Addition-invariant FO and regularity

Nicole Schweikardt
Goethe-Universität Frankfurt, Germany

Luc Segoufin
INRIA and ENS Cachan, France

Abstract

We consider formulas which, in addition to the symbols in the vocabulary, may use two designated symbols $\prec$ and $+$ that must be interpreted as a linear order and its associated addition. Such a formula is called addition-invariant if, for each fixed interpretation of the initial vocabulary, its result is independent of the particular interpretation of $\prec$ and $+$.

This paper studies the expressive power of addition-invariant first-order logic, $+$-inv-FO, on the class of finite strings. Our first main result gives a characterization of the regular languages definable in $+$-inv-FO: we show that these are exactly the languages definable in FO with extra predicates, denoted by "lm" for short, for testing the length of the string modulo some fixed number. Our second main result shows that every language definable in $+$-inv-FO, that is bounded or commutative or deterministic context-free, is regular. As an immediate consequence of these two main results, we obtain that $+$-inv-FO is equivalent to FO(lm) on the class of finite colored sets.

Our proof methods involve Ehrenfeucht-Fraïssé games, tools from algebraic automata theory, and reasoning about semi-linear sets.

1 Introduction

The model checking problem consists in testing whether a relational structure satisfies a property expressed in a logical formalism. It is a central problem in many areas of computer science such as databases or automated verification. In order to perform model checking in an automated way, the structure must be stored on the disk, and this induces a linear order on it. The logical formalism could then make use of this linear order, typically for looping through all the elements of the structure. A desirable property, however, is that the result should only depend on the structure itself and not on the linear order that is specific to its current representation on the disk. This is known as the *data independence principle* in the database context or as *closure under isomorphisms* of the logical formalism.

In this paper, we call this property *order-invariance*, denoted "$\prec$-inv-". A logical formalism $\mathcal{L}$, with a designated binary symbol "$\prec$" for accessing an extra linear order, is said to be order-invariant if, over any structure, its output is independent on the actual extra linear order. Two typical, celebrated examples are $\prec$-inv-LFP, which captures all properties computable in PTime, and $\prec$-inv-PFP, which captures all properties computable in PSpace [10, 21], whereas the least fixed-point logic LFP and the partial fixed-point logic PFP themselves are known to be too weak for capturing all of PTime and PSpace.

This shows that access to an arbitrary linear order increases expressiveness when one deals with powerful logics that can express recursive operators. What about weaker logics, such as first-order logic (FO)? A famous example due to Gurevich (see Theorem 5.3 in [11]) shows that $\prec$-inv-FO is more expressive than FO. But still, $\prec$-inv-FO is actually not very expressive. It can express only *local* queries [9]. Furthermore, it lacks arithmetic: while LFP is able to define addition and multiplication from the order, this is no longer the case for FO.

This paper deals with a setting, where the FO-formulas not only have access to an arbitrary extra linear order, but also to the addition and multiplication induced by this order. As for order-invariance, the result should be independent on the extra linear order. When only addition is used, we write "$+$-inv-" while, when both addition and multiplication are used, we write "$(+, *)$-inv-". Note that the least fixed-point formalism of $\prec$-inv-LFP is strong enough to define arithmetic, thus $\prec$-inv-LFP is equivalent to $(+, *)$-inv-LFP.

For weaker logics such as monadic least-fixed point logic MLFP or monadic second-order logic MSO, however, the presence of extra arithmetic enables the logics to express interesting properties that they could not do with just the extra linear order. For instance, on strings, $\prec$-inv-MSO and $\prec$-inv-MLFP both capture the regular languages and are no more expressive than MSO and MLFP. But $+$-inv-MLFP can define all properties in DLIN (i.e., computable by a deterministic linear time random access machine), while $+$-inv-MSO captures the linear time hierarchy LinH [14, 17].

What about the first-order case? Notice that, unlike for MLFP and MSO, multiplication is no longer definable from addition, and hence we need to distinguish between

+-inv-FO and $(+, *)$-inv-FO. Apart from the fact that all properties expressible in +-inv-FO or $(+, *)$-inv-FO belong to uniform AC^0, not much is known about these two formalisms. As a step towards understanding their expressive power, we propose to investigate simple structures. We mainly consider *strings*, as structures of finite labeled graphs whose edges form a single directed path, and *transitive strings*, as the corresponding structures in which also the transitive closure of the edge relation is present. The simplest structures we consider are finite *colored sets*.

Main results. We start our study by showing that the regular languages that can be defined in +-inv-FO are exactly those definable in FO with extra predicates for testing the length of the string modulo some fixed number. As an intermediate result of independent interest, we obtain a decidable characterization for definability in this later logic. See Theorem 3.12, Theorem 3.15, and Theorem 3.16.

We then wonder whether all languages definable in +-inv-FO are regular. We show that every language definable in +-inv-FO that is *bounded* or *commutative* or *deterministic context-free* is regular (cf., Theorem 4.1, Theorem 5.1, and Theorem 5.4). Here, a language L is called *bounded* if there exists a number n and strings $w_1, \ldots, w_n$ such that $L \subseteq w_1^* w_2^* \cdots w_n^*$ (cf. [8]). A language L is called *commutative* if for any string $u \in L$, any permutation of the letters of u is also a string in L. A language L is called *deterministic context-free* if it is recognized by a deterministic pushdown-automaton.

As an immediate consequence of the result on commutative languages and our characterization of regular languages definable in +-inv-FO, we obtain a characterization of the *colored sets* definable in +-inv-FO: Over the class of finite colored sets, every +-inv-FO-sentence is logically equivalent to an FO-sentence with extra predicates for testing the cardinality of the underlying structure's universe modulo some fixed number (cf. Corollary 5.3).

We conclude with an example of a context-free (and nonregular) language that is definable in $(+, *)$-inv-FO, but for which we could not settle whether it is definable in +-inv-FO or not. We conjecture, however, that it is not definable in +-inv-FO and, moreover, that all languages definable in +-inv-FO are regular.

Related work. Besides the references already cited above, we further note that $\prec$-inv-FO$(+1)$ was studied over words and trees in [3], where it was shown to have the same expressive power as FO$(+1)$. Note that $\prec$-inv-FO$(+1)$ is simpler than +-inv-FO$(+1)$; it is immediate from the definition that $\prec$-inv-FO$(+1)$ defines only regular languages.

Structure of the paper. We start with the necessary notations and definitions in Section 2. In Section 3 we characterize the regular languages definable in +-inv-FO. Section 4 shows that bounded languages definable in +-inv-FO$(<)$ are regular. Section 5 deals with commutative languages, deterministic context-free languages, and colored sets. Due to space limitations, many technical details of the proofs are deferred to an appendix.

2 Preliminaries

Basic notation. $\mathbb{Z}$ denotes the set of integers. $\mathbb{N} = \{0, 1, 2, ...\}$ and $\mathbb{N}_{\geqslant 1} = \mathbb{N} \setminus \{0\}$ denote the set of natural numbers and of positive natural numbers, respectively. For $n \in \mathbb{N}_{\geqslant 1}$, we write $[n]$ to denote the set $\{0, ..., n-1\}$. For $i, j \in \mathbb{N}$ and $q \in \mathbb{N}_{\geqslant 1}$, we write $i \equiv j \; [q]$ to indicate that i is congruent to j modulo q. If S is a finite subset of $\mathbb{N}_{\geqslant 1}$, we write lcm S to denote the least common multiple of the elements in S.

Strings and transitive strings. We fix a finite alphabet Σ. We let ϱ be the signature that consists of a unary relation symbol P_a for each letter $a \in \Sigma$. In this paper, a *string* over Σ is a finite relational structure over the signature $\sigma = \varrho \cup \{E\}$, containing unary predicates P_a for all $a \in \Sigma$, partitioning the elements of the universe, and one binary predicate E that is interpreted as a graph whose edges form a single directed path. A *transitive string* over Σ is a finite relational structure over the signature σ' that extends σ with a binary predicate E^+ interpreted as the transitive closure of E. Hence, each element of Σ^* can be viewed either as a transitive string or as a string, depending on whether we can compare any two of its positions or only successive positions.

Given a string (or a transitive string) w, we denote its length (i.e., the cardinality of its universe) by $|w|$.

Logics. We denote by FO$(=)$, FO$(+1)$, and FO$(<)$ the first-order logics over ϱ, σ, and σ' respectively. The semantics of their formulas are defined in the natural way (where we assume that equality "$=$" can be used in atomic formulas). Each closed formula φ defines a language L_φ which is the set of all strings $w \in \Sigma^*$ that, when seen as a logical structure, satisfy φ.

We will consider strings with an extra built-in linear order $\prec$ together with the associated arithmetic, and logics that can make use of this extra arithmetic in an *order-invariant* way. This is formalized as follows.

Let $\sigma[+]$ (resp. $\sigma'[+]$ or $\varrho[+]$) be the extension of σ (resp. σ' or ϱ) with a binary predicate $\prec$ and a ternary predicate $+$. We denote the corresponding first-order logics on these extensions of σ, σ', and ϱ by FO$(+1, \prec, +)$, and FO$(<, \prec, +)$, and FO$(=, \prec, +)$.

A $\sigma[+]$-*expansion* of a string w is a structure over $\sigma[+]$ which interprets the predicates of σ as in w and interprets $\prec$ as a linear order, and $+$ as the addition induced by $\prec$. I.e., $a + b = c$ holds true on a string w whose universe is linearly ordered by $\prec$ iff $\hat{a} + \hat{b} = \hat{c}$, where $\hat{x}$ denotes the index of the element x in the linear order $\prec$ (here we adopt the convention that the smallest element w.r.t. $\prec$ has index

0). It is important to not confuse the linear order $\prec$ with the transitive closure of E: they might not be identical!

Example 2.1. For every $q \in \mathbb{N}_{\geqslant 1}$ and every $i \in [q]$ there is a FO($=, \prec, +$)-sentence $\varphi_{i,q}$ such that a $\sigma[+]$-expansion of a string w satisfies $\varphi_{i,q}$ iff $|w| \equiv i \ [q]$.

For example, the formula $\varphi_{1,2}$, expressing that the length of a string is odd, can be chosen as follows:

$$\exists x \, \exists z \, (x + x = z \, \wedge \, \forall y \, (\, y \prec z \vee y = z \,))$$

(recall that we adopt the convention that the smallest element w.r.t. $\prec$ has index 0). $\qquad\square$

A sentence φ of FO($+1, \prec, +$) is said to be *addition-invariant* if for any string w and any two $\sigma[+]$-expansions w_1 and w_2 of w we have $w_1 \models \varphi$ iff $w_2 \models \varphi$. We write $+$-inv-FO($+1$) to denote the class of all addition-invariant FO($+1, \prec, +$)-formulas. If φ is a sentence in $+$-inv-FO($+1$), we write $w \models \varphi$ to indicate that for some (respectively, every) $\sigma[+]$-expansion w_1 of w we have $w_1 \models \varphi$. The classes $+$-inv-FO($<$) and $+$-inv-FO($=$) are defined in the analogous way.

Note that Example 2.1 shows that $+$-inv-FO($=$) can test the length of a string modulo some constant.

The goal of this paper is to understand the expressive power of these logics. Note that, as defined, their syntax is not necessarily recursive, as testing whether a formula of FO($+1, \prec$) is order-invariant is undecidable [3]. Whether they have an equivalent effective syntax is an interesting open problem. In Section 5 we show that this is the case for $+$-inv-FO($=$).

We start by investigating the regular languages definable in $+$-inv-FO($<$), $+$-inv-FO($+1$), and $+$-inv-FO($=$) in Section 3. Then we move to bounded languages in Section 4 and to commutative languages and deterministic context-free languages in Section 5.

