

Arbitrary Sequence RAMs

Michael Brand^a

^a*Faculty of IT, Monash University, Clayton, VIC 3800, Australia*

Abstract

It is known that in some cases a Random Access Machine (RAM) benefits from having an additional input that is an arbitrary number, satisfying only the criterion of being sufficiently large. This is known as the ARAM model. We introduce a new type of RAM, which we refer to as the Arbitrary Sequence RAM (ASRAM), that generalises the ARAM by allowing the generation of additional arbitrary large numbers at will during execution time. We characterise the power contribution of this ability under several RAM variants.

In particular, we demonstrate that an arithmetic ASRAM is more powerful than an arithmetic ARAM, that a sufficiently equipped ASRAM can recognise any language in the arithmetic hierarchy in constant time (and more, if it is given more time), and that, on the other hand, in some cases the ASRAM is no more powerful than its underlying RAM.

Keywords: Arbitrary number, Random Access Machine, arithmetic complexity

1. Introduction

The Random Access Machine, or RAM, (see [1] for a formal definition) is a computational model that affords all that we expect from a modern computer in terms of flow control (loops, conditional jump instructions, etc.) and access to variables (direct and indirect addressing). It is denoted by $\text{RAM}[op]$, where op is the set of operations that are assumed to be executable by the RAM in a single unit of time each. A comparator for equality is also assumed to be available, and this also executes in a single unit of time. The variables (or *registers*) of an integer RAM contain nonnegative integers and are also indexable by addresses that are nonnegative integers.

To discuss the power of RAMs, let us consider RAMs as calculating functions. We initialise the RAM by storing the input value, inp , in the RAM's $R[0]$ register (setting all other registers to zero), and the output of the function is taken to be the value of $R[0]$ at termination time. This definition can be extended to functions receiving any fixed number of inputs. Alternatively, RAMs can be discussed as language acceptors, where inp is taken to be in the language if and only if the return value is non-zero. Traditionally, when viewing the RAM as an acceptor, non-termination is taken to mean rejection of the input. By contrast, when viewing the RAM as a function calculator, non-termination is

Email address: michael.brand@alumni.weizmann.ac.il (Michael Brand)

usually taken to mean that the RAM calculates a partial function, rather than a function. The two frameworks can be unified by arbitrarily taking a non-terminating computation in a function-calculating RAM to yield an output of zero.¹

Ben-Amram and Galil [2] write “The RAM is intended to model what we are used to in conventional programming, idealized in order to be better accessible for theoretical study.” However, in practice, the RAM’s ability to manipulate very large numbers in constant time has been shown to reduce algorithmic complexities beyond what is usually considered “reasonable”. For example, it was shown regarding many RAMs working with fairly limited instruction sets that they are able to recognise any PSPACE problem in deterministic polynomial time [16, 7, 3, 14], and a unit-cost RAM equipped only with arithmetic operations, Boolean operations and bit shifts can, in fact, recognise in constant time any language that is recognised by a TM in time and/or space constrained by *any* elementary function of the input size [4].

In most cases (e.g., [11, 9, 12, 10, 17, 13]), the large integers to be efficiently manipulated by the RAM are generated to precise values that are conducive to the computation at hand. However, in other cases (e.g., [5, 8, 3]) some of the integers manipulated are arbitrary, subject only to the condition of being sufficiently large. We refer to such arbitrary large numbers as ALNs.

Recently, in [4], a general framework was proposed for the study of the power contribution of ALNs, this being the ARAM. An ARAM[*op*] program is defined by a RAM[*op*] program, r , in the following way. The ARAM is said to compute the function $\rho_A(inp)$ if r computes the function $\rho(inp, A)$, and for all inp

$$\forall^\infty A \rho(inp, A) = \rho_A(inp),$$

where \forall^∞ denotes “all but a finite number” (usually written as “almost all”). For the purpose of complexity calculations, the run-time associated with the ARAM is the worst-case run-time of r with the same inp over any possible choice of A (including the possibilities for which the results of ρ and of ρ_A differ). If the run-time for a given inp is unbounded, over the possible choices of A , the ARAM is said not to terminate.

We now introduce a new computational model which generalises the ARAM, this being the Arbitrary Sequence RAM (ASRAM). To define the ASRAM, let us first define the Arbitrary Large Sequence (ALS) set.

