcup_k AAL[n^k]$. \Box

We come next to a somewhat surprising result: an AARM-program can recognise 3SAT using just $\log^* n + \mathcal{O}(1)$ steps. To prove the theorem, we give the following lemma, which illustrates most of the power of AARMs.

Lemma 5 (Log-Star Lemma). Let $u, v \in \Sigma^*$. Let $\#, \$ \notin \Sigma$. Then both languages $\{u'\$v' : u' \in \#^*u\#^*, v' \in \#^*v\#^* \text{ and } u = v\}$ and $\{u'\$v' : u' \in \#^*u\#^*, v' \in \#^*v\#^* \text{ and } u \neq v\}$ are in $AAL[\log^* n + \mathcal{O}(1)]$.

The Log-Star Lemma essentially states that a comparison of two substrings can be done by an AARM in $\log^* n + \mathcal{O}(1)$ time. This is done by ignoring the unnecessary symbols in the register by replacing them with #'s and adding a separator (\$) between the two strings.

Proof. We now prove the Log-Star Lemma. The algorithm below recursively reduces the problem to smaller sizes of u, v in constant number of steps (the maximum of the length of u, v is reduced logarithmically in constant number of steps). For the base case, if size of u or v is bounded by a constant, then clearly both languages can be recognized in one step.

For larger size u, v, the algorithm/protocol works as follows. For ease of explanation, suppose Anke is trying to show that u = v (case of Anke showing $u \neq v$ will be similar). Given input s = u'\$v', player Anke will try to give each symbol except \$'s a mark $\in \{0, 1, 2, 3\}$ as follows:

- 1. For each # in u' and v', the mark of 3 will be given.
- 2. For the contiguous symbols of u, starting from the first symbol, the following infinite marking will be given (whitespaces are for the ease of readability and not part of marking):

20 21 200 201 210 211 2000 2001 2010 2011 2100 2101 2110 2111 20000 \cdots

Namely, a series of blocks of string in ascending length-lexicographical order. Let T be the so defined infinite sequence. Given a string s = u'\$v', where $u' \in \#^*u\#^*$ and $v' \in \#^*v\#^*$ for some $u, v \in \Sigma^*$, each contiguous subsequence of u (resp. v) whose sequence of positions is equal to the sequence of positions of T of some string in $2\{0,1\}^*$ such that the next symbol in T is 2 will be called a *block*. Each block starts with 2 followed by a binary string. Let k (≥ 2) be the maximum size of a block. Summing the lengths of the blocks of u gives that $(k-2) \cdot 2^{k-1} + k \leq n$, and thus $k \leq \log n$.

3. For the contiguous symbols of v, the marking will be similar.

The marking is considered *valid* if all above rules are satisfied. This is an example of a *valid* marking of S = #foobar##\$foobar##":

If u = v and the marking is *valid*, player Anke will guarantee that each symbol of u and v will be marked with exactly the same marking. However if $u \neq v$ and the marking is *valid*, either the length of u and v are different or there will be at least a single block which differs on at least one symbol between u and v. Therefore, player Boris can have the following choices of challenges:

- 1. Challenge that player Anke did not make a valid marking, or
- 2. $|u| \neq |v|$, or
- 3. the string in a specified block differs on at least one symbol between u and v.

Notice that u = v if and only if player Boris could not successfully challenge player Anke. The first challenge will ensure that player Anke gave a valid marking. There are three possible cases of invalid marking:

