Upper Bounds on the Automata Size for Integer and Mixed Real and Integer Linear Arithmetic*

Jochen Eisinger

Albert-Ludwigs-Universität Freiburg, Germany
eisinger@informatik.uni-freiburg.de

Abstract. Automata-based decision procedures have proved to be a particularly useful tool for infinite-state model checking, where automata are used to represent sets of real and integer values. However, not all theoretical aspects of these decision procedures are completely understood. We establish triple exponential upper bounds on the automata size for $\mathrm{FO}(\mathbb{Z}, +, <)$ and $\mathrm{FO}(\mathbb{R}, Z, +, <)$. While a similar bound for Presburger Arithmetic, i.e., $\mathrm{FO}(\mathbb{Z}, +, <)$ was obtained earlier using a quantifier elimination based approach, the bound for $\mathrm{FO}(\mathbb{R}, Z, +, <)$ is novel. We define two graded back-and-forth systems, and use them to derive bounds on the automata size by establishing a connection between those systems and languages that can be described by formulas in the respective logics. With these upper bounds that match the known lower bounds, the theoretical background for automata-based decision procedures for linear arithmetics becomes more complete.

1 Introduction

Automata-theoretic methods have long been a useful mathematical tool to understand the decidability of various logics. Büchi observed, in the 1960s, that automata over finite and infinite words can be used to study arithmetical theories [6, 5]. In addition to being a theoretical tool, automata-based methods are increasingly employed as the basis for implementations of decision procedures. An important example of such a decision procedure is Presburger Arithmetic, i.e., $\mathrm{FO}(\mathbb{Z}, +, <)$, which can be decided using deterministic finite automata (DFA) [4]. The elements of the domain are represented by finite words and for a given formula, and an automaton is constructed recursively over the formula structure that accepts precisely the words that represent the integers that satisfy the formula. A similar approach works for mixed real and linear arithmetic, i.e., $\mathrm{FO}(\mathbb{R}, Z, +, <)$, which can be decided using weak deterministic Büchi automata (WDBA) [3]. To represent reals, one uses infinite words. Note that

* This work was supported by the Deutsche Forschungsgemeinschaft (German Research Foundation).

WDBAs can be handled algorithmically almost as efficient as DFA, i.e., they can be efficiently complemented and minimized [18].

Although there exist efficient implementations of these automata-based decision procedures [8, 2, 17], many research questions are still only partially answered. Such questions regard an upper bound on the size of the automata for deciding $\mathrm{FO}(\mathbb{R}, Z, +, <)$. For instance, the results presented in [10], where certain systematical redundancies in WDBAs are exploited to decrease the automata sizes, suggest that the automata-based decision procedure for $\mathrm{FO}(\mathbb{R}, Z, +, <)$ might not be optimal. A naive analysis of the size of the automata yields one exponent for each nested negation. In contrast, Fischer and Rabin established in [12] a lower bound for any decision procedure for $\mathrm{FO}(\mathbb{R}, Z, +, <)$ [12], namely double exponential in non-deterministic time.

In this paper, we establish two tight upper bounds, first on the size of a minimal DFA for deciding $\mathrm{FO}(\mathbb{Z}, +, <)$, and second on the size of a minimal WDBA for deciding $\mathrm{FO}(\mathbb{R}, Z, +, <)$. We employ a method recently developed by Klaedtke to establish an upper bound on the automata size for $\mathrm{FO}(\mathbb{R}, +, <)$ [15]. Roughly speaking, the states of a minimal automaton for a formula are related to equivalence classes of an appropriately chosen refinement of the equivalence relation defined by Ehrenfeucht-Fraissé games. Such refinements are called *graded back-and-forth systems* or sometimes Ehrenfeucht-Fraissé relations [13, 11]. It is often easier to reason about such a refinement, and to show an upper bound on the index of these relations and therefore on the index of the equivalence relation defined by Ehrenfeucht-Fraissé games.

We first define two graded back-and-forth systems for $\mathrm{FO}(\mathbb{Z}, +, <)$ and $\mathrm{FO}(\mathbb{R}, Z, +, <)$, which characterize sets of integers and reals, respectively, that can be expressed using integer and mixed real and integer linear arithmetic. These systems are parameterized by the dimension of the sets and the quantifier rank of the formulas. Upper bounds on the indices of the equivalence relations of the graded back-and-forth systems are proved. In the second part of this paper, we then show that these graded back-and-forth systems can be used to refine the Nerode congruence relation on words. By this, we yield upper bounds on the size of the minimal DFA for deciding $\mathrm{FO}(\mathbb{Z}, +, <)$ and the minimal WDBA for deciding $\mathrm{FO}(\mathbb{R}, Z, +, <)$. The triple exponential upper bounds given here match the known lower bounds for [14, 12], and thus make the theoretical picture for those automata-based decision procedures more complete.

Related to this work is the result by Klaedtke [15], where a double exponential upper bound on the size of a minimal WDBA for deciding

FO($\mathbb{R}, +, <$) is established. We use this result and combine it with our result for FO($\mathbb{Z}, +, <$) to establish an upper bound for FO($\mathbb{R}, Z, +, <$). From an implementation point of view, the difference between an automata-based decision procedure for FO($\mathbb{R}, +, <$) and FO($\mathbb{R}, Z, +, <$) is minimal, since no algorithms tailored for FO($\mathbb{R}, +, <$) are known. Therefore, existing implementations only support the more general theory FO($\mathbb{R}, Z, +, <$) [2, 17]. Also related to this is the work by Klaedtke [14], where a triple exponential bound on the size of a minimal DFA for deciding FO($\mathbb{Z}, +, <$) is established. In contrast to our approach, this bound is established by quantifier elimination. The quantifier elimination approach relies on a specific quantifier elimination procedure, and several upper bounds for quantifier-free formulas. Note that FO($\mathbb{Z}, +, <$) does not admit quantifier elimination directly but needs to be augmented with divisibility predicates and constant symbols. On the other hand, our approach is more direct and independent of how the DFA is actually constructed. While the resulting bound is identical in both cases, our approach allows for a straight-forward adoption of the results for showing an upper bound for FO($\mathbb{R}, Z, +, <$).

The rest of the paper is structured as follows. In section 2, we recall preliminaries and basic definitions. In section 3, we define equivalence relations on tuples of reals and integers, which are then (section 4 and section 5) used to establish upper bounds on the automata size for integer linear arithmetic and mixed real and integer linear arithmetic respectively. Finally, in section 6 we summarize our results and draw conclusions. Proof details can be found in the appendix.

2 Preliminaries

We assume that the reader is familiar with logic and automata theory. For the sake of completeness and to fix notation, we state basic definitions and well-known facts from these areas.

2.1 Words and Languages

Let Σ be an alphabet. We denote the set of all finite words over Σ by Σ^* and by Σ^+ the set $\Sigma^* \setminus \{\varepsilon\}$, where ε is the empty word. Σ^ω is the set of all ω-words over Σ. The *concatenation* of words is written as juxtaposition. We write $|u|$ for the *length* of $u \in \Sigma^*$. We often write a word $u \in \Sigma^*$ of length $\ell \geq 0$ as $u(0) \dots u(\ell-1)$ and an ω-word $\gamma \in \Sigma^\omega$ as $\gamma(0)\gamma(1)\gamma(2)\dots$, where $u(i)$ and $\gamma(i)$ denote the $(i+1)$th letter of u and γ, respectively.

For $L \subseteq \Sigma^*$, we define the (*Nerode*) congruence relation $\sim_L$ on $\Sigma^* \times \Sigma^*$ as $u \sim_L v$ iff $uw \in L \Leftrightarrow vw \in L$, for all $w \in \Sigma^*$. For ω-languages, the congruence relation $\sim_L$ is defined analogously.