Definition 1 (ALS). An *Arbitrary Large Sequence (ALS) set* is a nonempty set of (infinite) integer sequences, \mathbf{S} , such that for any i and any sequence $\{A_k\} \in \mathbf{S}$ there exists a sequence $\{B_k\} \in \mathbf{S}$ such that $B_i = A_i + 1$, and if $j < i$, then $B_j = A_j$.

The definition of the ALS set is such that if any finite list of integers appears as a prefix of any sequence in \mathbf{S} , the last integer can be increased by 1 (and, by induction, can be

¹All RAMs discussed in this paper are guaranteed to terminate in finite time, so handling the case of non-termination is never an issue.

replaced by any larger number), and the result would still be a prefix of a sequence in \mathbf{S} . This being the case, any finite list of integers appearing as a prefix of any sequence in \mathbf{S} remains a prefix in \mathbf{S} if one extends it by another element, given that this element exceeds some threshold value. Other than being “large enough”, the new element can be chosen arbitrarily.

Definition 2 (ASRAM). An *ASRAM* is a computational model that provides the same functionality as the RAM, but also allows calls to a pseudofunction, “ $ALN()$ ”, that returns integers.

An ASRAM is said to compute the function $f(inp)$ if for each inp there exists an ALS set, \mathbf{S} , such that for any $\{A_i\} \in \mathbf{S}$, if the i 'th invocation of $ALN()$ is replaced by the constant A_i then the resulting RAM calculates $f(inp)$.

The run-time of the ASRAM on a given inp is the run-time of the underlying RAM with the worst-case choice of $\{A_i\}$. (The ASRAM is taken to be non-terminating if this worst-case is unbounded.)

This definition reflects a situation where every application of $ALN()$ returns a number that is arbitrary other than being sufficiently large with respect to everything that occurred in earlier steps of the ASRAM's execution.

The ASRAM can be used to investigate a scenario in which an unbounded number of ALNs are required. However, we can also use it for the intermediate scenario, where only a predefined number (e.g. 2) of ALNs are available to the algorithm. This is simply done by limiting the number of times the $ALN()$ pseudofunction can be executed. The original ARAM is an ASRAM limited to use $ALN()$ at most once.

2. Arithmetic complexity

At face value, one may believe that multiple arbitrary numbers are no more powerful than a single arbitrary number. However, this is not so.

In this section we show that the extra power of arbitrary sequences is present already in the traditional arithmetic complexity model, this being the computational model in which the basic operations used are the four arithmetic functions, $\{+, \dot{+}, \times, \div\}$, where $a \dot{+} b \stackrel{\text{def}}{=} \max(a + b, 0)$ and “ \div ” is integer division. We also use “mod” freely in the arithmetic model, because it is an operation straightforward to simulate using the available operations.

We stress that despite use of the name “arithmetic”, the results presented rely heavily on the non-arithmetic nature of “ \div ”. In the literature [8], this operation is, in fact, sometimes referred to as non-arithmetic division.

Formally stated, what we prove is the following theorem.

Theorem 1. *The class of functions that can be computed in polynomial time by an arithmetic ASRAM is strictly larger than the class of functions that can be computed in polynomial time by an arithmetic ARAM.*

Proof. Consider Algorithm 1. This algorithm utilises the fact that for an ALN, A , and a polynomial, P , the calculation $P(A) \bmod (A - x)$ is an algorithm for computing $P(x)$.² Utilising this property, the algorithm calculates each P_i so that it equals $A_i^{2^{2^{(x-i)}}}$. After $O(x)$ steps, it returns the value $2^{2^{2^x}}$.