In our proofs, we will sometimes also refer to the logic FO($<, +$), consisting of all first-order formulas of signature $\sigma' \cup \{+\}$. When evaluating such a formula on a transitive string, the symbol $+$ is interpreted with the particular addition relation that fits to the *natural* linear order $<$ on the positions of the string.

3 Regular languages and addition-invariance

The goal of this section is to characterize the regular languages definable in $+$-inv-FO($<$), $+$-inv-FO($+1$), and $+$-inv-FO($=$). We start with the most expressive of the three, $+$-inv-FO($<$), and we follow the methodology of [3].

Using an Ehrenfeucht-Fraïssé game argument, we show in Section 3.1 that regular languages definable in $+$-inv-FO($<$) have particular closure properties. Then, using an algebraic argument, we show in Section 3.2 that the

regular languages satisfying these closure properties are exactly those definable in FO($<, lm$), where lm provides predicates for testing the total length of the string modulo some fixed number (see Section 3.2 for the precise definition). As these predicates are expressible in $+$-inv-FO($<$) (cf., Example 2.1), we conclude that the languages definable in FO($<, lm$) are exactly the regular languages definable in $+$-inv-FO($<$) (see Theorem 3.12).

Using similar arguments, we also obtain (in Section 3.3) characterizations of the regular languages definable in $+$-inv-FO($+1$) and $+$-inv-FO($=$) by the logics FO($+1, lm$) and FO($=, lm$).

3.1 Closure properties of $+$-inv-FO($<$)

Given a language L, its syntactic congruence $=_L$ is defined for strings x and y by $x =_L y$ iff $\forall u, v \in \Sigma^*$, $uxv \in L$ iff $uyv \in L$. A string x is called *idempotent* (for L) if $xx =_L x$. Recall that L is regular iff its syntactic congruence has finite index (see e.g. [19]). Hence, for every regular language L there is a natural number ω, depending only on L, such that for all strings x, the string x^ω is idempotent.

We say that L is *closed under modulo transfers* if for all $x, y, z \in \Sigma^*$ we have:

$$\text{if} \quad |x| = |z|, \quad \text{then} \quad x^\omega xyz^\omega =_L x^\omega yzz^\omega. \qquad (1)$$

The next theorem provides a closure property of regular languages definable in $+$-inv-FO($<$); the rest of Section 3.1 is devoted to the proof of this theorem.

Theorem 3.1. *Let L be a regular language definable in $+$-inv-FO($<$). Then L is closed under modulo transfers.*

Proof. For the sake of a contradiction, assume that L is a regular language that is *not* closed under modulo transfers. Then there exist strings x, y, z such that $|x| = |z|$ but $x^\omega xyz^\omega \neq_L x^\omega yzz^\omega$. By symmetry, we can assume that there exist strings u, v such that $ux^\omega xyz^\omega v \in L$ but $ux^\omega yzz^\omega v \notin L$. By the definition of ω we have for all $\alpha, \beta \in \mathbb{N}_{\geqslant 1}$ that

$$ux^{\alpha\omega} xyz^{\beta\omega} v \in L \quad \text{and} \quad ux^{\alpha\omega} yzz^{\beta\omega} v \notin L. \qquad (2)$$

From Σ we construct the finite alphabet $\bar{\Sigma} := \Sigma \cup \{(a, x) \mid a \in \Sigma\} \cup \{(a, z) \mid a \in \Sigma\}$. Let $\bar{x}$ and $\bar{z}$ be the strings constructed from x and z by tagging the letters with the appropriate symbol of $\bar{\Sigma}$. I.e., $\bar{x}$ is obtained from x by replacing every letter a of x with the letter (a, x). Analogously, $\bar{z}$ is obtained from z.

In the following, for $w \in \bar{\Sigma}^*$ we write $|w|_{\bar{x}}$ (and $|w|_{\bar{z}}$) to denote the number of occurrences of the string $\bar{x}$ (and $\bar{z}$) in w. We consider the languages

$$L_1 := \{\, w \in uyv\,\bar{x}\,(\bar{x}\bar{z}\,|\,\bar{z}\bar{z})^* \;:\; |w|_{\bar{x}}, |w|_{\bar{z}} \geqslant \omega,$$
$$|w|_{\bar{x}} \equiv 1\,[\omega], \quad |w|_{\bar{z}} \equiv 0\,[\omega]\,\},$$

$$L_2 := \{\, w \in uyv\,\bar{x}\,(\bar{x}\bar{z}\,|\,\bar{z}\bar{z})^* \;:\; |w|_{\bar{x}}, |w|_{\bar{z}} \geqslant \omega,$$
$$|w|_{\bar{x}} \equiv 0\,[\omega], \quad |w|_{\bar{z}} \equiv 1\,[\omega]\,\}.$$

A formula φ is said to *separate* L_1 from L_2, if L_φ contains L_1 but does not intersect with L_2. Using equation (2) and the assumption that L is definable in +-inv-FO($<$), we obtain:

Claim 3.2. *There is a formula of* FO($<, +$) *that separates* L_1 *from* L_2.

Proof of Claim 3.2. Recall that, by assumption, L is definable in +-inv-FO($<$). We will use this formula, along with a suitable FO($<, +$) interpretation, to obtain an FO($<, +$)-formula that separates L_1 from L_2.

The FO($<, +$) interpretation is constructed in such a way that, when given a string $w \in uyv\,\bar{x}\,(\bar{x}\bar{z}\,|\,\bar{z}\bar{z})^*$, it defines a string $w' \in ux^*yz^*v$ such that $w \in L_1$ implies $w' \in L$, and $w \in L_2$ implies $w' \notin L$.

This FO($<, +$) interpretation replaces letters in $\bar{x}$ and $\bar{z}$ by the corresponding letters in x and z. Furthermore, it consists of two formulas ψ_{Succ} and ψ_{Ord}, each with two free variables. When evaluated in w, the formulas ψ_{Succ} and ψ_{Ord} define the following successor relation and its associated transitive closure:

First, there come all the positions in u (in the order in which they appear in w). Then, there come all positions that belong to one of the substrings $\bar{x}$, in the order in which they appear in w (this is doable in FO because we use labels in $\bar{\Sigma}$). Afterwards, there come all positions that belong to y, in the order in which they appear in w. Then, there come all positions that belong to one of the substrings $\bar{z}$, in the order in which they appear in w (again, this is doable in FO since we use labels in $\bar{\Sigma}$). Finally, there come all positions that belong to v, in the order in which they appear in w.

From a word $w \in uyv\,\bar{x}\,(\bar{x}\bar{z}\,|\,\bar{z}\bar{z})^*$, this construction produces a word w' of the form ux^iyz^jv with $i = |w|_{\bar{x}}$ and $j = |w|_{\bar{z}}$. If $w \in L_1$, then $i, j \geqslant \omega$ and $i \equiv 1\,[\omega]$ and $j \equiv 0\,[\omega]$. Similarly, if $w \in L_2$, then $i, j \geqslant \omega$ and $i \equiv 0\,[\omega]$ and $j \equiv 1\,[\omega]$. Thus, by equation (2) we obtain:

If $w \in L_1$, then $w' \in L$. If $w \in L_2$, then $w' \notin L$.

Now recall that, by assumption, L is definable by a +-inv-FO($<$)-sentence φ_L. We modify this sentence according to the FO($<, +$) interpretation that defines w' in w. I.e., we replace every occurrence of the symbols E and E^+ (for the successor and the natural linear order on the positions of the string) with the formulas ψ_{Succ} and ψ_{Ord}. Thereby, we obtain an FO($<, +$)-sentence φ that is satisfied by w iff $w' \models \varphi_L$ (note that this is the place where *addition-invariance* of φ_L is essential). In particular, φ separates L_1 from L_2. Thus, the proof of Claim 3.2 is complete. $\square$

The desired contradiction for finishing the proof of Theorem 3.1 now immediately follows from Claim 3.2 and the next proposition.

Proposition 3.3. *Let* x, y, z, u, v *be strings with* $|x| = |z| \geqslant 1$, *and let* $\bar{x}, \bar{z}$ *be obtained from* x, z *as above. Fix an arbitrary* $\omega \geqslant 2$, *and let* L_1, L_2 *be chosen as above. Then, no formula of* FO($<, +$) *can separate* L_1 *from* L_2.

Proof. The proof of the proposition is a consequence of the following technical lemma that is based on an Ehrenfeucht-Fraïssé game argument. In the statement below, $w \approx_k^+ w'$ indicates that the strings w and w' satisfy the same sentences of FO($<, +$) of quantifier rank $\leqslant k$. It has an Ehrenfeucht-Fraïssé game counterpart requiring the existence of a winning strategy for the duplicator in the corresponding k-round game [11]. Similarly, we define $w \approx_k^< w'$ when only sentences of FO($<$) are considered.

Lemma 3.4. *Let* $\bar{x}, \bar{z}, y, u, v$ *be chosen as in Proposition 3.3. For any* k, *there exist* $d, d' \in \mathbb{N}_{\geqslant 1}$ *with* $d < d'$, *and numbers* $i_0, i_1, \dots, i_{d'} \in \mathbb{N}_{\geqslant 1}$, *such that:*[1]

1. $uyv\,\bar{x}\,(\bar{x}\bar{z})^{i_0}\big(\bar{z}\bar{z}(\bar{x}\bar{z})^{i_j}\big)_{j\in\{1,\dots,d\}} \approx_k^+$
   $uyv\,\bar{x}\,(\bar{x}\bar{z})^{i_0}\big(\bar{z}\bar{z}(\bar{x}\bar{z})^{i_j}\big)_{j\in\{1,\dots,d'\}}$

2. $\sum_{j=0}^{d} i_j \equiv -d \equiv 0\,[\omega]$

3. $\sum_{j=0}^{d'} i_j \equiv -d' \equiv -1\,[\omega]$.

Before proving Lemma 3.4, let's see why it implies the proposition. Assume for the sake of a contradiction that there is a formula φ separating L_1 from L_2. Let k be its quantifier rank, and let $d, d', i_0, \cdots, i_{d'}$ be as stated in Lemma 3.4. Let w be $uyv\,\bar{x}(\bar{x}\bar{z})^{i_0}\big(\bar{z}\bar{z}(\bar{x}\bar{z})^{i_j}\big)_{j\in\{1,\dots,d\}}$ and let w' be $uyv\,\bar{x}(\bar{x}\bar{z})^{i_0}\big(\bar{z}\bar{z}(\bar{x}\bar{z})^{i_j}\big)_{j\in\{1,\dots,d'\}}$.

By Item 2, $|w|_{\bar{x}} = 1 + \sum_{j=0}^{d} i_j \equiv 1\,[\omega]$ and $|w|_{\bar{z}} = 2d + \sum_{j=0}^{d} i_j \equiv 0\,[\omega]$. Furthermore, since $i_0, \dots, i_d \neq 0$, we have $|w|_{\bar{x}}, |w|_{\bar{z}} \geqslant \omega$. Therefore, $w \in L_1$. Similarly, by Item 3, we have $|w'|_{\bar{x}} = 1 + \sum_{j=0}^{d'} i_j \equiv 0\,[\omega]$ and $|w'|_{\bar{z}} = 2d' + \sum_{j=0}^{d'} i_j \equiv 1\,[\omega]$. Therefore, $w' \in L_2$. But due to Item 1, either w and w' both satisfy φ, or neither of them satisfies φ. Hence, φ cannot separate L_1 from L_2.

Proof of Lemma 3.4. The proof is essentially an Ehrenfeucht-Fraïssé game argument, the difficulty being to exhibit a winning strategy in the presence of addition. In order to do so, we use the following generalization of a result by Lynch [12], which was proved in [18] and which allows us to reduce the existence of a winning strategy in a game with addition to the existence of a winning strategy in another game, where addition is not present.