- (a) There is a # in u' or v' which is not given by a mark of 3. In this case, player Boris may point out its exact position. Here, player Boris needs 1 step.
- (b) For u and v, the first block is not marked with "20". This can also be easily pointed out by player Boris. Here, player Boris needs 1 step.
- (c) For u and v, a block is not followed by its successor. This can be pointed out by player Boris by checking two things: the length of the 'successor' block should be less than or equal to the length of the 'predecessor' block plus one, and the 'successor' block indeed should be the successor of the 'predecessor' block. Also, we note that the last block may be incomplete.
 - (i) The length case can be checked by looking at how many symbols there are between the pair of 2's bordering each block. Let p and q be the length of 'predecessor' block and the 'successor' block respectively. In the case that the 'successor' block is not the last block (not incomplete), player Boris may challenge if $p \neq q$ and $p + 1 \neq q$. This can be done by marking both blocks with 1 separated by \$ and the rest with dummy symbols # and then doing the protocol for equality of the modified u and v recursively. As player Boris may try to find the 'short' challenge, player Boris will find the earliest block which has the issue and thus make sure that p is at most logarithmic in the maximum of the lengths of u and v. As q may be much larger than p, player Boris may limit the second block by taking at most p + 2 symbols.
 - (ii) The successor case can be checked by the following observation. A successor of a binary string can be calculated by finding the last 0 symbol and flipping all digits from that position to the end while maintaining the previous digits. As an illustration, the successor of "101100111" will

be "10110<u>1</u>000" where the symbols are separated in 3 parts: the prefix which is the same, the last 0 digit, which is underlined, becoming 1; and all 1 digits on suffix becoming 0. Player Boris then may challenge the first part not to be equal or the last part not to be the same length or not all 1's by providing the position of the last 0 on the 'predecessor' block (or the last 1 on the 'successor' block, if any). Checking the equality of two strings can be done recursively, also similarly applied for checking the length. Notice a corner case of all 1's which has the successor consisting of 1 followed by 0's with the same length, which can be handled separately. Also notice that the 'successor' block may be incomplete if it is the last block, which can also be handled in a similar manner as above.

For the second challenge, player Boris can (assuming the marking is valid) check whether the last two blocks of u and v are equal. Again, player Boris may limit it for a 'short' challenge so the checking size is decreasing to its log. For the third challenge, player Boris will specify the two blocks on u and v (same block on both) which differ on at least one symbol between u and v. Again, same protocol will apply and the size is decreasing to its log. Furthermore, both the marking and selection of blocks are done in a single turn.

Thus, the above algorithm using one alternation of each of the players reduces the problem to logarithmic in the size of the maximum of the lengths of u and v. In particular, when the size of u and v are small enough, the checking will be done in constant number of steps. Thus, the complexity of the problem satisfies: $T(m_{k+1}) \leq T(\log m_k)$, where m_i denotes the maximum of the sizes of u and v at step i. As the lengths of u, v at each step are bounded by the length of the whole input string, the lemma follows. Note that either player can enforce that the algorithm runs in $\log^* n + \mathcal{O}(1)$ steps. The player makes the own markings always correct and challenges incorrect markings of the opponent at the first error so that the logarithmic size descent is guaranteed. Challenged correct markings always cause the size to go down once in a logarithmic scale.

Theorem 6. There is an NP-complete problem in $AAL[\log^* n + O(1)]$.

Proof. Consider any encoding of a SAT formula in conjunctive normal form such that after each variable occurrence there is a space for a symbol indicating the truth value of that variable. For example, literals may be represented as + or – followed by a variable name and then a space for the variable's truth value, clauses may be separated by semicolons, literals may be separated by commas and a dot represents the end of the formula. Anke sets a truth value for each variable occurrence in the formula and a dfa then checks whether or not between any two semicolons, before the first semicolon and after the last semicolon there is a true literal; if so, Boris can challenge that two identical variables received different truth values. It is now player Anke's job to prove that the two variables picked by Boris are different. By the Log-Star Lemma, this verification needs $\log^* n + O(1)$ steps. Hence, CNF-SAT ∈ AAL[$\log^* n + O(1)$]. □

The Log-Star Lemma can also be applied, using a technique similar to that in the proof of Theorem 6, to show that for any $k \geq 3$, the NP-complete problem k-COLOUR of deciding whether any given graph G is colourable with k colours belongs to AAL[log* n + O(1)]. Using a suitable encoding of nodes, edges and colours as strings, Anke first nondeterministically assigns any one of k colours to each node and ensures that no two adjacent nodes are assigned the same colour; Boris then challenges Anke on whether there are two substrings of the current input that encode the same node but encode different colours.