Algorithm 1 An arithmetic ASRAM calculating $2^{2^{2^x}}$ in $O(x)$ time

```

1: for  $i \in 1, \dots, x$  do
2:    $A_i \leftarrow ALN()$ 
3: end for
4:  $P_x \leftarrow A_x \times A_x$ 
5: for  $i \in x - 1, \dots, 1$  do
6:    $temp \leftarrow P_{i+1} \bmod (A_{i+1} - A_i)$ 
7:    $P_i \leftarrow P_{i+1} \bmod (A_{i+1} - temp)$ 
8: end for
9:  $temp \leftarrow P_1 \bmod (A_1 - 2)$ 
10:  $rc \leftarrow P_1 \bmod (A_1 - temp)$ 
11: return  $rc$ 

```

From [5], we know that an ARAM $[+, \cdot, \times, \div]$ can only calculate 2^{2^x} in $\Omega(\sqrt{x})$ time. The fact that Algorithm 1 calculates it in $\Theta(\log x)$ time makes this an example that is polynomial for an ASRAM but not for an ARAM.³ \square

3. ASRAM $[+, \leftarrow, Bool]$

In the remaining sections we consider ASRAMs with instruction sets that are more powerful than the arithmetic operations. These include left shifting ($a \leftarrow b \stackrel{\text{def}}{=} a \times 2^b$) and bitwise Boolean operations. These ASRAMs will be investigated in terms of their abilities to accept languages (rather than to calculate functions). We use the notation $f(x)$ -RAM $[op]$ to denote the class of languages recognisable by a RAM $[op]$ in $f(x)$ time. (“RAM” can be replaced by “ARAM” or “ASRAM”.) For example, $O(1)$ -ARAM $[op]$ is the class of languages recognisable by an ARAM $[op]$ in constant time, whereas P-ASRAM $[op]$ is the class of languages recognisable by an ASRAM $[op]$ in polynomial time.

We begin by examining a case where ASRAMs afford no additional computational power.

Theorem 2. $P\text{-ASRAM}[+, \leftarrow, Bool] = PSPACE$, where $PSPACE$ is the class of languages recognisable by a Turing machine (TM) working on a tape of polynomial size.

²This is evident from the fact that in any ring, R , for any elements $x, y \in R$ and any polynomial P over R , the following holds: $x \equiv y \pmod{R} \Rightarrow P(x) \equiv P(y) \pmod{R}$.

³Though not appearing in this description, Algorithm 1 can be modified in a straightforward way to calculate 2^{2^x} for any x , and not just for x values that are powers of 2.

Both the RAM and ARAM working with the same operation set have been shown [18, 4] to be able to recognise PSPACE in polynomial time.

We remark that if it was known that the class of functions recognisable by ARAM[op] working under some time constraints equals the class of functions recognisable by a RAM[op] working under the same time constraints, then this result would have been directly also applicable to ASRAMs, by recursively reducing the number of ALNs required. However, [4] only proves that ALNs do not add power for ARAMs that are language recognisers. It is still possible that there are functions that can be calculated by an ARAM[$+, \leftarrow, Bool$] but not by a RAM[$+, \leftarrow, Bool$], and the availability of the pseudofunction “ALN()” may add more functions still. Theorem 2 shows that for this particular operation set, the fact that an ARAM does not recognise more languages than a RAM carries over also to ASRAMs. However, for results regarding language recognition, this is by no means known to hold for a general operation set.

Proof of Theorem 2. The proof is a direct extension of the proof of Theorem 4 in [4]. In the original proof, it was shown that a polytime ARAM with said operation set can be simulated by a PSPACE TM, given that a PSPACE TM can determine which is larger of a pair of expressions of the form $a\omega + b$, where a and b are known nonnegative integer constants and 2^ω is the ARAM’s ALN. Because ω is, by definition, “large enough”, the answer can be reached by simple lexicographical comparison.

In the ASRAM scenario, we begin by picking our ALNs, A_1, A_2, \dots so as to be powers of two: $2^{\omega_1}, 2^{\omega_2}, \dots$. We then simulate the ASRAM in exactly the same way as was done for the ARAM. Utilising exactly the same proof as that of Theorem 4 in [4], we conclude now that a polytime ASRAM with said operation set can be simulated by a PSPACE TM, given that a PSPACE TM can determine which is larger of a pair of expressions of the form $a_0 + \sum_{i=1}^k a_i \omega_i$, where both k and a_0, \dots, a_k are given nonnegative integers.

Once again, because each ω_i is, per assumption, large enough compared to all ω_j with $j < i$, a simple lexicographic comparison is enough to determine which of two formal expressions has the larger value.

Thus, the entire simulation of the ASRAM can be performed in PSPACE. \square

4. ASRAM[$+, /, \leftarrow, Bool$]

In this section we prove two theorems.