---

[1]Here, we use the following notation: For strings $w_1, \dots, w_d$, we write $(w_j)_{j\in\{1,\dots,d\}}$ to denote the string $w_1 w_2 \cdots w_d$.

Proposition 3.5 (Immediate from [18])**.** *For all* $m, h, k' \in \mathbb{N}$ *there is a number* $r = r(m, h, k') \in \mathbb{N}$ *and an infinite set* $P = \{ p_1 < p_2 < p_3 < \cdots \} \subseteq \mathbb{N}$ *with* $p_1 > h$ *and* $p_j \equiv h \, [m]$, *for all* $j \geqslant 1$, *such that the following is true for all* $\ell_1, \ell_2 \in \mathbb{N}_{\geqslant 1}$:

$$\text{if} \qquad \mathbf{1}^{\ell_1} \approx^<_r \mathbf{1}^{\ell_2}$$
$$\text{then} \qquad (\mathbb{Z}, <, +, P, P_1) \approx^+_{k'} (\mathbb{Z}, <, +, P, P_2),$$

where P_1 *is* $\{p_1, \ldots, p_{\ell_1}\}$ *while* P_2 *is* $\{p_1, \ldots, p_{\ell_2}\}$, *and* $\mathbf{1}^{\ell_1}$ *and* $\mathbf{1}^{\ell_2}$ *are words of length* ℓ_1 *and* ℓ_2 *over the singleton alphabet* $\{\mathbf{1}\}$.

Fix $m_1 = |\bar{x}\bar{z}| = |\bar{z}\bar{z}|$, $m = m_1\omega$, $h = |uyv\bar{x}|$. For any given k' let r, and $p_1, p_2, \cdots$ be given by Proposition 3.5 with these values for k', m, and h.

Now let $i_0 = (p_1 - h)/m_1$ and for $j \geqslant 1$, $i_j = (p_{j+1} - p_j - m_1)/m_1$. Then for all ℓ we have $\sum_{j=0}^{\ell} i_j = (p_{\ell+1} - h - \ell \cdot m_1)/m_1 \equiv -\ell \, [\omega]$.

We then choose d and d' in $\mathbb{N}_{\geqslant 1}$ such that $\mathbf{1}^d \approx^<_r \mathbf{1}^{d'}$, $d \equiv 0 \, [\omega]$ and $d' \equiv 1 \, [\omega]$. The existence of such d and d' is guaranteed using a standard game argument on transitive strings (cf., [11]). By Proposition 3.5 we have

$$(\mathbb{Z}, <, +, P, P_1) \approx^+_{k'} (\mathbb{Z}, <, +, P, P_2). \tag{3}$$

A standard first-order interpretation then transforms the structures of equation (3) into the strings desired for Item 1 of the lemma. The interpretation assigns a label to each number i with $0 \leqslant i < \mu$ (where μ is the minimum element in P that's not in P_1, resp. P_2), using the following rules:

1. if $i < h$, then it uses the label of the $(i+1)^{\text{st}}$ position in $uyv\,\bar{x}$
   (this is definable in FO, since h and $uyv\,\bar{x}$ are fixed)

2. if $i \geqslant h$, $i \equiv j \, [m_1]$, $0 \leqslant j < m_1$, and position $i - j$ is not in P, then it uses the label of the $(j+1)^{\text{st}}$ position of $\bar{x}\bar{z}$,
   (this is definable in FO, since h, m_1, and $\bar{x}\bar{z}$ are fixed and $+$ is available in the structures of equation (3))

3. if $i \geqslant h$, $i \equiv j \, [m_1]$, $0 \leqslant j < m_1$, and position $i - j$ is in P, then it uses the label of the $(j+1)^{\text{st}}$ position of $\bar{z}\bar{z}$.

Let k_0 be the quantifier rank of the FO interpretation that establishes this translation of $(\mathbb{Z}, <, +, P, P_1)$ and $(\mathbb{Z}, <, +, P, P_2)$ into the corresponding strings w_1 and w_2. Note that w_1 and w_2 are of the form stated in Item 1 of Lemma 3.4. Furthermore, equation (3) implies that $w_1 \approx^+_k w_2$, for $k := k' - k_0$. This concludes the proof of Lemma 3.4, of Proposition 3.3, and of Theorem 3.1. $\square$

3.2 Characterization of FO($<, lm$)

We show in this section that closure under modulo transfers corresponds to definability in FO($<, lm$), where FO($<$,

lm) is the logic extending FO($<$) with predicates $lm(i, q)$ (for all $i, q \in \mathbb{N}$), that hold true in a structure iff the size of its universe is equal to i modulo q.

Theorem 3.6. *Let L be a regular language. Then L is definable in* FO($<, lm$) *iff L is closed under modulo transfers.*

The "only if" direction of Theorem 3.6 follows for instance from Theorem 3.1, as languages definable in FO($<, lm$) are also definable in $+$-inv-FO($<$) by Example 2.1. Proving the "if" direction requires more work; the remainder of Section 3.2 is devoted to the proof.

We will make use of the following straightforward observation:

Claim 3.7. *A language is definable in* FO($<, lm$) *iff it is a finite union of languages of the form $S \cap Z_i^q$, where S is definable in* FO($<$) *(i.e., S is a starfree regular language, cf. [13]), i and q are natural numbers, and Z_i^q is the set of all strings of length i modulo q.*

As a further ingredient, we use the following consequence of closure under modulo transfers.

Proposition 3.8. *Let L be a regular language that is closed under modulo transfers. There exists $q \in \mathbb{N}_{\geqslant 1}$ such that for all $k \in \mathbb{N}_{\geqslant 1}$, and all strings $v_1, \ldots, v_k$ and $x_1, \ldots, x_{k+1}$ over Σ we have: If $\delta_1, \cdots, \delta_k$ are natural numbers such that*

$$\delta_1|v_1| + \cdots + \delta_k|v_k| \equiv 0 \, [q], \tag{4}$$

then we have

$$x_1 v_1^\omega v_1^{\delta_1} x_2 v_2^\omega v_2^{\delta_2} \cdots x_k v_k^\omega v_k^{\delta_k} x_{k+1}$$
$$=_L \ x_1 v_1^\omega x_2 v_2^\omega \cdots x_k v_k^\omega x_{k+1}. \tag{5}$$

The proof is by induction on k and makes use of Bézout's identity. Details can be found in Appendix B.1.

Let L be a regular language closed under modulo transfers. Let q be the number given by Proposition 3.8. For $0 \leqslant i < q$, let L_i be the restriction of L to strings of length i modulo q. Notice that because of (4), both sides of (5) have the same length modulo q. Hence, (5) remains true after replacing $=_L$ with $=_{L_i}$. We show that L_i is definable in FO($<, lm$). This will conclude the proof, as $L = \bigcup_i L_i$.

Our goal is to show that $L_i = M \cap Z_i^q$ for some *counter-free* regular language M. By Theorem 3.9 below, this implies that M is definable in FO($<$) and therefore L_i is definable in FO($<, lm$).

Let A be a minimal deterministic automaton, and let δ_A be its transition function. A *counter* for A is a string u and a set $P = \{p_0, \ldots, p_{k-1}\}$, with $k \geqslant 2$, of states such that $\delta_A(p_i, u) = p_{i+1 \bmod k}$. A string u is a *counter* if it forms a counter with some set P. We will use the following well-known result.

Theorem 3.9 ([13]). *A regular language L is definable in* FO($<$) *iff its minimal deterministic automaton does not have any counter.*

Note that if $u = v\,v$ is a counter, then v is also a counter. Similarly, if $u = u_1 u_2$ is a counter, then its *cyclic shift* $u_2 u_1$ is also a counter. A counter u is *prime* if u is not of the form $v\,v$ for any v. The *size* of a counter u is the length of u. A simple pumping argument shows that if A has a counter u, then it has a counter of size bounded by a number N that depends only on A. It thus suffices to consider prime counters of size $< N$.

Let A be the minimal deterministic automaton for L_i.

Let C be the set of prime counters of A of size $< N$. I.e., C is a set of pairs (u, P) where $u \in \Sigma^*$, $|u| < N$, and P is a set of states of A of size $\geqslant 2$, satisfying the condition of prime counters. We keep in C only one counter per cyclic shift of u. Let C_S be the set of strings that are counters occurring in C, and let k be the maximal length of such strings. Notice that because A is deterministic, if $(u, P) \in C$ and $(u, P') \in C$, then $P \cap P' = \emptyset$.

We construct an automaton B such that the minimal deterministic finite automaton equivalent to B has no counter, and $L_i = \mathcal{L}(B) \cap Z_i^q$, where $\mathcal{L}(B)$ denotes the language accepted by B. This will conclude the proof of Theorem 3.6.

The automaton B essentially simulates A. On top of that, it remembers in its states the last k previous letters read. It also has one counter per element of C_S that counts up to $\omega \cdot q$. The transition table of B is given by the following rules, where c_u is the current value of the counter for u, and v is the string of the last k letters read, including the currently read letter a:

1. For all u in C_S such that v does not end with a cyclic shift of u, B sets the counter c_u to 0.

2. If $v = v'u$, $u \in C_S$, and $c_u < \omega \cdot q$, then B simulates A and increases the counter c_u by 1.

3. If $v = v'u$, $u \in C_S$, $c_u = \omega \cdot q$, and the simulation of A on the current letter gives a state $p \in P$ such that $(u, P) \in C$, then B non-deterministically selects a state of P. Note that this is the only case where B does not simply simulate A.

4. In all other cases, B simply simulates A.

From the construction of B we immediately obtain:

Lemma 3.10. *A string w is accepted by B iff it can be decomposed as $w = w_1 \cdots w_n$, for some $n \geqslant 1$, such that*

- $w_1 u_1^{\delta_1} w_2 u_2^{\delta_2} \cdots w_n$ *is accepted by A for some* $\delta_1, \cdots, \delta_{n-1} \in \mathbb{N}$,
- $u_i^{\omega q}$ *is a suffix of w_i, for each $i < n$, and*
- $u_i \in C_S$ *for all $i < n$.*

Note that the case $n = 1$ implies that every word accepted by A is accepted by B, i.e., $L_i \subseteq \mathcal{L}(B)$.

It turns out that B has the desired properties:

Proposition 3.11. *(a)* $L_i = \mathcal{L}(B) \cap Z_i^q$.

(b) The minimal deterministic automaton recognizing $\mathcal{L}(B)$ *does not have any counter.*

Proof. We begin by proving part (a).

By Lemma 3.10, $L_i \subseteq \mathcal{L}(B)$, and hence it suffices to show that $\mathcal{L}(B) \cap Z_i^q \subseteq L_i$. Let w be a string of length i modulo q, accepted by B. By Lemma 3.10 we can decompose w as $w_1 w_2 \cdots w_n$, such that $w_1 u_1^{\delta_1} w_2 u_2^{\delta_2} \cdots w_n$ is accepted by A. By definition of A, this word has length i modulo q. Hence we have $\sum_i |u_i| \delta_i \equiv 0 \ [q]$. We can therefore apply Proposition 3.8 and obtain that $w_1 w_2 \cdots w_n$ is accepted by A, as desired.

The proof of part (b) makes use of Proposition 3.8 and Lemma 3.10, along with a careful analysis of the (potential) counters of A and the minimal deterministic automaton equivalent to B. Details can be found in Appendix B.1. $\square$

This completes the proof of Theorem 3.6. Classical techniques now imply that, given an automaton for L, it is decidable whether L is closed under modulo transfers: Using the pumping lemma, one shows that all quantified strings can be assumed to be short. Then, a brute force analysis yields the decision algorithm.