Additional notation. Let $r \geq 1$ and $1 \leq i \leq r$. We denote the ith component of $b \in \Sigma^r$ by $b_{\restriction i}$ and we write $u_{\restriction i}$ for the ith *track* of $u \in (\Sigma^r)^*$, i.e., $u_{\restriction i}$ is the word $v \in (\Sigma)^*$ defined as $v(j) = u_{\restriction i}(j)$ for $0 \leq j < |u|$. We use the same notation for ω-words.

2.2 First-order Logic

We define first-order logic as usual and assume familiarity with the basic notions of signatures and first-order formulas (see e.g. [9]). In the following, we restrict ourselves to relational signatures, i.e., signatures without function symbols and constants.

We write $\varphi(x_1, \dots, x_r)$ for a formula φ with free variables from $x_1, \dots, x_r$. The *quantifier rank* of a formula φ is denoted as $\mathrm{qr}(\varphi)$. A first-order structure $\mathfrak{A}$ over a relational signature defines a domain $\mathrm{dom}(\mathfrak{A})$ and for each relation symbol of the signature with arity r, $\mathfrak{A}$ defines a relation over $\mathrm{dom}(\mathfrak{A})^r$. We use $\mathfrak{Z}$, $\mathfrak{R}$, and $\mathfrak{M}$ to denote the structures $(\mathbb{Z}, +, <)$, $(\mathbb{R}, +, <)$, and $(\mathbb{R}, Z, +, <)$, where $+$ is the ternary addition relation, $<$ is the binary order predicate over the integers and the reals respectively, and Z is an unary predicate such that $Z(x)$ is true iff x is an integer.

For $a_1, \dots, a_r \in \mathrm{dom}(\mathfrak{A})$ and a formula $\varphi(x_1, \dots, x_r)$, we write $\mathfrak{A} \models \varphi[a_1, \dots, a_r]$ if φ is satisfied in $\mathfrak{A}$ with x_i interpreted as a_i for all $1 \leq i \leq r$. We often write $\bar{x}$ and $\bar{a}$ for $x_1, \dots, x_r$ and $a_1, \dots, a_r$ when r is obvious from the context.

For $m, r \in \mathbb{N}$ and $\bar{a}, \bar{b} \in \mathrm{dom}(\mathfrak{A})^r$ we write $\bar{a} \equiv_m^r \bar{b}$ iff $\mathfrak{A} \models \varphi[\bar{a}] \Leftrightarrow \mathfrak{A} \models \varphi[\bar{b}]$ for all formulas $\varphi(x_1, \dots, x_r)$ with $\mathrm{qr}(\varphi) \leq m$. Note that $\equiv_m^r$ partitions $\mathrm{dom}(\mathfrak{A})^r$ such that the elements of an equivalence class cannot be distinguished by any formula of quantifier rank less than or equal to m. The equivalence classes of $\equiv_m^r$ can be game-theoretically characterized using so-called Ehrenfeucht-Fraissé games (see e.g. [13]). Since it is often difficult to reason about $\equiv_m^r$ directly, we will define relations that refine $\equiv_m^r$, and which are easier to reason about.

2.3 Representing Sets of Reals and Integers

In the remainder, let $\varrho \in \mathbb{N}$ with $\varrho > 1$ and $\Sigma = \{0, \dots, \varrho - 1\}$ be fixed. ϱ is called the *base*.

We will use the following well-known mapping from words and ω-words to reals [4], to define languages corresponding to sets of integers and reals. Note that this encoding of reals as words is based on the ϱ's complement, most significant bit first representation. In this representation, the first letter of a word determines the sign of the value. Also, the first letter can be repeated arbitrarily often, so that we can assume that for a vector of values, each track of the corresponding word has the same length, even if a single component could be encoded with less letters. The symbol $\star$ plays the role of a decimal point, separating the integer part from the fractional part. In the following, let $r \in \mathbb{N}$ with $r \geq 1$.

1. V_r denotes the set of all ω-words over the alphabet $\Sigma^r \cup \{\star\}$ of the form $u \star \gamma$, where $u \in (\Sigma^r)^+$ and $\gamma \in (\Sigma^r)^\omega$. The word u is called the integer part and γ the fractional part.
2. An ω-word $u \star \gamma \in \mathsf{V}_r$ represents the vector of reals with r components
$$\langle u \star \gamma \rangle = \sum_{0<i<|u|} \varrho^{|u|-i-1} \cdot u(i) + \sum_{i \geq 0} \varrho^{-i-1} \cdot \gamma(i) + \begin{cases} \bar{0} & \text{if } u(0) = \bar{0}, \\ -\varrho^{|u|-1} & \text{otherwise,} \end{cases}$$
where vector addition and scalar multiplication are componentwise.[1] For $u \in (\Sigma^r)^+$ and $u' \in (\Sigma^r)^*$, we define $\langle u \rangle = \langle u \star \bar{0}^\omega \rangle$ and $\langle u \star u' \rangle = \langle u \star u' \bar{0}^\omega \rangle$.
3. For a formula $\varphi(x_1, \ldots, x_r)$, we define $L(\varphi) = \{\gamma \in \mathsf{V}_r : \mathfrak{M} \models \varphi[\langle \gamma \rangle]\}$, and $L^*(\varphi) = \{u \in (\Sigma^r)^+ : \mathfrak{Z} \models \varphi[\langle u \rangle]\}$.

Additional notation. For $a \in \mathbb{R}$, $\lfloor a \rfloor$ denotes the largest integer that is less than or equal to a, $\lceil a \rceil$ denotes the smallest integer that is greater than or equal to a, and $\{a\}$ denotes the *fractional part* of a, i.e., $a - \lfloor a \rfloor$. We use the same notation for tuples of values where $\lfloor \cdot \rfloor$, $\lceil \cdot \rceil$, and $\{\cdot\}$ are applied componentwise.

3 Characterization of Sets Definable in Linear Arithmetic

In this section, we introduce three families of relations, which refine $\equiv_m^r$ on the structures $\mathfrak{Z}$, $\mathfrak{R}$, and $\mathfrak{M}$ respectively. Such relations are commonly known as *graded back-and-forth systems* or *Ehrenfeucht-Fraissé relations* [13, 11]. For $\mathfrak{Z}$, we define a family of relations which refine the relations used by Ferrante and Rackoff in [11], and for $\mathfrak{R}$, we will use the relations defined by Klaedtke in [15]. The latter is a refinement of the relations given by Kozen in [16]. With the refinements of $\equiv_m^r$ on the structure $\mathfrak{Z}$ and $\mathfrak{R}$, we can then define a family of relations on $\mathfrak{M}$.

In all three cases, the definitions of the relations closely resemble quantifier elimination methods for the respective structures [7, 21, 20].

[1] Note that we do not distinguish between vectors and tuples.

3.1 Integer Linear Arithmetic

We will define relations that equate tuples of integers that cannot be distinguished by linear functions with bounded coefficients. First, we define sets of possible coefficients. The definition of the coefficients is technical, but it is required to establish a tight upper bound on the indices of the relations. Roughly speaking, we allow only double exponential many integer values out of the set of integer values whose absolute value is triple-exponentially bounded in m. For an understanding of this paper, it is sufficient to consider the sets B_m defined in the following as the set of integer values whose absolute value is triply exponentially bounded in m. In this section, all formulas are over the structure $\mathfrak{Z}$.

For $m \in \mathbb{N}$, we inductively define the sets B_m as $B_0 = \{-2, -1, 0, 1, 2\}$, $B'_m = \{\delta v/v' : \delta = \mathrm{lcm}(B_m); v, v' \in B_m; v' \neq 0\}$, and $B_{m+1} = \{v + v' : v, v' \in B'_m\}$, where $\mathrm{lcm}(A)$ denotes the least positive common multiple of all non-zero members of $A \subseteq \mathbb{Z}$.

Next, we define sets of linear functions, where the coefficients are taken from the sets B_m.