The next theorem shows that the class $AAL[log^* n + O(1)]$ contains NLOGSPACE.

Theorem 7. $NLOGSPACE \subseteq AAL[\log^* n + \mathcal{O}(1)].$

Proof. Consider an NLOGSPACE computation that takes time n^c . One creates a new variable consisting of \sqrt{n} equal-sized blocks of length \sqrt{n} (so the overall length is n) such that each block is used to store some configuration in the history so that constantly many alternating rounds between two players allow to check a LOGSPACE computation. Let s be the total number of steps on the input. Anke guesses for each block the following information:

- The overall number of steps needed, s;
- The block number;
- The rounded number of steps done in this block (approximately $\frac{s}{\sqrt{n}}$ steps);
- The total number of steps done until this block;
- The starting configuration at this block;
- The ending configuration at this block.

Furthermore, the number of variables needed is 2c plus a constant.

Boris can now challenge that some configuration is too long or that the number of digits is wrong or that the information at the end of one block does not coincide with the information at the start of another block or that initial and final configurations are not starting and ending configurations or select a block whose computation has to be checked in the next round, again by distributing the steps covered in this interval evenly onto \sqrt{n} blocks in the next variable.

By $\mathcal{O}(c)$ iterations, the distance of steps between two neighbouring configurations becomes 1. Now Boris can select two pieces of information copied to check whether they are right or whether the LOGSPACE computation in the last step read the symbol correctly out of the input word and so on. These checks can all be done in $\log^* n + \mathcal{O}(1)$ steps.

As yet, we have no characterisation of those problems in NP which are in $AAL[\mathcal{O}(\log^* n)]$ and we think that for each such problem it might depend heavily on the way the problem is formatted. The reason is that it may be difficult to even prove whether or not P is contained in $AAL[\mathcal{O}(\log^* n)]$, due to the following proposition. We will later show that the class $PAAL[\log^* n + \mathcal{O}(1)]$ which is obtained from $AAL[\log^* n + \mathcal{O}(1)]$ by starting with one additional step which generates a variable of polynomially sized length coincides with the polynomial hierarchy (PH). **Proposition 8.** Assume that f is monotonically increasing and computed in PSPACE and there is a polynomial p with $f(n) \leq p(n)$ for all n. Then $AAL[f(n)] \subseteq DSPACE[\mathcal{O}(f(n) \cdot (f(n) + n)] \subseteq DSPACE[\mathcal{O}((n + f(n)) \cdot f(n))] \subseteq DSPACE[\mathcal{O}((n + p(n)) \cdot p(n))] \subset PSPACE$ and $P \subseteq AAL[f(n) + \mathcal{O}(1)]$ implies $P \subset PSPACE$.

Proof. This result follows from Theorem 3 (the condition $f(n) \ge n$ is not necessary for the first inclusion relation to hold) and the space hierarchy theorem [19, Corollary 9.4].

4 Polynomial-Size Padded Alternating Automatic Register Machine

An AARM is constrained by the use of *bounded* automatic relations during each computation step. This is a real limitation: it can be shown that for any $f(n) = \Omega(\log \log n)$, the class of languages recognised in time $\mathcal{O}(f(n))$ by alternating automatic register machines that use *unbounded* automatic relations contains DSPACE $\left[\mathcal{O}(2^{2^{\mathcal{O}(f(n))}})\right]$ [16], and so by Theorem 3 and the space hierarchy theorem, this class properly contains AAL $[\mathcal{O}(f(n))]$. In fact, the exponential time hierarchy coincides with the class of languages recognised by AARMs using unbounded automatic relations in $\log^* n + \mathcal{O}(1)$ steps.