Hence, Theorem 3.6 provides an effective test for definability in FO($<, lm$), a result of independent interest. As an immediate consequence of Theorem 3.1 and Theorem 3.6, we obtain an effective syntax and a complete characterization of the regular languages definable in +-inv-FO($<$):

Theorem 3.12. *A regular language is definable in* +-*inv*-FO($<$) *iff it is definable in* FO($<, lm$). *Furthermore, given an automaton for a regular language L, it is decidable whether L is definable in* FO($<, lm$).

3.3 +-inv-FO(+1) and +-inv-FO(=)

A characterization of the regular languages definable in +-inv-FO($+1$) can be obtained in the same way, using an additional closure property taken from [19]. A regular language L is *closed under swaps* if $\forall e, f, x, y, z \in \Sigma^*$ such that e, f are idempotent we have:

$$e\,x\,f\,y\,e\,z\,f \ =_L \ e\,z\,f\,y\,e\,x\,f. \tag{6}$$

The proof of the following theorem is done as for Theorem 3.1, using an Ehrenfeucht-Fraïssé game argument that can be found in Appendix B.2.

Theorem 3.13. *Let L be a regular language definable in* +-*inv*-FO($+1$). *Then L is closed under swaps.*

As for Theorem 3.6, we can show the following (see Appendix B.3 for a proof):

Theorem 3.14. *Let L be a regular language. Then L is definable in $\mathrm{FO}(+1, lm)$ iff L is closed under modulo transfers and under swaps.*

In summary, we have:

Theorem 3.15. *A regular language is definable in $+$-inv-$\mathrm{FO}(+1)$ iff it is definable in $\mathrm{FO}(+1, lm)$. Furthermore, given an automaton for a regular language L, it is decidable whether L is definable in $\mathrm{FO}(+1, lm)$.*

By further requiring commutativity of the language, we obtain similar results for $+$-inv-$\mathrm{FO}(=)$ (the proof can be found in Appendix B.4).

Theorem 3.16. *A regular language is definable in $+$-inv-$\mathrm{FO}(=)$ iff it is definable in $\mathrm{FO}(=, lm)$ iff it is commutative and closed under modulo transfers. Furthermore, given an automaton for a regular language L, it is decidable whether L is definable in $\mathrm{FO}(=, lm)$.*

4 Bounded languages

A language $L \subseteq \Sigma^*$ is called *bounded* if there exists an $n \in \mathbb{N}_{\geqslant 1}$ and n strings $w_1, \ldots, w_n \in \Sigma^*$ such that $L \subseteq w_1^* w_2^* \cdots w_n^*$. Bounded languages received quite some attention in the literature, cf. e.g. [5, 8, 7, 16, 4]. This section's main result is:

Theorem 4.1. *Every bounded language definable in $+$-inv-$\mathrm{FO}(<)$ is regular.*

Due to space limitations, we prove Theorem 4.1 only for the special case where $|w_1| = \cdots = |w_n|$; the proof of the general version will be given in the full paper. More precisely, we here give the proof of the following Proposition 4.2. The proof of this proposition contains already all the ingredients necessary for proving Theorem 4.1.

Proposition 4.2. *Let $n \in \mathbb{N}_{\geqslant 1}$, let $w_1, \ldots, w_n \in \Sigma^*$ be such that $|w_1| = \cdots = |w_n| \geqslant 1$, and let $\alpha_1, \ldots, \alpha_{n+1} \in \Sigma^*$. Every language $L \subseteq \alpha_1 w_1^* \alpha_2 w_2^* \cdots \alpha_n w_n^* \alpha_{n+1}$ that is definable in $+$-inv-$\mathrm{FO}(<)$ is regular.*

The remainder of Section 4 is devoted to the proof of Proposition 4.2.

For $n \in \mathbb{N}_{\geqslant 1}$ and $\alpha_1, \ldots, \alpha_{n+1}, w_1, \ldots, w_n \in \Sigma^*$ we write $\overline{\alpha}$ and $\overline{w}$ to denote the tuples $(\alpha_1, \ldots, \alpha_{n+1})$ and $(w_1, \ldots, w_n)$. By $M_{\overline{\alpha}}^{\overline{w}}$ we denote the language $\alpha_1 w_1^* \alpha_2 w_2^* \cdots \alpha_n w_n^* \alpha_{n+1}$. For proving Proposition 4.2, it is convenient to identify a vector $x = (x_1, \ldots, x_n) \in \mathbb{N}^n$ with the string $\alpha_1 w_1^{x_1} \alpha_2 w_2^{x_2} \cdots \alpha_n w_n^{x_n} \alpha_{n+1} \in M_{\overline{\alpha}}^{\overline{w}}$. For each $L \subseteq M_{\overline{\alpha}}^{\overline{w}}$, let $\mathscr{S}_{\overline{\alpha}}^{\overline{w}}(L) \subseteq \mathbb{N}^n$ be the *set of vectors associated with the words of L*.

It turns out that for languages $L \subseteq M_{\overline{\alpha}}^{\overline{w}}$ definable in $+$-inv-$\mathrm{FO}(<)$, $\mathscr{S}_{\overline{\alpha}}^{\overline{w}}(L)$ is *semi-linear* in the following sense: A set $S \subseteq \mathbb{N}^n$ is called *linear* if there exist a number $t \in \mathbb{N}$ and vectors $v_0, \ldots, v_t \in \mathbb{N}^n$ such that

$$ S = v_0 + \mathbb{N}v_1 + \cdots + \mathbb{N}v_t. $$

A set $S \subseteq \mathbb{N}^n$ is called *semi-linear* if S is empty or S is a finite union of linear sets.

A set $S \subseteq \mathbb{N}^n$ is called *first-order definable in* $(\mathbb{N}, <, +)$ if there is a $\mathrm{FO}(<, +)$-formula $\varphi(y_1, \ldots, y_n)$ such that $S = \{(x_1, \ldots, x_n) \in \mathbb{N}^n : (\mathbb{N}, <, +) \models \varphi(x_1, \ldots, x_n)\}$.

Theorem 4.3 ([6]). *A set $S \subseteq \mathbb{N}^n$ is first-order definable in $(\mathbb{N}, <, +)$ if and only if it is semi-linear.*

Using Theorem 4.3 along with a standard FO interpretation, it is easy to prove the following (in fact, the lemma is true not only for $+$-inv-$\mathrm{FO}(<)$, but even for $\mathrm{FO}(<, +)$) (see Appendix C.1):

Lemma 4.4. *Let $L \subseteq M_{\overline{\alpha}}^{\overline{w}}$ be a language that is definable in $+$-inv-$\mathrm{FO}(<)$. Then $\mathscr{S}_{\overline{\alpha}}^{\overline{w}}(L)$ is semi-linear.*

It is easy to see that there are non-regular languages such that the associated set of vectors is semi-linear. Hence, in order to derive regularity, we need to show that the set of vectors associated with a language definable in $+$-inv-$\mathrm{FO}(<)$ has a special property.

For this, we use Ginsburg and Spanier's characterization [8] of *regular* bounded languages by subsets of $\mathbb{N}^n$ that we call *semi-diced* here[2]: A set $S \subseteq \mathbb{N}^n$ is called *diced* if there exist a number $t \in \mathbb{N}$, an arbitrary vector $v_0 \in \mathbb{N}^n$, and vectors $v_1, \ldots, v_t \in \mathbb{N}^n$ **each of which has exactly one non-zero component**, such that $S = v_0 + \mathbb{N}v_1 + \cdots + \mathbb{N}v_t$. S is called *semi-diced* if S is empty or S is a finite union of diced sets. In [8] it was shown that a bounded language is regular iff its associated set of vectors is semi-diced. From this, we obtain:

Theorem 4.5 (Immediate from [8]). *Let $L \subseteq M_{\overline{\alpha}}^{\overline{w}}$. Then, L is regular iff $\mathscr{S}_{\overline{\alpha}}^{\overline{w}}(L)$ is semi-diced.*

For proving Proposition 4.2, it therefore suffices to show that for a language definable in $+$-inv-$\mathrm{FO}(<)$, the associated set is semi-diced. This is our goal throughout the remainder of Section 4. For achieving this goal, we give in Section 4.1 characterizations for semi-linear sets and semi-diced sets. Based on these characterizations, in Section 4.2 we use a game argument to show that for every $+$-inv-$\mathrm{FO}(<)$-definable bounded language L, the semi-linear set $\mathscr{S}_{\overline{\alpha}}^{\overline{w}}(L)$ is actually semi-diced.

---

[2]Ginsburg and Spanier did not assign a particular name to these sets

4.1 Semi-linear sets and semi-diced sets

For $x \in \mathbb{Z}^n$ let $||x|| := \sum_{i=1}^{n} |x_i|$. For $K \geqslant 0$, we write $N_K(x)$ to denote the K-neighborhood of x, i.e.,

$$N_K(x) := \{y \in \mathbb{Z}^n : ||x - y|| \leqslant K\}.$$

For $S \subseteq \mathbb{N}^n$, $x, y \in \mathbb{N}^n$, and $K \in \mathbb{N}$ we say that $N_K(x)$ and $N_K(y)$ are identical with respect to S if for all $z \in \mathbb{Z}^n$ with $||z|| \leqslant K$ we have $x + z \in S \iff y + z \in S$.

We believe that the next lemma, which essentially says that any semi-linear set is ultimately periodic, is known to researchers in the area of algebra and number theory. Note, however, that Muchnik [15] gave a characterization of semi-linear sets based on a similar closure property that differs with the one stated in the lemma in the fact that it does not include the universal quantification over j (it is assuming $j = 1$). As this extra quantification will be important for us, and since we are not aware of a reference that contains a proof of the closure property as stated below, we included a proof in Appendix C.3.

Lemma 4.6. *For every semi-linear set $S \subseteq \mathbb{N}^n$ there exists a finite set $U \subseteq \mathbb{N}^n \setminus \{\mathbf{0}\}$ such that $\forall K \in \mathbb{N}$, $\exists \ell \in \mathbb{N}$ such that the following is true: $\forall x \in \mathbb{N}^n$ with $||x|| \geqslant \ell$, $\exists u \in U$ such that $\forall j \in \mathbb{N}$, $N_K(x)$ and $N_K(x + j \cdot u)$ are identical with respect to S.*

Lemma 4.6 will be our starting point for showing that the set of vectors associated with a language definable in +-inv-FO($<$) is semi-diced. The second ingredient is a characterization of semi-diced sets analogous to the one given in [15] for semi-linear sets. A *section* of a set $S \subseteq \mathbb{N}^n$ is any set of the form $S_{i,\ell} := \{x = (x_1, \dots, x_n) \in S : x_i = \ell\}$, where $i \in \{1, \dots, n\}$ and $\ell \in \mathbb{N}$.

Theorem 4.7. *A set $S \subseteq \mathbb{N}^n$ is semi-diced iff the following is true: (a) every section of S is semi-diced, and (b) there exists a finite set $V \subseteq \mathbb{N}^n \setminus \{\mathbf{0}\}$ such that **every element in V has exactly one non-zero coordinate** and $\forall K \in \mathbb{N}$, $\exists \ell \in \mathbb{N}$ such that the following is true: $\forall x \in \mathbb{N}^n$ with $||x|| \geqslant \ell$, $\exists v \in V$ such that $N_K(x)$ and $N_K(x + v)$ are identical with respect to S.*

The proof of the "only if" direction is straightforward. The proof of the "if" direction is more elaborate. It proceeds by induction on $|V|$; details can be found in Appendix C.4.