For $r, m \in \mathbb{N}$, let B^r_m be the set of functions of the form $f(\bar{x}) = c_0 + \sum_{i=1}^{r} c_i x_i$, where $c_1, \ldots, c_r \in B_m$, $c_0 \in \mathbb{Z}$, and $|c_0| \leq (r+1)(\mathrm{lcm}(B_m))^2$. For a function $f \in B^r_m$ with $f(\bar{x}) = c_0 + \sum_{i=1}^{r} c_i x_i$, we use $f^*(\bar{x})$ to denote the function $f(\bar{x}) - c_0$. Note that also $f^* \in B^r_m$.

The difference between our definition and the definition given by Ferrante and Rackoff can be pin-pointed to the set of functions B^r_m, where Ferrante and Rackoff define a smaller bound for the constant element c_0 of a function, namely $|c_0| \leq (\mathrm{lcm}(B_m))^2$. Consequently, the family of relations defined here refines the family of relations given by Ferrante and Rackoff. We will need this refinement for Lemma 14 where we establish a connection between this family of relations and languages. This lemma would not hold when using the original definition.

Definition 1. *For $\bar{a}, \bar{b} \in \mathbb{Z}^r$ we define the equivalence relation E^r_m as*

$\bar{a} E^r_m \bar{b}$ *iff*

(1) $f(\bar{a}) \geq 0 \Leftrightarrow f(\bar{b}) \geq 0$ *for every function* $f \in B^r_m$*, and*

(2) $a_i = b_i \pmod{(\mathrm{lcm}(B_m))^2}$*, for all* $1 \leq i \leq r$.

Observe that E^r_{m+1} refines E^r_m. We will use this fact in the following without explicitely referencing it.

The next three lemmas state properties of the relations E^r_m. The first two lemmas state that E^r_m refines $\equiv^r_m$ on $\mathfrak{Z}$, while the third lemma establishes an upper bound on the index of E^r_m. Although our definition deviates from the one given by Ferrante and Rackoff, the proofs are similar. Details can be found in the appendix.

Lemma 2. *For $\bar{a}, \bar{b} \in \mathbb{Z}^r$ with $\bar{a} E^r_{m+1} \bar{b}$, it holds that for all $a_{r+1} \in \mathbb{Z}$ there is a $b_{r+1} \in \mathbb{Z}$ such that $(\bar{a}, a_{r+1}) E^{r+1}_m (\bar{b}, b_{r+1})$.*

Lemma 3. *For $m, r \in \mathbb{N}$, it holds that $\bar{a} E^r_m \bar{b}$ implies $\bar{a} \equiv^r_m \bar{b}$.*

Lemma 4. *There is a constant $c \in \mathbb{N}$ such that the index of E^r_m is bounded by $2^{2^{2^{c(m+r)}}}$.*

3.2 Real Linear Arithmetic

In this section, all formulas are over the structure $\mathfrak{R}$. Similar to the previous section, we will now introduce a family of relations F^r_m over the reals, as used by Klaedtke in [15]. Since divisibility cannot be expressed using first-order formulas over $\mathfrak{R}$, the relations F^r_m are only defined over the sign of certain functions with bounded coefficients.

For $r, m \in \mathbb{N}$, let C^r_m be the set of functions of the form $f(\bar{x}) = c_0 + \sum_{i=1}^{r} c_i x_i$, where $c_0, \ldots, c_r \in \mathbb{Z}$, $|c_0| \leq rm$, and $|c_i| \leq m$ for all $1 \leq i \leq r$.

Definition 5. *For $\bar{a}, \bar{b} \in \mathbb{R}^r$, we define the equivalence relation F^r_m as $\bar{a} F^r_m \bar{b}$ iff $f(\bar{a}) \geq 0 \Leftrightarrow f(\bar{b}) \geq 0$, for all $f \in C^r_m$.*

Next, we state properties of the relations F^r_m, which we will use later in our proofs. Due to space limitations we refer the reader to [15] for the proof details.

Lemma 6. *For $\bar{a}, \bar{b} \in \mathbb{R}^r$ with $\bar{a} F^r_{4m^2} \bar{b}$, it holds that for all $a_{r+1} \in \mathbb{R}$, there is a $b_{r+1} \in \mathbb{R}$ such that $(\bar{a}, a_{r+1}) F^{r+1}_m (\bar{b}, b_{r+1})$.*

Lemma 7. *For all $\bar{a}, \bar{b} \in \mathbb{R}^r$ it holds that $\bar{a} F^r_{2^{3 \cdot 2^m - 2}} \bar{b}$ implies $\bar{a} \equiv^r_m \bar{b}$.*

Lemma 8. *There is a constant $c \in \mathbb{N}$ such that the index of $F^r_{2^{2^m}}$ is bounded by $2^{2^{c(m+r)}}$.*

3.3 Mixed Real and Integer Linear Arithmetic

Using the relations defined in the previous two sections, we now define a family of relations Gm, n^r that refine $\equiv^r_m$ on $\mathfrak{M}$. Roughly speaking, $G^r_{m,n}$ relates two tuples of real values, if their integer parts are in the same equivalence class of E^r_m, and their fractional part are in the same equivalence class of F^r_n. Note that both $\mathfrak{Z}$ and $\mathfrak{R}$ can be interpreted in $\mathfrak{M}$. In this section, all formulas will be over the structure $\mathfrak{M}$.

Definition 9. *For $\bar{a}, \bar{b} \in \mathbb{R}^r$ we define the equivalence relation $G^r_{m,n}$ as*

$$\bar{a} G^r_{m,n} \bar{b} \text{ iff } \lfloor \bar{a} \rfloor E^r_m \lfloor \bar{b} \rfloor \text{ and } \{\bar{a}\} F^r_n \{\bar{b}\}.$$

The next lemmas state that this family of relations refines $\equiv^r_m$ on the structure $\mathfrak{M}$, and establish an upper bound on the index of $G^r_{m,n}$. We will use a standard technique from the field of model theory. First, we show that $G^r_{m,n}$ has the back-and-forth property.

Lemma 10. *For $\bar{a}, \bar{b} \in \mathbb{R}^r$ with $\bar{a} G^r_{m+1,4n^2} \bar{b}$, it holds that for all $a_{r+1} \in \mathbb{R}$, there is a $b_{r+1} \in \mathbb{R}$ with $(\bar{a}, a_{r+1}) G^{r+1}_{m,n} (\bar{b}, b_{r+1})$.*

Proof. Given $\bar{a}$, $\bar{b}$, and a_{r+1} with $\bar{a} G^r_{m+1,4n^2} \bar{b}$. Because $\bar{a} G^r_{m+1,4n^2} \bar{b}$ implies $\lfloor \bar{a} \rfloor E^r_{m+1} \lfloor \bar{b} \rfloor$, Lemma 2 states that for $\lfloor a_{r+1} \rfloor$ there is a $b'_{r+1} \in \mathbb{Z}$ such that $\lfloor \bar{a}, a_{r+1} \rfloor E^{r+1}_m \lfloor \bar{b}, b'_{r+1} \rfloor$ holds. Similarly, $\bar{a} G^r_{m+1,4n^2} \bar{b}$ implies $\{\bar{a}\} F^r_{4n^2} \{\bar{b}\}$, so from Lemma 6 it follows that for $\{a_{r+1}\}$, there is a $b''_{r+1} \in \mathbb{R}$ such that $\{\bar{a}, a_{r+1}\} F^{r+1}_n \{\bar{b}, b''_{r+1}\}$ holds.

Choose $b_{r+1} = b'_{r+1} + b''_{r+1}$, then for $(\bar{a}, a_{r+1}) G^{r+1}_{m,n} (\bar{b}, b_{r+1})$ it remains to show that $0 \leq \{a_{r+1}\} < 1$ implies $0 \leq b''_{r+1} < 1$. Note that the functions x_{r+1} and $-x_{r+1} + 1$ from C^{r+1}_n are both positive for $\{\bar{a}, a_{r+1}\}$, and so $\{\bar{a}, a_{r+1}\} F^{r+1}_n \{\bar{b}, b''_{r+1}\}$ implies $0 \leq b''_{r+1} < 1$. ☐

Next, we state that $G^r_{m,n}$ refines $\equiv^r_m$. by an inductive argument, using the back-and-forth property for the induction step.