We study the effect of allowing a polynomial-size padding to the input of an Alternating Automatic Register Machine on its time complexity; this new model of computation will be called a Polynomial-Size Padded Bounded Alternating Automatic Register Machine (PAARM). The additional feature of a polynomial-size padding will sometimes be referred to informally as a "booster" step of the PAARM. Intuitively, padding the input before the start of a computation allows a larger amount of information to be packed into the register's contents during a computation history. We show two contrasting results: on the one hand, even a booster step does not allow an PAARM with time complexity $\mathcal{O}(1)$ to recognise non-regular languages; on the other hand, the class of languages recognised by PAARMs in time $\log^* n + \mathcal{O}(1)$ coincides with the polynomial hierarchy.

Formally, a Polynomial-Size Padded Bounded Alternating Automatic Register Machine (PAARM) M is represented as a quintuple $(\Gamma, \Sigma, A, B, p)$, where Γ is the register alphabet, Σ the input alphabet, A and B are two finite sets of instructions and p is a polynomial. As with an AARM, the register R initially contains an input string over Σ , and R's contents may be changed in response to an instruction, $J \subseteq \Gamma^* \times \Gamma^*$ which is a bounded automatic relation. A computation history of a PAARM with input w for any $w \in \Sigma^*$ is defined in the same way that was done for an AARM, except that the initial configuration is (ℓ, x, wv) for some $I_{\ell} \in A$, some $x, v \in \Gamma^*$, $(x, wv) \in I_{\ell}$, where $v = @^k$ for a special symbol $@ \in \Gamma - \Sigma$ and $k \ge p(|w|)$. Think of $@^k$ as padding of the input. Anke's and Boris' strategies, denoted by \mathcal{A} and \mathcal{B} respectively, are defined as before. For any $u \in \Gamma^*$, a winning strategy for Anke with respect to (M, u) is also defined as before. Given any $w \in \Sigma^*$, M accepts w if for every $v \in @^*$, with $|v| \ge p(|w|)$, Anke has a winning strategy with respect to (M, wv). Similarly, M rejects w if for every $v \in @^*$, with $|v| \ge p(|w|)$, Boris has a winning strategy with respect to (M, wv). Note that the winning strategies need to be there for every long enough padding. If Anke and Boris do not satisfy the above properties, then (A, B) is not a valid pair.

Definition 9. (Polynomial-Size Padded Bounded Alternating Automatic Register Machine Complexity). Let $M = (\Gamma, \Sigma, A, B, p)$ be a PAARM and let $t \in \mathbb{N}_0$. For each $w \in \Sigma^*$, M accepts w in time t if for every $v = @^k$, where $k \ge p(|w|)$ and $@ \in \Gamma - \Sigma$, Anke has a winning strategy \mathcal{A} with respect to (M, wv) and for any strategy \mathcal{B} played by Boris, the length of $\mathcal{H}(\mathcal{A}, \mathcal{B}, M, wv)$ is not more than t. For any function f, PAAL[f(n)] is defined analogously to AAL[f(n)].

Remark 10. Note that a PAARM-program can trivially simulate an AARMprogram by ignoring the generated padding; thus $AAL[\mathcal{O}(f(n))] \subseteq PAAL$ $[\mathcal{O}(f(n))]$. On the other hand, to simulate a booster step, an AARM-program needs $\mathcal{O}(p(n))$ steps as each bounded automatic relation step can only increase the length by a constant.

As with $AAL[\mathcal{O}(f(n))]$, the class $PAAL[\mathcal{O}(f(n))]$ is closed under the usual settheoretic Boolean operations as well as regular operations [9, Theorem 16]. Our main result concerning PAARMs is a characterisation of the polynomial hierarchy as the class $PAAL[\log^* n + \mathcal{O}(1)]$.

Theorem 11. $PH = PAAL[\log^* n + \mathcal{O}(1)].$

To help with the proof, we first extend the Log-Star Lemma as follows. Recall that a *configuration* (or *instantaneous description*) of a Turing Machine is represented by a string xqw, where q is the current state of the machine and x and w are strings over the tape alphabet, such that the current tape contents is xw and the current head location is the first symbol of w [12].

Lemma 12. Checking the validity of a Turing Machine step, i.e., whether a configuration of Turing Machine follows another configuration (given as input, separated by a special separator symbol) can be done in $AAL[\log^* n + O(1)]$, where n is the length of the shorter of the two configurations.