Theorem 3. $O(1)\text{-ASRAM}[+, /, \leftarrow, Bool] = AH$.

Theorem 4. $\omega(1)\text{-ASRAM}[+, /, \leftarrow, Bool] \supset AH$.

In the statements of Theorems 3 and 4, “/” is exact division (a weaker form of division, yielding the same results as integer division, but defined only when the division is without a remainder). AH refers to the entire arithmetic hierarchy, $\bigcup_{i=0}^{\infty} \Sigma_i^0 \cup \Pi_i^0$.

In order to prove the above, we utilise Theorem 5 of [4]:

Theorem 5 ([4]). *Any recursively enumerable (r.e.) set can be recognised in $O(1)$ time by an ARAM[+, /, \leftarrow , Bool].*

Proof of Theorem 3. Any ASRAM running k steps (and therefore utilising at most k ALNs, A_1, \dots, A_k) can be transformed into an equivalent ASRAM that first generates A_1, \dots, A_k and then performs any other computation. The part of the computation after the generation of the ALNs is a RAM computation. We consider this RAM as a language acceptor, and denote the predicate logically-equivalent to it $\phi(inp, A_1, \dots, A_k)$.

The function computed by the ASRAM is the value of ϕ for a sufficiently large A_k given a sufficiently large A_{k-1} , given a sufficiently large A_{k-2} , etc.. Technically, given an appropriate choice of A_1, \dots, A_{k-1} , we say that there exists some threshold, N_k , such that for any choice of A_k satisfying $A_k > N_k$, the value of $\phi(inp, A_1, \dots, A_k)$ is always the same, and it is taken to be the value of the ASRAM. In particular, the ASRAM accepts if and only if for any choice of threshold, N_k , there exists a value of A_k larger than the threshold for which $\phi(inp, A_1, \dots, A_k)$ is true.

This indicates that the predicate computed by the ASRAM can be formulated as

$$\forall N_1 \exists A_1 \forall N_2 \exists A_2 \dots \forall N_k \exists A_k (A_1 > N_1) \cap (A_2 > N_2) \cap \dots \cap (A_k > N_k) \cap \phi(inp, A_1, \dots, A_k).$$

Because ϕ is calculated by a RAM, it is known to be in Σ_1^0 , so the predicate computed by the ASRAM is, by definition, in Π_{2k}^0 .

We have thus established that the formula computed by the ASRAM is in AH. We now show that any formula, “ $\phi = \exists a_1 \forall a_2 \dots \exists a_k \chi(inp, a_1, \dots, a_k)$ ”, with any k quantifiers, can be computed by a constant time ASRAM with k ALNs. The way to do this is to bound every a_i except the last by an ALN A_i . The formula ϕ is logically equivalent to “ $\forall N_1 \exists A_1 \dots \forall N_{k-1} \exists A_{k-1} \exists (a_1 < A_1) \forall (a_2 < A_2) \dots \exists a_k$ such that $(A_1 > N_1) \cap \dots \cap (A_{k-1} > N_{k-1}) \cap \chi(inp, a_1, \dots, a_k)$ ”. (If an a_i exists to satisfy some condition, its value can be bounded by some A_i , whereas if something is true for every a_i , it will also be true for every bounded a_i .)

This derivation shows that any formula with k quantifiers can be computed as a formula with a single quantifier, given $k - 1$ ALNs.

We now make use of Theorem 5, which is equivalently stated as $O(1)$ -ARAM[+, /, \leftarrow , Bool] $\supseteq \Sigma_1^0$.

Note that an $O(1)$ -ARAM certainly terminates, and therefore its underlying RAM certainly terminates as well. This means that its return value can be inverted, making it accept a new language that is the complement of the original accepted language. The set of complements to Σ_1^0 is Π_1^0 , from which we can conclude that $O(1)$ -ARAM[+, /, \leftarrow , Bool] $\supseteq \Sigma_1^0 \cup \Pi_1^0$, this being the set of all formulae with a single quantifier.

We therefore first generate $k - 1$ ALNs, in a total of $O(k)$ time. Given the values of the $k - 1$ ALNs, the formula to be calculated is in $\Sigma_1^0 \cup \Pi_1^0$ (its one remaining unbounded quantifier being a_k), so we know it to be computable in an additional $O(1)$ time by an ARAM, for which we now use the k 'th ALN. In total, the ASRAM runs in $O(k)$ -time.