Lemma 11. *For $m, r \in \mathbb{N}$, it holds that $G^r_{m,2^{3 \cdot 2^m - 2}}$ refines $\equiv^r_m$.*

Proof. Given $\bar{a}, \bar{b} \in \mathbb{R}^r$ with $\bar{a} G^r_{m,2^{3\cdot 2^m - 2}} \bar{b}$. We prove the claim by induction over $m \in \mathbb{N}$. For $m = 0$, it suffices to show that $\bar{a}$ and $\bar{b}$ satisfy the same atomic formulas, namely $x + y = z$, $x = y$, $x < z$, and $Z(x)$. Observe that $\bar{a} G^r_{0,2^{3\cdot 2^0 - 2}} \bar{b}$ implies both $\lfloor \bar{a} \rfloor E^r_0 \lfloor \bar{b} \rfloor$ and $\{\bar{a}\} F^r_{2^{3\cdot 2^0 - 2}} \{\bar{b}\}$ which refine $\equiv^r_0$ on $\mathfrak{Z}$ and $\mathfrak{R}$ respectively. It is easy to see that $a_i + a_j = a_k$ iff $b_i + b_j = b_k$ for all $1 \leq i, j, k \leq r$, and similar for $x = y$ and $x < y$. For $Z(x)$, observe that $\{a_i\} = 0$ iff $\{b_i\} = 0$ for all $1 \leq i \leq r$, otherwise there is a function $f \in C^r_{2^{2cm}}$ with $f(\bar{x}) = -x_i$ and $f(\{\bar{a}\}) = 0$ and $f(\{\bar{b}\}) < 0$ contradicting $\{\bar{a}\} F^r_{2^{3\cdot 2^0 - 2}} \{\bar{b}\}$. Therefore, $Z(a_i)$ iff $Z(b_i)$ holds for all $1 \leq i \leq r$.

Now assume that the claim is true for some $m \geq 0$. We have to show that $G^r_{m+1,2^{3\cdot 2^{m+1} - 2}}$ refines $\equiv^r_{m+1}$. Observe that all formulas φ with $\mathrm{qr}(\varphi) = m + 1$ are equivalent to a Boolean combination of formulas of the form $\exists x \psi$ with $\mathrm{qr}(\psi) \leq m$. So it suffices to show that $\mathfrak{M} \models \exists x \psi[\bar{a}]$ iff $\mathfrak{M} \models \exists x \psi[\bar{b}]$, where ψ is a formula with $\mathrm{qr}(\psi) \leq m$. For reasons of symmetry, it is enough to show one direction. Assume $\mathfrak{M} \models \exists x\psi[\bar{a}]$, then there is a $a_{r+1} \in \mathbb{R}$ such that $\mathfrak{M} \models \psi[\bar{a}, a_{r+1}]$.

Assume that $\bar{a} G^r_{m+1,2^{3\cdot 2^{m+1}-2}} \bar{b}$. Since $4(2^{3\cdot 2^m-2})^2 = 2^{3\cdot 2^{m+1}-2}$, from Lemma 10, we can conclude that there is a $b_{r+1} \in \mathbb{R}$ such that $(\bar{a}, a_{r+1}) G^{r+1}_{m,2^{3\cdot 2^m-2}} (\bar{b}, b_{r+1})$. By the induction hypothesis, it follows that $\mathfrak{M} \models \psi[\bar{b}, b_{r+1}]$, and therefore $\mathfrak{M} \models \exists x\psi[\bar{b}]$. □

Finally, we establish an upper bound on the index of $G^r_{m,n}$.

Lemma 12. *There is a constant $c \in \mathbb{N}$ such that the index of $G^r_{m,2^{2m}}$ is bounded by $2^{2^{2^{c(m+r)}}}$.*

Proof. The index of $G^r_{m,2^{2m}}$ is bounded by the product of the upper bounds on the index of E^r_m and $F^r_{2^{2m}}$, so with Lemmas 4 and 8, there is a constant c such that the claimed bound holds. □

4 Integer Linear Arithmetic

In this section, we establish a connection between the relations E^r_m defined in Definition 1 and the Nerode relation $\sim_{L^*_\varphi}$ for first-order formulas φ over the structure $\mathfrak{Z}$. We achieve this by showing that E^r_m has certain congruence properties with regard to word concatenation. This property is the heart of our proof for an upper bound to the index of the Nerode relation of a given language, and under the assumption that Lemma 14 has been shown, it is easy to see that the following theorem holds.

Theorem 13. *Let $\varphi(x_1, \ldots, x_r)$ be a formula with $\mathrm{qr}(\varphi) \leq m$. There is a constant $c \in \mathbb{N}$ such that the index of $\sim_{L^*_\varphi}$ is at most $2^{2^{2^{cn}}}$, where n is the size of φ, i.e., the number of symbols in φ.*

This theorem follows immediately from the definition of the Nerode relation, the upper bound on the index of E^r_m in Lemma 4, and the following lemma.

Lemma 14. *For $u, v \in (\Sigma^r)^+$, if $\langle u\rangle E^r_m \langle v\rangle$, then $\langle uw\rangle E^r_m \langle vw\rangle$ for all $w \in (\Sigma^r)^*$.*

Proof. Recall that for a linear function f, the linear function f^* is defined as $f^*(\bar{x}) = f(\bar{x}) - f(\bar{0})$. We will use the two facts that for $u \in (\Sigma^r)^+$,

$w \in (\Sigma^r)^*$, and for any integer linear function f, in particular for $f \in B^r_m$, the following holds:

$$\langle uw\rangle = \langle u\rangle \varrho^{|w|} + \langle \bar{0}w\rangle \text{ and}$$
$$f(\langle uw\rangle) = f(\bar{0}) + f^*(\langle u\rangle)\varrho^{|w|} + f^*(\langle \bar{0}w\rangle).$$

Assume that the claim is false, i.e., let $u, v \in (\Sigma^r)^+$ with $\langle u\rangle E^r_m \langle v\rangle$, and assume that there is a word $w \in (\Sigma^r)^*$ such that $\langle uw\rangle E^r_m \langle vw\rangle$ does not hold. Let $\delta = \mathrm{lcm}(B_m)$. Obviously, $\langle uw_i\rangle = \langle vw_i\rangle \pmod{\delta^2}$, so we can conclude that there exists a linear function $f \in B^r_m$ and either (1) $f(\langle uw\rangle) \geq 0$ and $f(\langle vw\rangle) < 0$ or (2) $f(\langle uw\rangle) < 0$ and $f(\langle vw\rangle) \geq 0$. Because (2) can be reduced to (1) with a function $g(\bar{x}) = -f(\bar{x})$, we will restrict ourselves to (1).

We will argue that $f^*(\langle u\rangle)\varrho^{|w|}$ and $f^*(\langle v\rangle)\varrho^{|w|}$ are large enough such that the addition of $f^*(\langle w\rangle)$ is negligible. Hence, if the sign of $f(\langle uw\rangle)$ and $f(\langle vw\rangle)$ is different, already the sign of $f(\langle u\rangle)$ and $f(\langle v\rangle)$ has to be different. But this is a contradiction to $\langle u\rangle E^r_m \langle v\rangle$.

We continue with the proof by establishing bounds on $f^*(\langle u\rangle)$, $f^*(\langle v\rangle)$ and $f^*(\langle w\rangle)$. Because the words u and v are in the same equivalence class of E^r_m, and $f^*(\langle u\rangle) \neq f^*(\langle v\rangle)$ holds, we can conclude that $|f^*(\langle u\rangle)|$ and $|f^*(\langle v\rangle)|$ are large. Indeed, we can assume that $|f^*(\langle u\rangle)|, |f^*(\langle v\rangle)| \geq (r+1)\delta^2$. If $|f^*(\langle u\rangle)| < (r+1)\delta^2$ or $|f^*(\langle v\rangle)| < (r+1)\delta^2$, then there is a function $g \in B^r_m$ that just shifts $f^*(x)$ by a value smaller than or equal to $(r+1)\delta^2$, such that $g(\langle u\rangle) \geq 0$ and $g(\langle v\rangle) < 0$. But this is a contradiction to $\langle u\rangle E^r_m \langle v\rangle$.