4.2 Proof of Proposition 4.2

Fix a language $L \subseteq M_{\overline{\alpha}}^{\overline{w}}$ that is definable in +-inv-FO($<$). Let $S \subseteq \mathbb{N}^n$ be $\mathscr{S}_{\overline{\alpha}}^{\overline{w}}(L)$. By Theorem 4.5 it suffices to show that S is semi-diced. By Theorem 4.7 it suffices to show that S has the properties (a) and (b) stated in Theorem 4.7. The most difficult part is to show property

(b). Property (a) then follows essentially by induction on n. The induction argument can be found in Appendix C.5. We sketch here the proof for property (b).

By Lemma 4.4, S is semi-linear. Let U be the finite set given by Lemma 4.6 for S.

For any vector $u = (u_1, \dots, u_n)$, we let $supp(u) := \{i \in \{1, \dots, n\} : u_i \neq 0\}$ be the *support* of u. We choose

$$V := \{ ||u|| \cdot e_i : u \in U \text{ and } i \in supp(u) \}, \quad (7)$$

where e_i is the unit vector of $\mathbb{N}^n$ which has a 1 in its i-th component and 0s in all other components. Clearly, V is a finite subset of $\mathbb{N}^n$, and every element in V has exactly one non-zero coordinate. We need to show that V has the desired property formulated in Theorem 4.7.

Let $K_0 := \max\{||v|| : v \in V\}$. Now let $K \in \mathbb{N}$ be an arbitrary number. Let $\hat{K} := K + K_0$. Choose ℓ to be the number obtained from Lemma 4.6 for the number $\hat{K}$.

Now let $x \in \mathbb{N}^n$ be an arbitrary vector with $||x|| \geqslant \ell$. By Lemma 4.6 we obtain an $u \in U$ such that for all $j \in \mathbb{N}$, $N_{\hat{K}}(x)$ and $N_{\hat{K}}(x + ju)$ are identical with respect to S.

If $|supp(u)| = 1$, then $u \in V$, and by choosing $v := u$ and $j := 1$ we obtain that $N_K(x)$ and $N_K(x+v)$ are identical with respect to S, and we are done.

For the remainder of this proof we consider the case that $|supp(u)| \geqslant 2$. In order to simplify the presentation, we assume that $supp(u) = \{1, 2\}$ (the general case is based on the same ideas and is presented in Appendix C.5). We choose $v := ||u|| \cdot e_1$. By (7) we have $v \in V$. Our goal is to prove that $N_K(x)$ and $N_K(x+v)$ are identical with respect to S. To this end, let us fix an arbitrary $z \in \mathbb{Z}^n$ with $||z|| \leqslant K$. We need to show that $x + z \in S \iff x + v + z \in S$. This is a consequence of the following claim.

Claim 4.8. *There exists a $J \in \mathbb{N}$ such that $x + Ju + u + z \in S \iff x + Ju + v + z \in S$.*

Before proving this claim, let us point out how to use the claim for showing that $x + z \in S \iff x + v + z \in S$.

Let J be chosen according to Claim 4.8. We know that $N_{\hat{K}}(x)$, $N_{\hat{K}}(x+Ju)$, and $N_{\hat{K}}(x+(J+1)u)$ are identical with respect to S. Furthermore, $||z|| \leqslant K$ and $||v|| \leqslant K_0$, thus $||z + v|| \leqslant K + K_0 = \hat{K}$. Therefore,

$$
\begin{aligned}
x + z \in S &\iff x + (J+1)u + z \in S && \text{since } ||z|| \leqslant \hat{K} \\
&\iff x + Ju + v + z \in S && \text{by Claim 4.8} \\
&\iff x + v + z \in S && \text{since } ||v + z|| \leqslant \hat{K}.
\end{aligned}
$$

In summary, we obtain that $N_K(x)$ and $N_K(x + v)$ are identical with respect to S. Therefore, in order to finish the proof of Proposition 4.2, it suffices to prove Claim 4.8. This is, where the game argument comes in.

Proof of Claim 4.8. We make use of a result similar to Proposition 3.5, in order to reduce the existence of a winning strategy in a game with addition to the existence of

8

a winning strategy in another game, where addition is not present.

Proposition 4.9 (Immediate from [18])**.** *For all $m, h, k' \in \mathbb{N}$ there is a number $r = r(m, h, k') \in \mathbb{N}$ and an infinite set $P = \{ p_1 < p_2 < p_3 < \cdots \} \subseteq \mathbb{N}$ with $p_1 > h$ and $p_j \equiv h \, [m]$, for all $j \geqslant 1$, such that the following is true for all $d, d' \in \mathbb{N}_{\geqslant 1}$:*

if $\mathbf{0}^d \mathbf{0}^{d'} \mathbf{1}^d \mathbf{2}^d \;\approx_r^< \; \mathbf{0}^d \mathbf{1}^{d'} \mathbf{1}^d \mathbf{2}^d$

then $(\mathbb{Z}, <, +, P, P_0, P_1, P_2) \approx_{k'}^+ (\mathbb{Z}, <, +, P, P_0', P_1', P_2')$,

where, for $d_j = d' + jd$, $P_0 = \{p_1, \dots, p_{d_1}\}$, $P_1 = \{p_{d_1+1}, \dots, p_{d_2}\}$, $P_2 = \{p_{d_2}, \dots, p_{d_3}\}$, *while* $P_0' = \{p_1, \dots, p_d\}$, $P_1' = \{p_{d+1}, \dots, p_{d_2}\}$, $P_2' = P_2$.

From Proposition 4.9, the result essentially follows by an FO interpretation. We here present the main ideas underlying this interpretation; the details are given in Appendix C.5.

For any $\chi := (\chi_1, \dots, \chi_n) \in \mathbb{N}^n$, let $\mathcal{W}(\chi)$ be the word $w_1^{\chi_1} \cdots w_n^{\chi_n}$. We let $H := \alpha_1 \alpha_2 \cdots \alpha_{n+1} \mathcal{W}(x+z)$, $U_0 := \mathcal{W}(u)$, $U_1 := \mathcal{W}(u + e_1 - e_2)$ and $U_2 := \mathcal{W}(u - e_1 + e_2)$. We then set $h := |H|$ and $m := |U_0|$. Notice that by our assumption on $|w_1| = \cdots = |w_n|$, we have $|U_0| = |U_1| = |U_2| = m$. For any given $k' \in \mathbb{N}$ let r and $p_1, p_2, \dots$ be the numbers given by Proposition 4.9 with these values of m, h and k'. Let d' be the second component of u, and let d be such that $\mathbf{0}^d \mathbf{0}^{d'} \mathbf{1}^d \mathbf{2}^d \;\approx_r^< \; \mathbf{0}^d \mathbf{1}^{d'} \mathbf{1}^d \mathbf{2}^d$ (the existence of d is guaranteed by standard Ehrenfeucht-Fraïssé game results [11]). By Proposition 4.9 we then have:

$$(\mathbb{Z}, <, +, P, P_0, P_1, P_2) \;\approx_{k'}^+ \; (\mathbb{Z}, <, +, P, P_0', P_1', P_2') \quad (8)$$

In order to transfer identity (8) into an identity over strings, we use an FO interpretation similar to the one given in the proof of Lemma 3.4 for assigning labels to numbers. This interpretation uses H for labeling the positions 0 up to $h-1$. For every $i \in \{\mathbf{0}, \mathbf{1}, \mathbf{2}\}$, it uses U_i for labeling m consecutive positions, the first of which is marked by P_i. Furthermore, it uses U_0 (and counting modulo m) for labeling all remaining positions. Thus, the interpretation transforms the structures of (8) into the strings

$$H \, (U_0)^{i_0} \left(U_0 \, U_0^{i_j} \right)_{j=1}^{d_1} \left(U_1 \, U_0^{i_j} \right)_{j=d_1+1}^{d_2} \left(U_2 \, U_0^{i_j} \right)_{j=d_2+1}^{d_3}$$

and

$$H \, (U_0)^{i_0} \left(U_0 \, U_0^{i_j} \right)_{j=1}^{d} \left(U_1 \, U_0^{i_j} \right)_{j=d+1}^{d_2} \left(U_2 \, U_0^{i_j} \right)_{j=d_2+1}^{d_3}$$

where $i_0 = (p_1 - h)/m$, and for $j \geqslant 1$, $i_j = (p_{j+1} - p_j - m)/m$. Denoting these strings by V and W, and letting k_1 be the quantifier rank of the FO interpretation, we obtain from (8) that

$$V \approx_{k'-k_1}^+ W. \quad (9)$$

Now let us consider the vector y_V (resp. y_W) in $\mathbb{N}^n$ that counts the number of occurrences of each of the w_i in the string V (resp. W), i.e.,

$$y_V = x + z + \left(\sum_{j=0}^{d_3} i_j \right) \cdot u + 3d \cdot u + d' \cdot u$$

$$\quad (10)$$

$$y_W = x + z + \left(\sum_{j=0}^{d_3} i_j \right) \cdot u + 3d \cdot u + d' \cdot (u + e_1 - e_2).$$

Recall that $supp(u) = \{1, 2\}$, and d' is the second component of u. Thus, $v = \|u\| \cdot e_1 = u + d' \cdot (e_1 - e_2)$. By setting $J := \left(\sum_{j=0}^{d_3} i_j \right) + 3d + d' - 1$, we therefore have that $y_V = x + z + Ju + u$ and $y_W = x + z + Ju + v$.

In view of (10) and (9), in order to conclude the proof of Claim 4.8, it would suffice to have an FO interpretation similar to the one in the proof of Claim 3.2 transforming the strings V and W into strings in $M_{\overline{\alpha}}^{\overline{w}}$.

However, depending on the shape of $\overline{\alpha}$ and $\overline{w}$, it might be the case that such an FO interpretation does not exist, because once in the middle of the string V or W, there is no way of distinguishing a letter in a copy of w_i from the same letter in a copy of w_j, for $i \neq j$. This problem is overcome in the same way as in Section 3.1, by using an expanded alphabet when performing the first interpretation after applying Proposition 4.9. The alphabet would be of the form $\Delta := \Sigma \times \{w, \alpha\} \times \{1, \dots, n+1\}$ and, in the argument above, instead of working with the strings w_i (resp., α_i), we use strings $\tilde{w}_i$ (resp., $\tilde{\alpha}_i$) in Δ^*, obtained by expanding the label of each letter in the obvious way.

Once this is done, we can conclude in the same way as in the proof of Claim 3.2. I.e., we construct an FO$(<, +)$-formula ψ_{Ord} defining a linear order such that reading the letters of V and W according to this linear order, one obtains the strings $\alpha_1 w_1^{y_1} \alpha_2 \cdots \alpha_n w_n^{y_n} \alpha_{n+1}$ and $\alpha_1 w_1^{y_1'} \alpha_2 \cdots \alpha_n w_n^{y_n'} \alpha_{n+1}$, for $(y_1, \dots, y_n) = y_V$ and $(y_1', \dots, y_n') = y_W$. Letting k_2 be the quantifier rank of the formula ψ_{Ord} and choosing k' large enough such that $k' - k_1 - k_2$ is bigger than the quantifier rank of the $+$-inv-FO$(<)$-formula that defines L, we obtain that $y_V \in S$ iff $y_W \in S$. This concludes the proof of Claim 4.8. The missing details can be found in Appendix C.5. $\quad\square$

5   Commutative languages, colored sets, and deterministic context-free languages

Commutative languages.   Recall that we call a language L *commutative* if for any string $u \in L$, any permutation of the letters of u is in L. As an easy consequence of Theorem 4.1, we obtain:

Theorem 5.1. *Every commutative language definable in $+$-inv-FO$(<)$ is regular.*

Proof. For a string $w = w_1 w_2 \cdots w_\ell$ of length $\ell \in \mathbb{N}$ and a permutation π of $\{1, \ldots, \ell\}$, be write w_π to denote the string $w_{\pi(1)} w_{\pi(2)} \cdots w_{\pi(\ell)}$. The *commutative closure* $c(L)$ of a language $L \subseteq \Sigma^*$ consists of the strings w_π for all $w \in L$ and all permutations π of $\{1, \ldots, |w|\}$. We use the following result by Ginsburg and Spanier [8], where $n \in \mathbb{N}_{\geqslant 1}$ and $\sigma_1, \ldots, \sigma_n$ are pairwise distinct letters:

Theorem 5.2 ([8]). *A language* $L \subseteq \sigma_1^* \sigma_2^* \cdots \sigma_n^*$ *is regular if and only if the commutative closure* $c(L)$ *is regular.*

The proof of Theorem 5.1 now follows by a simple combination of Theorem 5.2 and Theorem 4.1 (details can be found in Appendix D.1). $\qquad\square$

Colored sets. A *colored set* over Σ is a finite relational structure over the signature $\varrho = \{P_a \ : \ a \in \Sigma\}$, such that the predicates P_a form a partition of the structure's universe. By combining Theorem 5.1 and Theorem 3.16, we immediately obtain the following.