Proof. Let the input be the two configurations of the Turing Machine, where the second configuration is supposedly the successive step of the first one and separated by a separator symbol. Now there are two things that need to be checked: (1) The configuration is "copied" correctly from the previous step. Note that a valid Turing Machine transition will change only the cell on the tape head and/or both of its neighbour; thus "copied" here means the rest of the tape content should be the same; (2) The local Turing step is correct.

For the first checking, the player who wants to verify, e.g. Anke, will give the infinite valid marking as used in the Log-Star Lemma. In addition, Anke also marks the position of the old tape head on the second configuration. Boris can then challenge the following: (a) The Log-Star Lemma marking is not valid; (b) The old tape head position is not marked correctly (in the intended position) on the second configuration; (c) The string in a specified block differs, but not the symbols around the tape head; (d) The length difference of the configuration is not bounded by a constant.

Challenge (a) can be done in $\log^* n + \mathcal{O}(1)$ steps; this follows from the Log-Star Lemma. Challenge (b) can also be done in $\log^* n + \mathcal{O}(1)$ steps where both players reduce the block to focus on that position, and finally check whether it is on the same position or not. Challenge (c) can also be done in $\log^* n + \mathcal{O}(1)$ steps; this follows again from the Log-Star Lemma. Note that if Boris falsely challenges that the different symbol is around the tape head, Anke can counterchallenge by pointing out that at least one of its neighbours is a tape head. For challenge (d), note that a valid Turing Machine transition will only increase the length by at most one. Thus, Boris can pinpoint the last character of the shorter configuration and also its pair on another configuration, then check whether the longer one is only increased by up to one in length. This again can be done in $\log^* n + \mathcal{O}(1)$ steps.

For the second checking about the correctness of the Turing step, it can be done in a constant number of checks as a finite automaton can check the computation and determine whether the Turing steps are locally correct, that is, each state is the successor state of the previous steps head position and the symbol to the left or right of the new head position is the symbol following from the transition to replace the old symbol and so on. Therefore, all-in-all the validity of a Turing Machine step can be checked in AAL[log* n + O(1)] steps.

Proof Sketch of Theorem 11. We first prove that $PAAL[log^* n + \mathcal{O}(1)] \subseteq PH$. Define a binary function Tower recursively as follows:

Tower
$$(0, c) = 1$$

Tower $(d + 1, c) = 2^{c \cdot \text{Tower}(d, c)}$.

We prove by induction that for each $c \geq 1$, there is a c' such that for all d, Tower(d+c', 1) >Tower(d, c). When c = 1, Tower(d, c) gives the usual definition of the tower function. In particular, when c = 1, one has Tower(d + 1, c) >Tower(d, c) for all d, so the induction statement holds for all c = 1 and all d. Suppose that c > 1. Then there is some c' large enough so that Tower(c', 1) > $c^2 = c^2 \cdot$ Tower(0, c), and so the induction statement holds for d = 0. Assume by induction that c > 1 and that Tower $(c'' + d, 1) > c^2 \cdot$ Tower(d, c). Then $2^{\text{Tower}(c''+d,1)} > 2^{c^2 \cdot$ Tower $(d,c) \geq (2^{c \cdot$ Tower $(d,c))^c > c^2 \cdot 2^{c \cdot$ Tower $(d,c)}$, and therefore Tower $(c'' + d + 1, 1) > c^2 \cdot$ Tower(d + 1, c). This completes the induction step.