We can also find an upper bound for $|f^*(\langle \bar{0}w\rangle)|$, which is a sum of r products between a value from B_m, which is surely less or equal to δ^2, and a value which can be written in base ϱ with $|w|$ letters, so $|f^*(\langle \bar{0}w\rangle)| \leq r\delta^2(\varrho^{|w|} - 1)$.

With this, we can now continue our proof. There are two possible cases:

(i) $f^*(\langle u\rangle) \leq -(r+1)\delta^2$, but then $f(\langle uw\rangle) \leq (r+1)\delta^2 - (r+1)\delta^2\varrho^{|w|} + r\delta^2(\varrho^{|w|} - 1) < 0$, contradicting our assumption that $f(\langle uw\rangle) \geq 0$, and

(ii) $f^*(\langle u\rangle) \geq (r+1)\delta^2$, from which follows that $f^*(\langle v\rangle) \geq (r+1)\delta^2$ and we get a similar contradiction to $f(\langle vw\rangle) < 0$.

We have to conclude that such a linear function does not exist but $\langle uw\rangle E^r_m \langle vw\rangle$ is true for all $w \in (\Sigma^r)^*$. □

It becomes clear now, why we needed the finer graded back-and-forth system E^r_m. When using the original definition from Ferrante and Rackoff, we can only conclude that $|f^*(\langle u \rangle)|$ and $|f^*(\langle v \rangle)|$ are larger than δ^2, while the bound for $|f^*(\langle \bar{0}w \rangle)|$ also depends on r. Therefore, we defined B^r_m to include functions where the constant element c_0 is not bounded by δ^2 but by $(r+1)\delta^2$.

With this lemma at hand, it is clear that E^r_m refines the Nerode relation and hence that Theorem 13 holds. Note that for a non-trivial formula φ, the empty word is in its own equivalence class of the Nerode relation $\sim_{L^*_\varphi}$, but this does not affect our upper bound. Because for any formula φ, the language L^*_φ is regular, the equivalence classes of $\sim_{L^*_\varphi}$ determine the number of states of the minimal DFA accepting L^*_φ. Thus, Theorem 13 establishes a triple exponential bound with respect to the formula length on the number of states of the minimal DFA accepting L^*_φ.

Note that a similar result was already obtained by Klaedtke in [14] using a quantifier elimination approach. However, the structure $\mathfrak{Z}$ does not allow for quantifier elimination but needs to be augmented with divisibility predicates and constant symbols [7]. Therefore, the method presented there depends on the quantifier elimination method and relies on several other bounds both for the generated quantifier free formulas and automata accepting the languages defined by these formulas. On the other hand, the proof presented here is more direct and does not depend on the way the automaton is actually constructed from the formula. Also, we can reuse it to establish an upper bound on the automata size for deciding mixed linear integer and real arithmetic in the next section.

Also note that the upper bound on the automata size is tight, i.e., there exists a family of formulas φ_n such that the index of $\sim_{L^*_{\varphi_n}}$ is at least triple exponential in n [14].. These formulas are derived from the proof of a lower bound for any decision procedure for $\mathrm{FO}(\mathbb{Z},+,<)$ by Fischer and Rabin [12].

5 Mixed Linear Arithmetic

In this section, we will establish a connection between the relations $G^r_{m,n}$ and the relation $\sim_{L_\varphi}$ for first-order formulas φ over the structure $\mathfrak{M}$. While the general structure of this section is the same as for the previous section, the proofs are more involved. This has mainly two reasons.

First, the value encoded by a finite word $u \star u'$ with $u \in (\Sigma^r)^+$ and $u' \in (\Sigma^r)^*$ does not change when appending the letter $\bar{0}$. This means, the word $u \star u'$ and the words $u \star u'\bar{0}^+$ all encode a single value which in turn is member of a single equivalence class of $G^r_{m,n}$. However, when appending an ω-word $\gamma \in (\Sigma^r)^\omega$, the ω-words $u \star u'\gamma$ and $u \star u'\bar{0}^+\gamma$ might encode different real values. Obviously, these different values might be in different equivalence classes of $G^r_{m,n}$. They potentially encode different real values, because the fractional parts u' and $u'\bar{0}^+$ are of different length. Therefore, the letters of γ are encoding for digits at different positions of the fractional parts. In general, this problem occurs for all finite words $u \star u'$ and $v \star v'$ which encode real values in the same equivalence class of $G^r_{m,n}$, but u' and v' are of different length.

Second, we cannot treat the integer and the fractional part of a value encoded by an ω-word $u{\star}u'\gamma$ separately by just looking at $\langle u \rangle$ and $\langle \bar{0}{\star}u'\gamma \rangle$, since, e.g., the ω-word $\langle 0 \star (\varrho - 1)^\omega \rangle$ encodes the integer value 1. So when examining the fractional part of the values encoded by $u \star u'$ and $v \star v'$, we have to make sure that $u'_{\restriction i} \in (\varrho - 1)^*$ iff $v'_{\restriction i} \in (\varrho - 1)^*$ for $1 \leq i \leq r$. It is then the case that if the fractional part of a track in $u \star u'\gamma$ encodes 1, the fractional part of the same track in $v \star v'\gamma$ also encodes 1, and vice versa.

5.1 Relationship to Languages

Despite the two problems mentioned above, the following lemmas establish certain properties of $G^r_{m,n}$ with regard to word concatenation.

First, we recall a result for the family of relations F^r_m on $\mathfrak{R}$ from [15].

Lemma 15. *For $u, v \in (\Sigma^r)^+$ and $u', v' \in (\Sigma^r)^*$ the following fact holds. If $\langle u \star u' \rangle F^r_{2m} \langle v \star v' \rangle$ with $|u'| \geq |v'|$, then for all $\gamma \in (\Sigma^r)^\omega$, it holds that $\langle u \star u'\gamma \rangle F^r_m \langle v \star v'\bar{0}^k\gamma \rangle$ with $k = \min(\{|u'| - |v'|\} \cup \{k \in \mathbb{Z} : \varrho^k \geq rm\})$.*

Roughly speaking, this lemma states that, if two words $u{\star}u'$ and $v{\star}v'$ encode values that are in the same equivalence class of F^r_m, but u' and v' are of different length, we can extend the shorter one with zeros such that F^r_m has a congruence property with regard to word concatenation. We only need a bounded number of zeros. Because either after appending zeros to the shorter word, both words are that long that by appending an arbitrary ω-word, the change in the values encoded is negligible. Or, both words are of the same size after padding the shorter one with zeros.

With this result, and with Lemma 14, we can now proceed to show that $G^r_{m,n}$ also has a certain congruence property with regard to word concatenation. However, as mentioned earlier, this is not a direct result, since we cannot treat the integer part and the fractional part separately.

In the following, we will use the functions $\mathsf{D}(u) = \{i \in \mathbb{N} : 1 \leq i \leq r \text{ and } u_{\restriction i} \in (\varrho - 1)^*\}$ for $u \in (\Sigma^r)^*$, and $\mathsf{D}_\omega(\gamma) = \{i \in \mathbb{N} : 1 \leq 1 \leq r \text{ and } \gamma_{\restriction i} = (\varrho - 1)^\omega\}$ for $\gamma \in (\Sigma^r)^\omega$. We use these functions to identify tracks where the fractional part potentially encodes 1 instead of a strictly smaller value.

Lemma 16 states three properties of $G^r_{m,n}$ with regard to word concatenation, namely: (1) $G^r_{m,n}$ has the same properties as E^r_m for words without a fractional part; (2) $G^r_{m,n}$ has a similar property as F^r_n, if avoiding words which might result in the fractional part encoding for an integer value; And (3) $G^r_{m,n}$ has a congruence property with regard to word concatenation, if we restrict ourselves to words where the same tracks of the fractional part potentially encode the value 1.