Corollary 5.3. *Over the class of colored sets,* $+\text{-}inv\text{-}\mathrm{FO}(=)$ *and* $\mathrm{FO}(=, lm)$ *have the same expressive power.*

DCFL. By using similar Ehrenfeucht-Fraïssé game arguments as in Section 3.1 and 4.2, along with particular pumping properties of deterministic context-free languages exposed by Valiant in [20], we obtain the following (see the full paper Appendix D.2).

Theorem 5.4. *Every deterministic context-free language definable in* $+\text{-}inv\text{-}\mathrm{FO}(<)$ *is regular.*

6 Discussion

The first main result of this paper is a characterization of the **regular** languages definable in $+\text{-}inv\text{-}\mathrm{FO}(<)$ (resp. $+\text{-}inv\text{-}\mathrm{FO}(+1)$) by the logic $\mathrm{FO}(<, lm)$ (resp. $\mathrm{FO}(+1, lm)$). We also show that a language is definable in $+\text{-}inv\text{-}\mathrm{FO}(=)$ iff it is definable in $\mathrm{FO}(=, lm)$.

We conjecture that $+\text{-}inv\text{-}\mathrm{FO}(<)$ can only define regular languages. If this conjecture were true, our first main result would completely characterize the languages definable in $+\text{-}inv\text{-}\mathrm{FO}(<)$ and $+\text{-}inv\text{-}\mathrm{FO}(+1)$.

As a step towards proving this conjecture, our second main result shows that any language definable in $+\text{-}inv\text{-}\mathrm{FO}(<)$ that is also bounded, commutative, or deterministic context-free, is actually regular, and therefore definable in $\mathrm{FO}(<, lm)$.

Note that if we also have access to multiplication and define $(+, *)\text{-}inv\text{-}\mathrm{FO}$ in the obvious way, this formalism can express non-regular languages (e.g., the language of all strings whose length is a prime number).

As a challenge towards proving or disproving our conjecture, we conclude with the following example of a non-regular, context-free language, that is definable in $(+, *)\text{-}inv\text{-}\mathrm{FO}(<)$ as well as in $\mathrm{FO}(<, +)$, but for which we do not know whether or not it is definable in $+\text{-}inv\text{-}\mathrm{FO}(<)$.

For $n, i \in \mathbb{N}$ we denote by $\mathrm{bin}_n(i)$ (resp., $\overline{\mathrm{bin}}_n(i)$) the $\{0, 1\}$-string w of length n representing the binary encoding of i, starting with the least significant bit (resp., starting with the most significant bit). Let L be the language of strings of the form $\mathrm{bin}_n(0)\#\overline{\mathrm{bin}}_n(1)\#\mathrm{bin}_n(2)\#\overline{\mathrm{bin}}_n(3)\#\cdots\#\overline{\mathrm{bin}}_n(2^n{-}1)$, for $n \in \mathbb{N}$. For instance, L contains the string $000\#001\#010\#011\#001\#101\#011\#111$. Let $\bar{L}$ be the complement of L. We then have (details in Appendix E):

Proposition 6.1. $\bar{L}$ *is context-free and definable in* $(+, *)\text{-}inv\text{-}\mathrm{FO}(<)$ *and in* $\mathrm{FO}(<, +)$.

References

[1] D. A. M. Barrington, N. Immerman, C. Lautemann, N. Schweikardt, and D. Thérien. First-order expressibility of languages with neutral letters or: The Crane Beach conjecture. *J. Comput. Syst. Sci.*, 70(2):101–127, 2005.

[2] D. Beauquier and J.-E. Pin. Factors of words. In *Proc. ICALP*, pages 63–79, 1989.

[3] M. Benedikt and L. Segoufin. Towards a characterization of order-invariant queries over tame structures. *J. of Symbolic Logic*, 74(1):168–186, 2009.

[4] F. D'Alessandro, B. Intrigila, and S. Varricchio. The Parikh counting functions of sparse context-free languages are quasi-polynomials. *Theor. Comput. Sci.*, 410(47-49):5158–5181, 2009.

[5] S. Ginsburg. *The mathematical theory of context-free languages*. McGraw-Hill, New York, 1966.

[6] S. Ginsburg and E. Spanier. Semigroups, Presburger formulas, and languages. *Pacific J. Math.*, 16(2):285–296, 1966.

[7] S. Ginsburg and E. H. Spanier. Bounded ALGOL-like languages. *Trans. of the Amer. Math. Soc.*, 113:333–368, 1964.

[8] S. Ginsburg and E. H. Spanier. Bounded regular sets. *Proc. of the American Math. Soc.*, 17(5):1043–1049, 1966.

[9] M. Grohe and T. Schwentick. Locality of order-invariant first-order formulas. *ACM Trans. Computational Logic*, 1(1):112–130, 2000.

[10] N. Immerman. Relational queries computable in polynomial time. *Information and Control*, 68(1-3):86–104, 1986.

[11] L. Libkin. *Elements of Finite Model Theory*. Springer, 2004.

[12] J. Lynch. On sets of relations definable by addition. *J. of Symbolic Logic*, 47:659–668, 1982.

[13] R. McNaughton and S. Papert. *Counter-free Automata*. MIT Press, 1971.

[14] M. More and F. Olive. Rudimentary languages and second order logic. *Math. Log. Q.*, 43:419–426, 1997.

[15] A. Muchnik. The definable criterion for definability in Presburger arithmetic and its applications. *Theor. Comput. Sci.*, 290:1433–1444, 2003.

[16] D. Raz. Length considerations in context-free languages. *Theor. Comput. Sci.*, 183:21–32, 1997.

[17] N. Schweikardt. On the expressive power of monadic least fixed point logic. *Theor. Comput. Sci.*, 350(2-3):325–344, 2006.

[18] N. Schweikardt. An Ehrenfeucht-Fraïssé game approach to collapse results in database theory. *Information and Computation*, 205(3):311–379, 2007.

[19] H. Straubing. *Finite Automata, Formal Logic, and Circuit Complexity*. Birkhäuser, 1994.

[20] L. G. Valiant. Regularity and related problems for deterministic pushdown automata. *J. ACM*, 22(1):1–10, 1975.

[21] M. Vardi. The complexity of relational query languages. In *Proc. STOC*, pages 137–146, 1982.

APPENDIX

This appendix gives detailed proofs of the article's claims. Parts B, C, D, and E contain detailed proofs of the results in sections 3, 4, 5, and 6, respectively. Part A contains notations and technical material convenient for presenting these proofs.

A   A technical lemma summarizing our Ehrenfeucht-Fraïssé game arguments

Basic notation. We write ε to denote the empty string. For an alphabet Σ, we let $\varrho_\Sigma := \{P_a \, : \, a \in \Sigma\}$ be the signature that consists of a unary relation symbol P_a for each $a \in \Sigma$.

The *standard representation* of a string $w = w_1 \cdots w_N \in \Sigma^*$ of length $N \geqslant 1$ by a ϱ_Σ-structure is the structure

$$\underline{w} \; = \; \big(\, [N], (P_a^w)_{a \in \Sigma} \,\big)$$

with domain $[N] = \{0, \dots, N-1\}$, where, for each $a \in \Sigma$, $P_a^w = \{i \in [N] \, : \, w_{i+1} = a\}$.

The *standard interpretations* of $<$ and $+$ on $\mathbb{Z}$ are the relations

$$\begin{aligned} <^{\mathbb{Z}} \; &:= \; \{(i,j) \, : \, i,j \in \mathbb{Z} \text{ and } i < j\}, \\ +^{\mathbb{Z}} \; &:= \; \{(i,j,k) \, : \, i,j,k \in \mathbb{Z} \text{ and } i+j = k\} \end{aligned}$$

For any $N \in \mathbb{N}_{\geqslant 1}$ and any relation $R^{\mathbb{Z}} \subseteq \mathbb{Z}^r$ (for $r \geqslant 1$) we let $R^N := \{(i_1, \dots, i_r) \in R^{\mathbb{Z}} \, : \, i_1, \dots, i_r \in [N]\}$. For each $N \in \mathbb{N}_{\geqslant 1}$, the *standard interpretation* of $<$ and $+$ on $[N]$ are the relations $<^N$ and $+^N$.

From now on, when the context is clear, we will omit superscripts $\cdot^{\mathbb{Z}}$ (resp. $\cdot^N$) and simply write $<$ and $+$ to denote the *standard interpretations* of $<$ and $+$ on $\mathbb{Z}$ (or $[N]$, for $N \in \mathbb{N}_{\geqslant 1}$).

If $\mathcal{A}$ is a structure whose domain $dom(\mathcal{A})$ is a subset of $\mathbb{Z}$, we write $(\mathcal{A}, <)$ to denote the expansion of $\mathcal{A}$ by the relation $<^{\mathbb{Z}} \cap dom(\mathcal{A})^2$. Accordingly, $(\mathcal{A}, <, +)$ denotes the expansion of $(\mathcal{A}, <)$ by the relation $+^{\mathbb{Z}} \cap dom(\mathcal{A})^3$. Furthermore, if P is a subset of $\mathbb{Z}$, we write $(\mathcal{A}, <, +, P)$ to denote the expansion of $(\mathcal{A}, <, +)$ by an additional unary predicate that is interpreted by the set $P \cap dom(\mathcal{A})$.

If φ is a first-order formula, we write $qr(\varphi)$ to denote the quantifier rank of φ.

EF-games. We use the standard notation concerning Ehrenfeucht-Fraïssé games (EF-games, for short); see e.g. the textbook [11]. In particular, we write $\mathcal{A} \approx_r \mathcal{B}$ to indicate that the duplicator has a winning strategy in the r-round EF-game (for FO) played on two relational structures $\mathcal{A}$ and $\mathcal{B}$ of the same signature.

Furthermore, we will use $dom(\mathcal{A})$ and $dom(\mathcal{B})$ to denote the domain (i.e., the universe) of the structures $\mathcal{A}$ and $\mathcal{B}$, respectively. If τ is the signature of $\mathcal{A}$, we write $\tau^{\mathcal{A}}$ to denote the collection of relations and constants of $\mathcal{A}$. I.e., for every relation symbol R and every constant symbol c in τ, $\tau^{\mathcal{A}}$ contains the relation $R^{\mathcal{A}}$ and the constant $c^{\mathcal{A}}$ with which the symbols R and c are interpreted in $\mathcal{A}$.

If α is a mapping whose domain is $dom(\mathcal{A})$, then $\alpha(R^{\mathcal{A}})$ denotes the set of all tuples $(\alpha(x_1), \ldots, \alpha(x_r))$ for which $(x_1, \ldots, x_r) \in R^{\mathcal{A}}$. By $\alpha(\tau^{\mathcal{A}})$ we denote the collection of relations $\alpha(R^{\mathcal{A}})$ and elements $\alpha(c^{\mathcal{A}})$ for all relation symbols R and constant symbols c in τ.