Suppose that c is the number of states of the automaton M corresponding to the update function for the configuration of an AAL algorithm. Then the size of the dfa to recognise whether or not a player wins within k steps is at most Tower(k + 3, c). We prove that a dfa of size Tower(k + 2, c) recognises whether Anke (resp. Boris) wins within k steps when she (resp. Boris) starts. (We can similarly show that a dfa of size Tower(k+2, c) recognises whether Boris (resp. Anke) wins within k steps when Anke (resp. Boris) starts, so the union of the two languages is recognised by a dfa of size at most Tower(k+3, c).) Anke wins in one step on input x iff for some y such that M accepts conv(y, x), for all y', M does not accept conv(y', y); the latter condition can be checked with a dfa of size 2^{2^c} . She wins in zero steps on input x when Boris starts iff there is no y such that M accepts (y, x), which can be checked with a dfa of size 2^c . So a dfa of size $2^{c+2^c} \leq \text{Tower}(3, c)$ checks whether Anke wins within 1 step. Assume inductively that there is a dfa M_k of size Tower(k+2, c) accepting x iff Anke wins within k steps on input x when Boris (resp. Anke) starts. Suppose it is Anke's turn to start and we need to check if she wins within k+1 steps. (A similar construction applies if it is Boris' turn.) Define an nfa N as follows. For each state p of M, make Tower(k + 2, c) states $(p, q_1), \ldots, (p, q_{\text{Tower}(k+2, c)}),$ where $q_1, \ldots, q_{\text{Tower}(k+2,c)}$ are the states of M_k . Then each state (p,q) on input x goes to each state (p', q') such that in M, there is a string y such that p on conv(y, x) goes to p' and in M_k , q on y goes to q'. The start state of N is (p_1, q_1) , where p_1 and q_1 are the start states of M and M_k respectively, and the final states of N are states (p_f, q_f) such that p_f and q_f are final states of M and M_k respectively. Then N accepts x iff there is a string y such that M accepts (y, x) and Anke wins within k steps on input y when Boris starts. The nfa N, which is of size $c \cdot \text{Tower}(k+2, c)$, can then be converted into a dfa M' of size $2^{c \cdot \text{Tower}(k+2,c)} = \text{Tower}(k+3,c)$, as required. By the preceding result on the function Tower, Tower(k+3, c) is bounded by Tower(k+c', 1) for some c'. Thus any language in PAAL[log* $n + \mathcal{O}(1)$] is recognised in a constant number of alternating steps plus a predicate that can be computed by a dfa of size Tower($\log^* n - 3, 1$). This dfa can be computed in LOGSPACE since $\log^* n$ can be computed in logarithmic space. Then one constructs the dfa by determinizing out the last step until it reaches size $\log \log n$. This happens only when only constantly many steps are missing by the above tower result. These constantly many steps can be left as a formula with alternating quantifiers followed by a dfa computed in logarithmic space of size $\log \log n$. Thus the formula whether Anke wins is in PH. Similarly for the formula whether Boris wins and so the overall decision procedure is in PH.

For the proof that $\operatorname{PH} \subseteq \operatorname{PAAL}[\log^* n + \mathcal{O}(1)]$, we first note that PH can be defined with alternating Turing machines [6]. We define Σ_k^P to be the class of languages recognised by alternating Turing Machine in polynomial time where the machine alternates between existential and universal states k times starting with existential state. We also define Π_k^P similarly but starting with universal state. PH is then defined as the union of all Σ_k^P and Π_k^P for all $k \ge 0$. We now show $\Sigma_k^P \cup \Pi_k^P \subseteq \operatorname{PAAL}[\log^* n + \mathcal{O}(1)]$ for any fixed constant k. As the alternating Turing Machine runs in polynomial time on each alternation, the full computation (i.e., sequence of configurations) in one single alternation can be captured non-deterministically in p(m) Turing Machine steps, for some polynomial p (which we assume to be bigger than linear), where m is the length of the configuration at the start of the alternation. In a PAARM-program, Anke first invokes a booster step to have a string of length at least $p^k(n)$. After that, Boris