Lemma 16. *For $u, v \in (\Sigma^r)^+$ and $u', v' \in (\Sigma^r)^*$, the following three facts hold.*

(i) If $\langle u\rangle G^r_{m,n}\langle v\rangle$ then for all $w \in (\Sigma^r)^*$ it holds that $\langle uw\rangle G^r_{m,n}\langle vw\rangle$.

(ii) If $\langle u \star u'\rangle G^r_{m,2n}\langle v \star v'\rangle$ with $|u'| \geq |v'|$, then for all $\gamma \in (\Sigma^r)^\omega$ with $\mathsf{D}_\omega(\gamma) \cap (\mathsf{D}(u') \cup \mathsf{D}(v')) = \emptyset$, it holds that $\langle u \star u'\gamma\rangle G^r_{m,n}\langle v \star v'\bar{0}^k\gamma\rangle$ with $k = \min(\{|u'| - |v'|\} \cup \{k \in \mathbb{Z} : \varrho^k \geq rn\})$.

(iii) If $\langle u \star u'\gamma\rangle G^r_{m+1,n}\langle v \star v'\gamma\rangle$ for all $\gamma \in (\Sigma^r)^\omega$ with $\mathsf{D}_\omega(\gamma) \cap (\mathsf{D}(u') \cup \mathsf{D}(v')) = \emptyset$, and $\mathsf{D}(u') = \mathsf{D}(v')$, then $\langle u \star u'\gamma\rangle G^r_{m,n}\langle v \star v'\gamma\rangle$ holds for all $\gamma \in (\Sigma^r)^\omega$.

Proof. (i) This follows directly from Lemma 14 and Definition 9.

(ii) The restriction $\mathsf{D}_\omega(\gamma) \cap (\mathsf{D}(u') \cup \mathsf{D}(v')) = \emptyset$ enforces that by appending γ to either $u \star u'$ or $v \star v'\bar{0}^k$, the integer value of the encoded values cannot change. Therefore, this property follows from Lemma 15 and Definition 9.

(iii) Let $\gamma \in (\Sigma^r)^\omega$ with $\mathsf{D}_\omega(\gamma) \cap (\mathsf{D}(u') \cup \mathsf{D}(v')) \neq \emptyset$, i.e., certain tracks of the words $\bar{0}\star u'\gamma$ and $\bar{0}\star v'\gamma$ encode the value 1. Since $\mathsf{D}(v') = \mathsf{D}(u')$, the integer value of the values encoded by the words $u\star u'$ and $v\star v'$ change by the same amount when appending γ. Therefore, we can proceed to proof the third property separately for the integer part and for the fractional part. Recall that $\bar{a}G^r_{m,n}\bar{b}$ is defined as $\lfloor\bar{a}\rfloor E^r_m\lfloor\bar{b}\rfloor$ and $\{\bar{a}\}F^r_n\{\bar{b}\}$.

First, we consider the integer part. Since E^r_{m+1} refines E^r_m, and the change in the integer part is bounded (at most r components are changed by 1), it is easy to show that $\lfloor\langle u \star u'\gamma\rangle\rfloor E^r_m\lfloor\langle v \star v'\gamma\rangle\rfloor$ holds.

For the fractional part, we can just ignore those tracks of $\bar{0} \star u'\gamma$ (and also those of $\bar{0} \star v'\gamma$) that encode (the integer value) 1. But then we can find an ω-word $\gamma' \in (\Sigma^r)^\omega$ such that $f(\{\langle u \star u'\gamma\rangle\}) = f(\{\langle u \star u'\gamma'\rangle\})$ for all $f \in C^r_n$ (and similar for $v \star v'$).

Together with the precondition of (iii), we can now conclude that $\langle u \star u'\gamma\rangle G^r_{m,n}\langle v \star v'\gamma\rangle$ holds for all $\gamma \in (\Sigma^r)^\omega$. ☐

5.2 Upper Bounds

Using the results from this and the previous section, we will establish an upper bound on the index of $\sim_{L_\varphi}$.

Theorem 17. *Let $\varphi(x_1, \ldots, x_r)$ be a formula with $\mathrm{qr}(\varphi) \leq m$. There is a constant $c \in \mathbb{N}$ such that the index of $\sim_{L_\varphi}$ is at most $2^{2^{2^{cn}}}$, where n is the size of φ, i.e., the number of symbols in φ.*

In contrast to the integer linear arithmetic case, $G^r_{m,n}$ does not directly refine $\sim_{L_\varphi}$. However, we can use $G^r_{m,n}$ to define a family of relations that refines $\sim_{L_\varphi}$ using the results established in the previous lemma. The general idea is as follows. We consider all words separately that encode values of a single equivalence class of $G^r_{m,n}$. Then we partition these words by their length using Lemma 16(ii). We partition these new classes again into words with similar fractional parts as in the precondition of Lemma 16(iii). Then, after refining $G^r_{m,n}$ twice, we find a partition that refines $\sim_{L_\varphi}$, and we can use the upper bound on the index of $G^r_{m,n}$ to deduce an upper bound on the index of $\sim_{L_\varphi}$.

Proof. We now define such an equivalence relation S^r_m on $(\Sigma^r)^* \times (\Sigma^r)^*$. For all $u, v \in (\Sigma^r)^+$ we define $uS^r_m v$ iff $\langle u \rangle G^r_{m+1,2^{2^{2m+2}+1}} \langle v \rangle$ (cf. Lemma 16(i)). The empty word ε is in its own equivalence class, and all words $u \in (\Sigma^r \cup \{\star\})^*$ with two or more occurrences of $\star$, or where $u(0) = \star$, i.e., words not encoding for a value, are in one equivalence class.

It remains to define the equivalence classes of S^r_m on the words $u \star u'$ with $u \in (\Sigma^r)^+$ and $u' \in (\Sigma^r)^*$. For such a word $u \star u'$ consider the set $X = \{v \star v' : \langle u \star u' \rangle G^r_{m+1,2^{2^{2m+2}+1}} \langle v \star v' \rangle\}$. Assume that $|u'| \leq |v'|$ for all $v \star v' \in X$. Then we partition X into classes Y_k (cf. Lemma 16(ii)) such that

- for $k \in \{0, \ldots, \lceil \log_\varrho r 2^{2^{2m+2}+1} \rceil - 1\}$
  let $Y_k = \{v \star v' : v \star v' \in X \wedge |u'| + k = |v'|\}$, and
- for $k = \lceil \log_\varrho r 2^{2^{2m+2}+1} \rceil$
  let $Y_k = \{v \star v' : v \star v' \in X \wedge |u'| + k \leq |v'|\}$.

S^r_m then refines this partition of X such that $u \star u' S^r_m v \star v'$ iff both $\mathsf{D}(u') = \mathsf{D}(v')$ and $u \star u', v \star v' \in Y_k$ for some k (cf. Lemma 16(iii)).

It follows immediately that for all $u, v \in (\Sigma^r)^+$ and $u', v' \in (\Sigma^r)^*$

(i) $uS^r_m v$ implies $u \sim_{L_\varphi} v$, and
(ii) $u \star u' S^r_m v \star v'$ implies $u \star u' \sim_{L_\varphi} v \star v'$.