The following is a generalization of a result by Lynch [12] which was proved in [18] and which establishes a winning strategy for the duplicator in an EF-game on particular structures which have a built-in addition relation.

Proposition A.1 ([18]). *For all $m, h, g, k \in \mathbb{N}$ there is a number $r = r(m, h, g, k) \in \mathbb{N}$ and an infinite set*

$$P = \{ p_1 < p_2 < p_3 < \cdots \} \subseteq \mathbb{N}$$

with $p_1 > h$ and $p_j \equiv h \pmod{m}$, for all $j \geqslant 1$, such that the following is true for every signature τ, all linearly ordered finite $\tau \cup \{<\}$-structures $\mathcal{A}$ and $\mathcal{B}$, and the mappings $\alpha : dom(\mathcal{A}) \to P$ and $\beta : dom(\mathcal{B}) \to P$ which, for each j, map the j-th smallest element of $dom(\mathcal{A})$ w.r.t. the linear order $<^{\mathcal{A}}$ (respectively, of $dom(\mathcal{B})$ w.r.t. $<^{\mathcal{B}}$) to the j-th smallest element in P: If $\mathcal{A} \approx_r \mathcal{B}$, then the duplicator has a winning strategy in the k-round EF-game on

$$\mathfrak{A} := (\mathbb{Z}, <, +, P, \alpha(\tau^{\mathcal{A}})) \text{ and } \mathfrak{B} := (\mathbb{Z}, <, +, P, \beta(\tau^{\mathcal{B}}))$$

such that after the k-th round the following holds true: Let, for every $i \in \{1, \ldots, k\}$, $\mathfrak{a}_i$ and $\mathfrak{b}_i$ be the elements chosen in the i-th round on $\mathfrak{A}$ and $\mathfrak{B}$. Then we have

(I) $\mathfrak{a}_i \equiv \mathfrak{b}_i \ [m]$, for all $i \in \{1, \ldots, k\}$, and

(II) $(\mathfrak{a}_i - \mathfrak{a}_j = \mathfrak{b}_i - \mathfrak{b}_j)$ or $(|\mathfrak{a}_i - \mathfrak{a}_j| > 2g$ and $|\mathfrak{b}_i - \mathfrak{b}_j| > 2g)$, for all $i, j \in \{1, \ldots, k\}$.

This proposition is an immediate consequence of [18, Proposition 6.11 and 6.12].

Using this proposition, we can prove the following lemma that will serve as one of the main technical tools for proving our results on $+\text{-inv-FO}(+1)$ and $+\text{-inv-FO}(<)$.

Lemma A.2. *Let Σ, Δ, Γ be finite alphabets. Let $k' \in \mathbb{N}_{\geqslant 1}$, let $H, G, U \in \Delta^*$ with $|U| \geqslant 1$ and, for each $\gamma \in \Gamma$, let $U_\gamma \in \Delta^*$ with $|U_\gamma| = |U|$. Let $m \geqslant |U|$ be a multiple of $|U|$. For*

$$h := |H|, \quad g := \max\{h, m, |G|\}, \quad k'' := 2k' + 3$$

let $r := r(m, h, g, k'') \in \mathbb{N}$ and $P := \{ p_1, p_2, p_3, \ldots \} \subseteq \mathbb{N}$ be chosen according to Proposition A.1. Let $i_0 := \frac{p_1 - h}{|U|}$ and, for each $j \geqslant 1$, let $i_j := \frac{p_{j+1} - (p_j + |U|)}{|U|}$. In particular, $i_0 \equiv 0 \pmod{\frac{m}{|U|}}$ and, for each $j \geqslant 1$, $i_j \equiv -1 \pmod{\frac{m}{|U|}}$.

Let $v, w \in \Gamma^*$ be strings such that $(\underline{v}, <) \approx_r (\underline{w}, <)$, and let $d_v = |v|$ and $d_w = |w|$. Let $V, W \in \Delta^*$ be the following strings:

$$
\begin{aligned}
V &:= H \, U^{i_0} \left(Q_j \, U^{i_j} \right)_{j=1,\ldots,d_v} G, \\
W &:= H \, U^{i_0} \left(R_j \, U^{i_j} \right)_{j=1,\ldots,d_w} G,
\end{aligned}
$$

where, for each $j \geqslant 1$ and each $\gamma \in \Gamma$ the following is true: If γ is the j-th letter in v (respectively, w), then $Q_j = U_\gamma$ (respectively, $R_j = U_\gamma$). Then, the following holds:

(a) $(\underline{V}, <, +, P) \approx_{k'} (\underline{W}, <, +, P)$.

(b) Let $(\psi_a(x))_{a \in \Sigma}$ be a collection of $\text{FO}(\varrho_\Delta \cup \{<, +, P\})$-formulas which, on each of the structures $(\underline{V}, <, +, P)$ and $(\underline{W}, <, +, P)$, defines a partition of the domain into $|\Sigma|$ disjoint sets, and let $V', W' \in \Sigma^*$ be the strings obtained from V and W by replacing, for each x, the letter at position x with the particular letter $a \in \Sigma$ for which the formula $\psi_a(x)$ is satisfied.

Let $\psi_{Succ}(x, y)$ be a $\text{FO}(\varrho_\Delta \cup \{<, +, P\})$-formula which, when interpreted in $(\underline{V}, <, +, P)$ and $(\underline{W}, <, +, P)$, defines a successor relation on the domain. Let $V'', W'' \in \Sigma^*$ be the strings obtained from reading the letters of V' and W' according to this particular successor relation.

Let q be an upper bound on the quantifier rank of the formulas $\psi_a(x)$, for all $a \in \Sigma$. Then the following is true:

  (i) V'' and W'' satisfy the same $+\text{-inv-FO}(+1)$-sentences of quantifier rank at most $k := k' - \max\{q, qr(\psi_{Succ})\}$.

  (ii) If $\psi_{Ord}(x, y)$ is a $\text{FO}(\varrho_\Delta \cup \{<, +, P\})$-formula which, when interpreted in $(\underline{V}, <, +, P)$ and $(\underline{W}, <, +, P)$, defines the linear order that fits to the successor relation defined by $\psi_{Succ}(x, y)$, then V'' and W'' satisfy the same $+\text{-inv-FO}(<)$-sentences of quantifier rank at most $k := k' - \max\{q, qr(\psi_{Succ}), qr(\psi_{Ord})\}$.

Proof. Ad (a): We apply Proposition A.1 for $\tau := \varrho_\Gamma$ and $\mathcal{A} := (\underline{v}, <)$ and $\mathcal{B} := (\underline{w}, <)$. By assumption we know that $\mathcal{A} \approx_r \mathcal{B}$. Letting α and β be the mappings defined in Proposition A.1, we obtain that the duplicator has a winning strategy in the k''-round EF-game on

$$\mathfrak{A} := (\mathbb{Z}, <, +, P, \alpha(\tau^{\mathcal{A}})) \text{ and } \mathfrak{B} := (\mathbb{Z}, <, +, P, \beta(\tau^{\mathcal{B}}))$$

such that after the k''-th round the following holds true: Let, for every $i \in \{1, .., k''\}$, $\mathfrak{a}_i$ and $\mathfrak{b}_i$ be the elements chosen in the i-th round on $\mathfrak{A}$ and $\mathfrak{B}$. Then we have

(I) $\mathfrak{a}_i \equiv \mathfrak{b}_i \ [m]$, for all $i \in \{1, .., k''\}$, and

(II) $\left(\mathfrak{a}_i - \mathfrak{a}_j = \mathfrak{b}_i - \mathfrak{b}_j \right)$ or
  $\left(|\mathfrak{a}_i - \mathfrak{a}_j| > 2g \text{ and } |\mathfrak{b}_i - \mathfrak{b}_j| > 2g \right)$,
  for all $i, j \in \{1, .., k''\}$.

We let $\mathfrak{A}' := (\underline{V}, <, +, P)$ and $\mathfrak{B}' := (\underline{W}, <, +, P)$. Recall that $P = \{p_1 < p_2 < p_3 < \cdots\}$ and note that the string V (resp. W) is defined in such a way that (when making the convention that the first letter of H is at position 0), the first letter of Q_j (resp. R_j) is at position p_j (for each $j \geqslant 1$).

For showing that $\mathfrak{A}' \approx_{k'} \mathfrak{B}'$, we use the duplicator's winning strategy in the $k'' = 2k' + 3$-round EF-game on $\mathfrak{A}$ and $\mathfrak{B}$.

For finding a strategy for the duplicator in the game on $\mathfrak{A}'$ and $\mathfrak{B}'$, we let a "virtual duplicator" and a "virtual spoiler" play a game on $\mathfrak{A}$ and $\mathfrak{B}$ as follows: In the first three rounds, the "virtual spoiler" chooses positions $\mathfrak{a}_1 := 0$, $\mathfrak{a}_2 := p_{d_v+1} \in P$ (i.e., the smallest element in P that does not carry any of the letters in Γ), and $\mathfrak{a}_3 := \mathfrak{a}_2 + |G|$ in the structure $\mathfrak{A}$. It is easy to see that — in order to win this "virtual" game on $\mathfrak{A}$ and $\mathfrak{B}$ in such a way that condition (II) is satisfied — the "virtual duplicator" has to answer with $\mathfrak{b}_1 = 0$, $\mathfrak{b}_2 = p_{d_w+1}$ (i.e., the smallest element in P that does not carry any of the letters in Γ in $\mathfrak{B}$), and $\mathfrak{b}_3 = \mathfrak{b}_2 + |G|$. Note that $\mathfrak{a}_3$ (resp. $\mathfrak{b}_3$) is the smallest element that does not belong to the domain of $\mathfrak{A}'$ (resp. $\mathfrak{B}'$).

Now, for each $i \in \{1, .., k'\}$, the i-th round of the "real" game on $\mathfrak{A}'$ and $\mathfrak{B}'$ is played as follows: Let us assume that the spoiler chooses an $\mathfrak{a}_i'$ in $\mathfrak{A}'$ (the case where he chooses $\mathfrak{b}_i'$ in $\mathfrak{B}'$ is symmetric). To find a suitable answer $\mathfrak{b}_i'$ in $\mathfrak{B}'$, the duplicator plays two rounds (namely, rounds $2i+2$ and $2i+3$) of the "virtual" game as follows: first, she assumes that the "virtual spoiler" chooses in round $2i+2$ the particular element $\mathfrak{a}_{2i+2}$ which is the largest integer $\leqslant \mathfrak{a}_i'$ that is congruent h modulo $|U|$. Let $\mathfrak{b}_{2i+2}$ be the "virtual duplicator's" answer in $\mathfrak{B}'$.
Next, in round $2i+3$, the "virtual spoiler" chooses $\mathfrak{a}_{2i+3} := \mathfrak{a}_i'$. As $|\mathfrak{a}_{2i+3} - \mathfrak{a}_{2i+2}| < |U| \leqslant m \leqslant g$, we obtain that according to condition (II), which is enforced by the "virtual duplicator's" winning strategy on $\mathfrak{A}$ and $\mathfrak{B}$, the "virtual duplicator" then answers with the particular element $\mathfrak{b}_{2i+3}$ that has the same distance from $\mathfrak{b}_{2i+2}$ as $\mathfrak{a}_{2i+3}$ has from $\mathfrak{a}_{2i+2}$, i.e., $\mathfrak{b}_{2i+3} = \mathfrak{b}_{2i+2} + (\mathfrak{a}_i' - \mathfrak{a}_{2i+2})$.
Note that since $\mathfrak{a}_{2i+3} = \mathfrak{a}_i'$ is a position in $\mathfrak{A}'$, we know that $0 = \mathfrak{a}_1 \leqslant \mathfrak{a}_{2i+3} < \mathfrak{a}_3$. Thus, since the "virtual duplicator" wins the "virtual" game on $\mathfrak{A}$ and $\mathfrak{B}$, we also have $0 = \mathfrak{b}_1 \leqslant \mathfrak{b}_{2i+3} < \mathfrak{b}_3$. Hence, $\mathfrak{b}_{2i+3}$ belongs to the domain of $\mathfrak{B}'$, and thus the duplicator in the "real" game on $\mathfrak{A}'$ and

$\mathfrak{B}'$ can choose the element $\mathfrak{b}_i' := \mathfrak{b}_{2i+3}$ in $\mathfrak{B}'$ as her answer in the i-th round of the "real" game on $\mathfrak{A}'$ and $\mathfrak{B}'$.