Any formula in AH is on some level of the hierarchy. To simulate it, we fix k to be that level. Thus, the simulating ASRAM runs in $O(1)$ -time. \square

Corollary 5.1. *An ASRAM restricted to use only k ALNs (regardless of its time complexity) is equivalent to a formula on the $\Theta(k)$ -th level of the arithmetical hierarchy.*

Proof. This result is a direct corollary of the proof for Theorem 3, which shows that an ASRAM utilising k ALNs can compute any formula in $\Sigma_k^0 \cup \Pi_k^0$, and can be computed by a formula in Π_{2k}^0 . \square

Consider, now, what happens when the ASRAM (not restricted to any fixed number of ALNs), is allowed to run in $\omega(1)$ time.

Proof of Theorem 4. A well-known example of a function that is not in AH is “TRUTH”. This is a function that takes as input a formula, ψ , suitably encoded as an integer, and determines whether this formula is true or not.

The inability to describe TRUTH as a formula in AH is known as Tarski’s undefinability theorem [19]. It is a corollary of Gödel’s incompleteness theorem [6] and, in the formulation given above, is a direct result of Post’s theorem, stating that the arithmetical hierarchy does not collapse [see 15].

Consider, first, an ASRAM working in $\Theta(n)$ time, where $n = |inp|$ is the bit-length of its input, inp . As demonstrated in Theorem 3, such an ASRAM can compute, directly, any formula with $\Theta(n)$ quantifiers. Consider a formula, ψ , encoded in the straightforward manner as an integer with n bits. This formula will necessarily have $O(n)$ quantifiers, so a $\Theta(n)$ -time ASRAM (a linear-time ASRAM) can be used to compute its truth value. Hence, TRUTH is in $O(n)$ -ASRAM[+, /, \leftarrow , Bool].

To extend this result from $\Theta(n)$ -time execution to $\omega(1)$ -time execution, we note simply that the straightforward formula encoding used above may be, perhaps, the most efficient encoding possible, but is certainly not the only one. For example, it is possible to encode the statement less efficiently by re-encoding the original input number, inp , as $inp' = (2inp + 1) \times 2^T$. An arbitrary choice of T allows constant-time decoding of the original inp . However, because we measure complexity as a function of the bit-length of the input, $n' = |inp'|$, and because the procedure shown here artificially increases this bit-length by an arbitrarily-large value, $n - n' = T + 1$, choosing a large enough T effectively reduces the run-time complexity arbitrarily. For example, if T is chosen to be n^2 , we have $n' = \Theta(n^2)$, so the ASRAM’s run-time, which is still $\Theta(n)$, is merely $\Theta(\sqrt{n'})$ when considered as a function of the bit-length of its actual input, inp' . With an appropriate choice of T , the ASRAM’s execution time, though still $\Theta(n)$, can be taken to be as low as any $\omega(1)$ function of n' .

Tarski’s undefinability theorem is independent of the exact choice of encoding used to make the input formula, ψ , into a number. The new, tweaked TRUTH function must, therefore, also lie outside of AH.

Thus, an $\omega(1)$ -time ASRAM can compute functions that are outside of AH. \square

5. Conclusions and future work

We have fully characterised P-ASRAM[+, \leftarrow , Bool] and $O(1)$ -ASRAM[+, /, \leftarrow , Bool]. For $\omega(1)$ -ASRAM[+, /, \leftarrow , Bool], we have not provided a full characterisation, other than

stating that it is beyond AH, but perhaps this is the best characterisation one can hope for: stratification beyond AH is traditionally very coarse-grained. If anything, one can say that ASRAM complexity provides us with a new and effective tool for fine-grained stratification beyond AH.

Where future research appears most needed is regarding our result on the arithmetic ASRAM. We have shown that the ASRAM is a more powerful model than the ARAM under arithmetic complexity, but full quantification of this extra power is still an interesting open problem.