It remains to show an upper bound on the index of S^r_m. We defined S^r_m to partition the equivalence classes of $G^r_{m+1,2^{2^{2m+2}+1}}$ into $\lceil \log_\varrho r 2^{2^{2m+2}+1} \rceil$ sets and each of these sets into 2^r classes. From Lemma 12, we know that the index of $G^r_{m+1,2^{2^{2m+2}+1}}$ is bounded by $2^{2^{2^{d(m+r)}}}$ for some constant $d \in \mathbb{N}$. Observe that $1 \leq m+r \leq n$. Hence, there is a constant $c \in \mathbb{N}$ such that the index of S^r_m is bounded by

$$2^{2^{2^{d(m+r)}}} \cdot \lceil \log_{\varrho} r 2^{2^{2m+2}+1} \rceil \cdot 2^r \leq 2^{2^{2^{dn}}} \cdot 2^{3+n} \cdot 2^n \leq 2^{2^{2^{cn}}}. \qquad \square$$

Note that for any formula φ, the language L_φ is in the Borel class $F_\sigma \cap G_\delta$ [3], which exactly captures the expressive power of weak deterministic Büchi automaton (WDBA) [19]. Therefore, the equivalence classes of $\sim_{L_\varphi}$ determine the number of states of the minimal WDBA accepting L_φ [18]. Thus, Theorem 17 establishes a triple exponential bound with respect to the formula length on the number of states of the minimal WDBA accepting L_φ. Note that the upper bound on the automata size is tight, i.e., there exists a family of formulas φ_n such that the index of $\sim_{L_{\varphi_n}}$ is at least triple exponential in n. This is the same family of formulas as for the structure $\mathfrak{Z}$, because $\mathfrak{Z}$ can be interpreted in $\mathfrak{M}$.

6 Conclusion

We have established a triple exponential bound on the size of the minimal deterministic finite automata for deciding $\mathrm{FO}(\mathbb{Z}, +, <)$ using a most significant bit first (MSB) encoding, and on the size of the minimal weak deterministic Büchi automata for deciding $\mathrm{FO}(\mathbb{R}, Z, +, <)$. We defined two graded back-and-forth systems and showed that the refine the equivalence relation defined by Ehrenfeucht-Fraissé games. By establishing certain congruence properties of these systems with regard to word concatenation, we could use them to derived these bounds. The relation between the graded back-and-forth systems and the languages describing sets of values definable in linear arithmetic allows for interesting insights into the structure of the automata. For instance when interpreting $\mathrm{FO}(\mathbb{Z}, +, <)$ in $\mathrm{FO}(\mathbb{R}, Z, +, <)$, the size of the minimal WDBA for a formula is exponentially in the number of variables larger than the size of a minimal DFA. This overhead, which also appears in the proof of the upper bound for $\mathrm{FO}(\mathbb{R}, Z, +, <)$, is due to the ambiguous encoding of real values as ω-words.

Both theories, integer linear arithmetic and mixed real and integer linear arithmetic, are prominent examples for automata-based decision procedures, and are implemented in several tools used in, e.g., infinite state-space model checkers [1–3]. Our results make the theoretical background for these approaches more complete. The question, whether it is possible to construct the minimal automaton for a given formula in time polynomial to the size of the resulting minimal automaton remains open.

As future work, we plan to investigate the automata-based approach to deciding $\mathrm{FO}(\mathbb{Z}, +, <)$ using the least significant bit first (LSB) encoding. To the best of our knowledge, no tight upper bounds are known for this case. Note that the family of relations E^r_m presented here does not refine the Nerode relation for the LSB encoding. Additionally, we plan to identify further redundancies in the encoding of sets of values as languages and try to leverage them to achieve asymptotically smaller automata, similar to the "don't care" language approach presented in [10].

Acknowledgements. The author thanks Bernd Becker, Felix Klaedtke, Moritz Müller, Stefan Wölfl, and the anonymous reviewers for their comments on earlier versions of this paper.

References

1. S. Bardin, A. Finkel, J. Leroux, and L. Petrucci, *FAST: Fast acceleration of symbolic transition systems*, in CAV'03, vol. 2725 of LNCS, 2003, pp. 118–121.
2. B. Becker, C. Dax, J. Eisinger, and F. Klaedtke, *LIRA: Handling constraints of linear arithmetics over the integers and the reals*, in CAV'07, vol. 4590 of LNCS, 2007, pp. 307–310.
3. B. Boigelot, S. Jodogne, and P. Wolper, *An effective decision procedure for linear arithmetic over the integers and reals*, ACM Trans. Comput. Log., 6 (2005), pp. 614–633.
4. B. Boigelot and P. Wolper, *Representing arithmetic constraints with finite automata: An overview*, in ICLP'02, vol. 2401 of LNCS, 2002, pp. 1–19.
5. J. Büchi, *Weak second-order arithmetic and finite automata*, Zeitschrift der mathematischen Logik und Grundlagen der Mathematik, 6 (1960), pp. 66–92.
6. ———, *On a decision method in restricted second order arithmetic*, in Logic, Methodology and Philosophy of Science (Proc. 1960 Internat. Congr.), Stanford University Press, 1962, pp. 1–11.
7. D. C. Cooper, *Theorem proving in arithmetic without multiplication*, in Proceedings of the 7th Annual Machine Intelligence Workshop, B. Meltzer and D. Michie, eds., Edinburgh University Press, 1972, pp. 91–100.
8. J.-M. Couvreur, *A BDD-like implementation of an automata package*, in CIAA'04, vol. 3317 of LNCS, 2004, pp. 310–311.
9. H.-D. Ebbinghaus, J. Flum, and W. Thomas, *Mathematical Logic*, Springer-Verlag, 2nd ed., 1994.
10. J. Eisinger and F. Klaedtke, *Don't care words with an application to the automata-based approach for real addition*, in CAV'06, vol. 4144 of LNCS, 2006, pp. 67–80.
11. J. Ferrante and C. Rackoff, *The Computational Complexity of Logical Theories*, vol. 718 of LNM, Springer-Verlag, 1979.

12. M. J. Fischer and M. O. Rabin, *Super-exponential complexity of presburger arithmetic*, tech. rep., Massachusetts Institute of Technology, Cambridge, MA, USA, 1974.
13. W. Hodges, *A shorter model theory*, Cambridge University Press, New York, 1997.
14. F. Klaedtke, *On the automata size for Presburger arithmetic*, in LICS'04, IEEE Computer Society Press, 2004, pp. 110–119.
15. ———, *Ehrenfeucht-Fraïssé goes automatic for real addition*, in STACS'08, IBFI Schloss Dagstuhl, 2008, pp. 445–456.
16. D. Kozen, *Theory of Computation*, Springer-Verlag, New York, 2006.
17. LASH, *The Liège Automata-based Symbolic Handler*. `http://www.montefiore.ulg.ac.be/~boigelot/research/lash/`.
18. C. Löding, *Efficient minimization of deterministic weak ω-automata*, Information Processing Letters, 79 (2001), pp. 105–109.
19. O. Maler and L. Staiger, *On syntactic congruences for omega-languages*, Theoretical Comput. Sci., 181 (1997), pp. 93–112.
20. V. Weispfenning, *Mixed real-integer linear quantifier elimination*, in ISSAC'99, ACM, 1999, pp. 129–136.
21. V. Weispfenning and R. Loos, *Applying linear quantifier elimination*, The Computer Journal, 36 (1993), pp. 450–462.

A Proof Details

In this appendix, we give details for the proofs of Lemmas 2-4, which are omitted in the main paper. For the proofs, we need to following facts from [11]. There is a constant $c \in \mathbb{N}$ such that

(i) the cardinality of B_m (denoted $|B_m|$) is bounded by $2^{2^{cm}}$, and
(ii) $\max B_m \leq 2^{2^{2^{cm}}}$.

Note that the cardinality of B_m is one exponent smaller than the size of its maximal element. This enables us to get a smaller upper bound for $\operatorname{lcm} B_m \leq \max B_m^{|B_m|}$. This is crucial for establishing a triple exponential bound on the index of E_m^r. Hodges defines in [13] another graded back-and-forth system refining $\equiv_m^r$ on $\mathfrak{Z}$. He uses linear functions with coefficients smaller than a certain bound k, and thus uses k^k as a bound for the least common multiple of all possible coefficients. The index the relations he defines, however, is not triply exponentially bounded.

A.1 Proof of Lemma 2

Let $\delta = \operatorname{lcm} B_m$, and let T be the set of functions of the form $c_0 + \sum_{i=1}^{r} c_i x_i$ with $c_1, \ldots, c_r \in B'_m$, $c_0 \in \mathbb{Z}$, and $|c_0| \leq (r+2)\delta^3$.