and Anke will alternately guess the full computation of the algorithm of length $p(p^i(n)), i = 0, 1, \ldots$ in their respective alternation: Boris guesses the first p(n)computations (the first alternation), Anke then guesses the next p(p(n)) computations on top of it (the second alternation), etc. In addition, they also mark the position of the read head and symbol it looks upon in each step. Ideally, the PAARM-program will take k alternating steps to complete the overall algorithm. Note that a PAARM can keep multiple variables in the register by using convolution, as long as the number of variables is a constant. Thus, we could store the k computations in k variables: v_1, v_2, \cdots, v_k . Now each player can have the following choices of challenges to what the other player did: (1) Copied some symbol wrongly from the input i.e. in v_1 ; (2) Two successive Turing Machine steps in the computation are not valid (at some v_i); (3) The last Turing Machine step on some computation (at some v_i) does not follow-up with the first Turing Machine step on the next computation (at v_{i+1}). All the above challenges can be done in $\log^* n + \mathcal{O}(1)$ steps by a slight modification of Lemma 12. In particular, the third challenge needs one to compare the first Turing Machine configuration of v_{i+1} and the last Turing Machine configuration v_i , which can be done in a way similar to the proof of Lemma 12. Thus, $\Sigma_k^P \cup \Pi_k^P \subseteq \text{PAAL}[\log^* n + \mathcal{O}(1)]$ for every fixed constant k, therefore $PH \subseteq PAAL[\log^* n + \mathcal{O}(1)].$

Remark 13. As $PAAL[\log^* n + O(1)] = PH$, $PAAL[\log^* n + O(1)]$ is closed under polynomial time Turing reducibility. Similarly one can show that $PAAL[O(\log^* n)]$ is closed under polynomial time Turing reducibility. After Anke invokes the booster step, Boris will guess the accepting computation together with all of the oracle answers. Anke then can challenge Boris on either the validity of the computation (without challenging the oracle) or challenge one of the oracle answers. Both challenges can be done in the same fashion as in Theorem 11 but the latter needs one additional step to initiate the challenge of the oracle algorithm.

In order to obtain the next corollary, we use the fact that the problem of deciding TQBF_{f} – the class of true quantified Boolean formulas with $\log^* n + f(n) + \mathcal{O}(1)$ alternations – does not belong to any fixed level of the polynomial hierarchy (PH) when PH does not collapse.

Corollary 14. If PH does not collapse and f is a logspace computable increasing and unbounded function, then $AAL[\log^* n + f(n) + O(1)] \not\subseteq PH$.

Finally, we observe that if PH = PSPACE, then (i) by Theorem 11, PH = PAAL[$\mathcal{O}(\log^* n)$] = PSPACE; (ii) by Proposition 8, P $\not\subseteq$ AAL[$\mathcal{O}(\log^* n)$]; thus AAL[$\mathcal{O}(\log^* n)$] would be properly contained in PAAL[$\mathcal{O}(\log^* n)$].

Proposition 15. If PH = PSPACE and f satisfies the precondition of Proposition 8, then $AAL[f(n)] \subset PAAL[\log^* n + O(1)] = PSPACE$.

Theorem 16. If f is monotonically increasing and unbounded, then $AAL[\log^* n - f(n)] = REG$.

Proof. Assume that there is an AARM such that for each word w there is either for Anke or for Boris a winning strategy of $\log^* n - f(n)$ steps. Then by the tower lemma, the resulting size of the dfa is $\mathcal{O}(\log \log n)$ for almost all n and input words of length n. Thus the combined two dfas have at most size $poly(\log \log n)$ and there is no word w on which not exactly one accepts in the given time. Now assume that for a given dfa of sufficient large n, there is a word w where neither player succeeds in $\log^* n - f(n)$ rounds, where the n is fixed. Due to the pumping lemma, on words of arbitrary length with this property, one can pump down these words until they have size below n. However, such short words with this property do not exist by assumption. Thus for this fixed n, all words of arbitrary length are accepted by computations of length $\log^* n - f(n)$. Thus the language is actually in AAL[$\mathcal{O}(1)$] and in REG.

The main results on complexity classes defined by AARMs are summed up in Fig. 1 while those on complexity classes defined by PAARMs are summed up in Fig. 2. For any function f, AAL[f(n)] denotes the class of languages recognised by an AARM in f(n) time. An arrow is labelled with (a) reference(s) to the corresponding result(s) or definition(s) in the paper; folklore inclusions can be found in [12,19]. Results not stated in the present section are proven in [9]. Note that PSPACE = $\bigcup_k AAL[n^k]$ by Corollary 4.