References

- [1] Alfred V. Aho, John E. Hopcroft, and Jeffrey D. Ullman. *The Design and Analysis of Computer Algorithms*. Addison-Wesley Publishing Co., Reading, Mass.-London-Amsterdam, 1975. Second printing, Addison-Wesley Series in Computer Science and Information Processing.
- [2] Amir M. Ben-Amram and Zvi Galil. On the power of the shift instruction. *Inf. Comput.*, 117:19–36, February 1995.
- [3] Alberto Bertoni, Giancarlo Mauri, and Nicoletta Sabadini. A characterization of the class of functions computable in polynomial time on random access machines. In *Proceedings of the Thirteenth Annual ACM Symposium on Theory of Computing, STOC '81*, pages 168–176, New York, NY, USA, 1981. ACM.
- [4] Michael Brand. Computing with and without arbitrary large numbers. In T.-H. Hubert Chan, Lap Chi Lau, and Luca Trevisan, editors, *Theory and Applications of Models of Computation, 10th International Conference, TAMC 2013, Hong Kong, China, May 20-22, 2013. Proceedings*, volume 7876 of *Lecture Notes in Computer Science*, pages 181–192. Springer, 2013.
- [5] Nader H. Bshouty, Yishay Mansour, Baruch Schieber, and Prasoon Tiwari. Fast exponentiation using the truncation operation. *Comput. Complexity*, 2(3):244–255, 1992.
- [6] Kurt Gödel. Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme, I. *Monatshefte für Mathematik und Physik*, 38:173–198, 1931.
- [7] Juris Hartmanis and Janos Simon. On the power of multiplication in random access machines. In *15th Annual Symposium on Switching and Automata Theory (1974)*, pages 13–23. IEEE Comput. Soc., Long Beach, Calif., 1974.
- [8] Katharina Lürwer-Brüggemeier and Martin Ziegler. On faster integer calculations using non-arithmetic primitives. In *Unconventional Computation*, volume 5204 of *Lecture Notes in Comput. Sci.*, pages 111–128. Springer, Berlin, 2008.

- [9] Yishay Mansour, Baruch Schieber, and Prasoon Tiwari. The complexity of approximating the square root. In *Proceedings of the 30th Annual Symposium on Foundations of Computer Science*, pages 325–330, Washington, DC, USA, 1989. IEEE Computer Society.
- [10] Yishay Mansour, Baruch Schieber, and Prasoon Tiwari. Lower bounds for computations with the floor operation. In *Automata, Languages and Programming (Stresa, 1989)*, volume 372 of *Lecture Notes in Comput. Sci.*, pages 559–573. Springer, Berlin, 1989.
- [11] Yishay Mansour, Baruch Schieber, and Prasoon Tiwari. A lower bound for integer greatest common divisor computations. *J. Assoc. Comput. Mach.*, 38(2):453–471, 1991.
- [12] Yishay Mansour, Baruch Schieber, and Prasoon Tiwari. Lower bounds for computations with the floor operation. *SIAM J. Comput.*, 20(2):315–327, 1991.
- [13] W. Paul and J. Simon. Decision trees and random access machines. In *Logic and Algorithmic (Zurich, 1980)*, volume 30 of *Monograph. Enseign. Math.*, pages 331–340. Univ. Genève, Geneva, 1982.
- [14] Vaughan R. Pratt, Michael O. Rabin, and Larry J. Stockmeyer. A characterization of the power of vector machines. In *Sixth Annual ACM Symposium on Theory of Computing (Seattle, Wash., 1974)*, pages 122–134. Assoc. Comput. Mach., New York, 1974.
- [15] Hartley Rogers, Jr. *Theory of Recursive Functions and Effective Computability*. MIT Press, Cambridge, MA, second edition, 1987.
- [16] Arnold Schönhage. On the power of random access machines. In *Automata, Languages and Programming (Sixth Colloq., Graz, 1979)*, volume 71 of *Lecture Notes in Comput. Sci.*, pages 520–529. Springer, Berlin, 1979.
- [17] Adi Shamir. Factoring numbers in $O(\log n)$ arithmetic steps. *Inform. Process. Lett.*, 8(1):28–31, 1979.
- [18] Janos Simon. Division in idealized unit cost RAMs. *J. Comput. System Sci.*, 22(3):421–441, 1981. Special issue dedicated to Michael Machtey.
- [19] Alfred Tarski. On undecidable statements in enlarged systems of logic and the concept of truth. *J. Symbolic Logic*, 4:105–112, 1939.