There exists a function $f \in T$ with either $f(\bar{a}) \leq \delta a_{r+1}$ or $f(\bar{a}) \geq \delta a_{r+1}$. For reasons of symmetry, we will assume without loss of generality that $f(\bar{a}) \leq \delta a_{r+1}$ exists. Now choose $f \in T$ with $f(\bar{a}) \leq \delta a_{r+1}$ such that $f(\bar{a})$ is maximal. Let $u \in \mathbb{N}$ with $0 \leq u \leq \delta^3$ be such that $u = 0$ if $f(\bar{a}) = \delta a_{r+1}$ and $f(\bar{a}) + u = \delta a_{r+1} \pmod{\delta^3}$, $u \neq 0$ otherwise. Since δ^3 divides $(\operatorname{lcm} B_{m+1})^2$, and $\bar{a} E_{m+1}^r \bar{b}$ implies that $a_i = b_i \pmod{(\operatorname{lcm} B_{m+1})^2}$ for all $1 \leq i \leq r$, it holds that $g(\bar{a}) = g(\bar{b}) \pmod{\delta^3}$ for all $g \in T$, and $\delta a_{r+1} = f(\bar{a}) + u = f(\bar{b}) + u \pmod{\delta^3}$, which implies that $f(\bar{b}) + u$ is divisible by δ.

Define $b_{r+1} = (f(\bar{b}) + u)/\delta$. Before we continue, we show that $|b_{r+1}|$ is bounded by $(\max\{b_1, \ldots, b_r\} + 1) \cdot 2^{2^{2^{c(m+r)}}}$ for some constant $c \in \mathbb{N}$. This fact is used later in the proof of Lemma 4. The value $f(\bar{b}) + u$ is bounded by $r \cdot \max\{b_1, \ldots, b_r\} \cdot \max B'_m + (r+2)(\operatorname{lcm} B_m)^3 + (\operatorname{lcm} B_m)^3 \leq r \cdot \max\{b_1, \ldots, b_r\} \cdot \max B_{m+1} + (r+3)(\max B_{m+1})^{3|B_{m+1}|} \leq (\max\{b_1, \ldots, b_r\} + 1) \cdot 2^{2^{2^{c(m+r)}}}$ for some constant $c \in \mathbb{N}$.

Observe that $a_{r+1} = b_{r+1} \pmod{\delta^2}$. It remains to show that $g(\bar{a}, a_{r+1}) \geq 0$ iff $g(\bar{b}, b_{r+1}) \geq 0$ for all $g \in B_m^{r+1}$. Let $g \in B_m^{r+1}$ be a function $d_0 + \sum_{i=1}^{r+1} d_i x_i$, define $e_0 = d_0\delta/d_{r+1}$ and $e_i = d_i\delta/d_{r+1}$ for all

$1 \leq i \leq r$. Observe that $e_1, \dots, e_r \in B'_m$ and $|e_0| \leq (r+2)\delta^3$, and therefore $h(\bar{x}) = e_0 + \sum_{i=1}^r e_i x_i \in T$. We have to show that $h(\bar{a}) \geq \delta a_{r+1}$ iff $h(\bar{b}) \geq \delta b_{r+1}$.

We need the following fact to continue. For two function $f, f' \in T$ and $c \in \mathbb{Z}$ with $0 \leq c \leq (r+2)\delta^3$ it holds that $f(\bar{a}) - f'(\bar{a}) \geq c$ iff $f(\bar{b}) - f'(\bar{b}) \geq c$. Observe that $f(\bar{x}) - f'(\bar{x}) - c = (c_0 - c'_0 - c) + \sum_{i=1}^r (c_i - c'_i) x_i$ is a function from B^r_{m+1}, since $c_i - c'_i \in B_{m+1}$ and $|c_0 - c'_0 - c| \leq 3(r+2)\delta^2 \leq (r+1)(\operatorname{lcm} B_{m+1})^2$, and this claim follows $\bar{a} E^r_{m+1} \bar{b}$.

From the definition of b_{r+1}, it is easy to see that $h(\bar{a}) \geq \delta a_{r+1}$ iff $h(\bar{b}) \geq \delta b_{r+1}$ can only be false if there is a function $h' \in T$ with $f(\bar{b}) < h'(\bar{b}) \leq f(\bar{b}) + u$, where f is the function such that $f(\bar{a})$ is maximal and $f(\bar{a}) \leq \delta a_{r+1}$. But then $h'(\bar{b}) - f(\bar{b}) < u < \delta^3$ and with above claim also $f(\bar{a}) < h'(\bar{a}) \leq f(\bar{a}) + u \leq \delta a_{r+1}$, contradicting the maximality of $f(\bar{a})$. □

A.2 Proof of Lemma 3

We prove this lemma by induction over $m \in \mathbb{N}$. For $m = 0$, it suffices to show $\bar{a}, \bar{b} \in \mathbb{Z}^r$ with $\bar{a} E^r_0 \bar{b}$ satisfy the same atomic formulas, namely, $x = y$, $x < y$, and $x + y = z$. We will show this for $x = y$, the other cases are similar. Assume that $a_i = a_j$ for some $1 \leq i, j \leq r$, then $a_i - a_j \geq 0$ and $-a_i + a_j \geq 0$, and from $\bar{a} E^r_0 \bar{b}$ we can conclude that also $b_i - b_j \geq 0$ and $-b_i + b_j \geq 0$, and therefore $b_i = b_j$.

Next assume the claim is true for some $m > 0$. We have to show that $\bar{a} E^r_{m+1} \bar{b}$ refines $\equiv^r_{m+1}$, i.e., $\bar{a}$ and $\bar{b}$ satisfy the same formulas φ with $\operatorname{qr}(\varphi) \leq m+1$. But every formula φ with $\operatorname{qr}(\varphi) \leq m+1$ is equivalent to a Boolean combination of formulas $\exists x \psi$ with $\operatorname{qr}(\psi) \leq m$. It is therefore enough to show that $\mathfrak{Z} \models \exists x \psi[\bar{a}]$ iff $\mathfrak{Z} \models \exists x \psi[\bar{b}]$, where ψ is a formula with $\operatorname{qr}(\psi) \leq m$. For reasons of symmetry it is enough to show one direction. Assume $\mathfrak{Z} \models \exists x \psi[\bar{a}]$, then there is a $a_{r+1} \in \mathbb{Z}$ such that $\mathfrak{Z} \models \psi[\bar{a}, a_{r+1}]$. Since $\bar{a} E^r_{m+1} \bar{b}$, we know from Lemma 2 that there is a $b_{r+1} \in \mathbb{Z}$ such that $(\bar{a}, a_{r+1}) E^{r+1}_m (\bar{b}, b_{r+1})$. From our induction hypothesis we can conclude that $\mathfrak{Z} \models \psi[\bar{b}, b_{r+1}]$ since $\operatorname{qr}(\psi) \leq m$. But then also $\mathfrak{Z} \models \exists x \psi[\bar{b}]$ holds. □

A.3 Proof of Lemma 4

We will show the claim by induction over $r \in \mathbb{N}$. For $r = 0$, we know from the proof of Lemma 2 that each equivalence class of E^0_m has a representative b with $|b| \leq 2^{2^{2^{cm}}}$ for some constant $c \in \mathbb{N}$. Assume we know that the claim is true for some $r \geq 0$. Then each equivalence class of

E_m^{r-1} has a representative $\bar{a} \in \mathbb{Z}^{r-1}$ with $\max\{\bar{a}\} \leq 2^{2^{2^{d(m+r-1)}}}$, and with Lemma 2, the set $\{(\bar{a}, a_r) : |a_r| \leq (2^{2^{2^{d(m+r-1)}}} + 1)2^{2^{2^{e(m+r)}}}\}$ contains a representative for every equivalence class of E_m^r for some constant $e \in \mathbb{N}$. Observe that the cardinality of this set is bounded by $2^{2^{2^{c(m+r)}}}$ for some constant $c \in \mathbb{N}$. $\square$