Fig. 1. Relationships between complexity classes/CNF-SAT. A solid arrow from X to Y means that X is a proper subset of Y. A double-headed solid arrow between X and Y means that X is equal to Y. If X is a subset of Y but it is not known whether they are equal sets, then the arrow is dashed.



Fig. 2. Relationships between complexity classes.

References

- 1. Blumensath, A.: Automatic structures. Diploma thesis, RWTH Aachen University (1999)
- Blumensath, A., Grädel, E.: Automatic structures. In: Proceedings of IEEE Symposium on Logic in Computer Science (LICS), pp. 51–62 (2000)
- Bordihn, H., Fernau, H., Holzer, M., Manca, V., Martín-Vide, C.: Iterated sequential transducers as language generating devices. Theor. Comput. Sci. 369, 67–81 (2006)
- 4. Case, J., Jain, S., Seah, S., Stephan, F.: Automatic functions, linear time and learning. Log. Methods Comput. Sci. 9(3), (2013)
- Chandra, A., Kozen, D., Stockmeyer, L.: Alternation. J. Assoc. Comput. Mach. 28(1), 114–133 (1981)
- Chandra, A., Stockmeyer, L.: Alternation. In: 17th Annual Symposium on Foundations of Computer Science (FOCS 1976), pp. 98–108 (1976)
- 7. Floyd, R., Knuth, D.: Addition machines. SIAM J. Comput. 19, 329–340 (1990)
- 8. Fürer, M.: Alternation and the Ackermann case of the decision problem. L'Enseignement Mathématique II(XXVII), 137–162 (1981)
- Gao, Z., Jain, S., Li, Z., Sabili, A.F., Stephan, F.: Alternating automatic register machines. arXiv:2111.04254v5 [cs.CC] (2022). https://arxiv.org/pdf/2111. 04254v5.pdf
- 10. Hodgson, B.R.: Théories décidables par automate fini. Ph.D. thesis, Université de Montréal (1976)
- Hodgson, B.: Décidabilité par automate fini. Annales des sciences mathématiques du Québec 7, 39–57 (1983)
- Hopcroft, J., Ullman, J.: Introduction to Automata Theory, Languages, and Computation. Addison-Wesley, Maaschusetts (1979)
- Khoussainov, B., Minnes, M.: Three lectures on automatic structures. In: Proceedings of Logic Colloquium 2007. Lecture Notes in Logic, vol. 35, pp. 132–176 (2010)
- Khoussainov, B., Nerode, A.: Automatic presentations of structures. In: Leivant, D. (ed.) LCC 1994. LNCS, vol. 960, pp. 367–392. Springer, Heidelberg (1995). https://doi.org/10.1007/3-540-60178-3_93
- Kutrib, M., Malcher, A., Mereghetti, C., Palano, B.: Deterministic and nondeterministic iterated uniform finite-state transducers: computational and descriptional power. In: Anselmo, M., Della Vedova, G., Manea, F., Pauly, A. (eds.) CiE 2020. LNCS, vol. 12098, pp. 87–99. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-51466-2_8
- Li, Z.: Complexity of linear languages and its closures and exploring automatic functions as models of computation. Undergraduate Research Opportunities Programme (UROP) Project Report, National University of Singapore, 2018/2019
- 17. Lin, A.W., Rümmer, P.: Regular model checking revisited. Technical report (2020)
- Shepherdson, J.C., Sturgis, H.E.: Computability of recursive functions. J. Assoc. Comput. Mach. 10, 217–255 (1963)
- Sipser, M.: Introduction to the Theory of Computation, 3rd edn. Cengage Learning, Boston (2013)
- Stephan, F.: Automatic structures recent results and open questions. In: Third International Conference on Science and Engineering in Mathematics, Chemistry and Physics, vol. 622/1 (Paper 012013). J. Phys. Conf. Ser. (2015)
- 21. Stephan, F.: Methods and Theory of Automata and Languages. National University of Singapore, School of Computing (2016)