It is straightforward (but tedious) to check that after k' rounds of the "real" game on $\mathfrak{A}'$ and $\mathfrak{B}'$ (i.e., after $k'' = 2k' + 3$ rounds of the "virtual" game on $\mathfrak{A}$ and $\mathfrak{B}$), the duplicator has won the game on $\mathfrak{A}'$ and $\mathfrak{B}'$. — To see this, use the fact that the "virtual duplicator" wins the "virtual" game on $\mathfrak{A}$ and $\mathfrak{B}$ in such a way that the conditions (I) and (II) are satisfied, and note the following:

- If $\mathfrak{a}_i' = \mathfrak{a}_{2i+3}$ is one of the positions in H, then, in particular, $\mathfrak{a}_i' < h \leqslant g$, and due to (II) we have $\mathfrak{b}_i' = \mathfrak{b}_{2i+3} = \mathfrak{a}_{2i+3} = \mathfrak{a}_i'$. In particular, position $\mathfrak{a}_i'$ in $\mathfrak{A}'$ carries the same letter as position $\mathfrak{b}_i'$ in $\mathfrak{B}'$.

- Similarly, if $\mathfrak{a}_i' = \mathfrak{a}_{2i+3}$ is one of the positions in G, then $\mathfrak{b}_i' = \mathfrak{b}_{2i+3}$ has the same distance from $\mathfrak{b}_3$ as $\mathfrak{a}_i'$ has from $\mathfrak{a}_3$. In particular, position $\mathfrak{b}_i'$ in $\mathfrak{B}'$ carries the same letter as position $\mathfrak{a}_i'$ in $\mathfrak{A}'$.

- With the same reasoning one obtains that if $\mathfrak{a}_i'$ is a position that neither belongs to H nor to G, then also $\mathfrak{b}_i'$ is a position that neither belongs to H nor to G. Furthermore, we know from (I) that $\mathfrak{a}_i' \equiv \mathfrak{b}_i' \ [m]$ and, since m is a multiple of $|U|$, also $\mathfrak{a}_i' \equiv \mathfrak{b}_i' \ [|U|]$.

Along the particular choice of the duplicator's strategy, it is not difficult to see that there exists a $p \in P$ such that $0 \leqslant \mathfrak{a}_i' - p < |U|$ if, and only if, there exists a $q \in P$ such that $\mathfrak{b}_i' - q = \mathfrak{a}_i' - p$, and, moreover, position p in $\mathfrak{A}$ carries the same letter from Γ as position q in $\mathfrak{B}$ (to see this note that, if such p and q exist, then $p = \mathfrak{a}_{2i+2}$ and $q = \mathfrak{b}_{2i+2}$).
Recall that $|U| = |Q_j| = |R_j|$ (for any $j \geqslant 1$).

  - If, for $p, q \in P$, $\mathfrak{a}_i' - p = \mathfrak{b}_i' - q =: \delta \in \{0, .., |U|-1\}$, then we know from the particular choice of V and W that both, $\mathfrak{a}_i'$ in $\mathfrak{A}'$ and $\mathfrak{b}_i'$ in $\mathfrak{B}'$ carry the same letter (namely, the $(\delta+1)$-st letter of U_γ, where γ is the particular letter that positions p and q carry in $\mathfrak{A}$ and $\mathfrak{B}$.

  - On the other hand, if there do not exist $p, q \in P$ such that $0 \leqslant \mathfrak{a}_i' - p < |U|$ and $0 \leqslant \mathfrak{b}_i' - q < |U|$, then we immediately obtain from the definition of V and W and from the fact that $\mathfrak{a}_i' \equiv \mathfrak{b}_i' \ [|U|]$, that $\mathfrak{a}_i'$ in $\mathfrak{A}'$ and $\mathfrak{b}_i'$ in $\mathfrak{B}'$ both carry the $(\delta+1)$-st letter of U, for the particular number $\delta \in \{0, .., |U|-1\}$ with $\mathfrak{a}_i' \equiv h+\delta \ [|U|]$.

Altogether, this completes the proof of part (a) of Lemma A.2.

Ad (b): Let φ a $+$-inv-FO($+1$)-sentence of vocabulary $\varrho_\Sigma \cup \{+1, +\}$ and of quantifier rank at most k. Our aim is to show that $V'' \models \varphi \iff W'' \models \varphi$.

13

To this end let $\tilde{\varphi}$ be the FO($\varrho_\Delta \cup \{<, +, P\}$)-sentence obtained from φ by replacing every atom of the form $P_a(x)$ (for $a \in \Sigma$) by the formula $\psi_a(x)$, and replacing every atom of the form $E(x, y)$ by the formula $\psi_{Succ}(x, y)$. It is not difficult to see that

$$(\underline{V}, <, +, P) \models \tilde{\varphi} \iff V'' \models \varphi, \quad \text{and}$$
$$(\underline{W}, <, +, P) \models \tilde{\varphi} \iff W'' \models \varphi.$$

Furthermore, $\tilde{\varphi}$ has quantifier rank at most $k' = k + \max\{q, qr(\psi_{Succ})\}$. From part (a) of the lemma we know that $(\underline{V}, <, +, P) \approx_{k'} (\underline{W}, <, +, P)$.

Thus, $(\underline{V}, <, +, P) \models \tilde{\varphi} \iff (\underline{W}, <, +, P) \models \tilde{\varphi}$.

In summary, we obtain that $V'' \models \varphi \iff W'' \models \varphi$. I.e., V'' and W'' satisfy the same $+$-inv-FO($+1$)-sentences of quantifier rank at most k, and the proof of part (b) (i) of Lemma A.2 is complete. The proof of part (b) (ii) follows along the same lines. $\qquad \square$

Let us give an easy example of how to use Lemma A.2.

Example A.3. In this example we show that the language $L := \{a^n b^n : n \in \mathbb{N}\}$ is FO($<, +$)-definable, but not $+$-inv-FO($<$)-definable.

It is easy to see that L is FO($<, +$)-definable via a sentence which expresses that there exists a position x such that all positions $\leqslant x$ carry the letter a, all positions $> x$ carry the letter b, and $x + x + 1$ is the maximum position in the domain.

A simple application of Lemma A.2 shows that L is not $+$-inv-FO($<$)-definable: For contradiction, assume that L is definable by a $+$-inv-FO($<$)-sentence φ. Aiming at applying Lemma A.2, choose $\Sigma = \Delta = \{a, b\}$ and $\Gamma = \{\mathbf{0}, \mathbf{1}\}$. Let $k' := 1 + qr(\varphi)$. Let $H = G = \varepsilon$ and $U = ab$, $U_0 = aa$, and $U_1 = bb$. Choose $m := |U| = 2$ and let h, g, k'' and $r := r(m, h, g, k'')$ and $P \subseteq \mathbb{N}$ and i_j (for $j \in \mathbb{N}$) be chosen as in Lemma A.2.

We let $d \in \mathbb{N}_{\geqslant 1}$ be large enough such that

$$(\underline{v}, <) \approx_r (\underline{w}, <)$$

for the strings $v := \mathbf{0}^d \mathbf{1}^d$ and $w := \mathbf{0}^d \mathbf{1}^{d+1}$ (an easy EF-game argument shows that any $d > 2^r$ will do, see e.g. [11]).

Let V and W be chosen as in Lemma A.2, i.e.,

$$V = (ab)^{i_0} \left(aa \, (ab)^{i_j} \right)_{j=1,\dots,d} \left(bb \, (ab)^{i_j} \right)_{j=d+1,\dots,2d}$$
$$W = V \left(bb \, (ab)^{i_{2d+1}} \right)$$

Note that for $\ell_V := \sum_{j=0}^{2d} i_j$ and $\ell_W := \ell_V + i_{2d+1}$, the following is true: The string V consists of $n_V := \ell_V + 2d$ occurrences of the letter a and n_V occurrences of the letter b. The string W consists of $n_W := \ell_W + 2d$ occurrences of the letter a and $n_W + 2$ occurrences of the letter b.

Aiming at applying part (b) of Lemma A.2, let $\psi_a(x) := P_a(x)$ and $\psi_b(x) := P_b(x)$. Furthermore, let $\psi_{Ord}(x, y)$ be a quantifier-free formula which, when interpreted in $(\underline{V}, <)$ and $(\underline{W}, <)$, defines a linear order on the domain of $\underline{V}$ and $\underline{W}$, in which the positions that carry the letter a precede all positions that carry the letter b. For example, we can choose

$$\psi_{Ord}(x, y) :=$$
$$\left(P_a(x) \wedge P_b(y) \right) \vee \bigvee_{c \in \{a,b\}} \left(x < y \wedge P_c(x) \wedge P_c(y) \right).$$

Finally, let $\psi_{Succ}(x, y)$ be a formula (of quantifier rank 1) that defines the successor relation that corresponds to the linear order defined by $\psi_{Ord}(x, y)$. Then, the strings V'' and W'' chosen in Lemma A.2 (b) are exactly the strings $V'' = a^{n_V} b^{n_V}$ and $W'' = a^{n_W} b^{n_W+2}$. In particular, $V'' \in L$ and $W'' \notin L$.

From Lemma A.2 (b) (ii) we obtain that V'' and W'' satisfy the same $+$-inv-FO($<$)-sentences of quantifier rank at most $k = k' - 1$. Since, by our assumption, L is definable by a $+$-inv-FO($<$)-sentence φ of quantifier rank k, this is a contradiction to the fact that $V'' \in L$ and $W'' \notin L$. $\qquad \square$

B Proofs omitted in Section 3

B.1 Missing elements in the proof of Theorem 3.6

Proof of Proposition 3.8:
We start by defining q and then prove the proposition by induction on k.

Let L be a regular language. Recall that $=_L$ denotes the syntactic congruence of L. Let μ_L be the syntactic morphism of L, i.e. the morphism sending a word $u \in \Sigma^*$ to its syntactic equivalence class: $\mu_L(u) = \mu_L(v)$ iff $u =_L v$. Recall that $=_L$ has only finitely many equivalence classes.

Fix a number p and let Σ^p be the strings of length p. Let M_p be the syntactic classes of the strings of length p: $M_p = \mu_L(\Sigma^p)$. As we have only finitely many equivalence classes there must be $p < p'$ such that $M_p = M_{p'}$. Note that this implies that for any $i > p$ and $j \in \mathbb{N}$, we have $M_i = M_{i+j(p'-p)}$. Let $p_1, j \in \mathbb{N}$ be such that $p = p_1 + j(p' - p)$ and $p_1 < (p' - p)$. Let $q = p' - p_1$. Notice that we have $2q = q + p' - p_1 = q + p_1 + j(p' - p) + (p' - p) - p_1 = q + (j + 1)(p' - p)$. Hence we have $M_q = M_{2q}$. A simple induction shows that if u has length 0 modulo q we have $\mu_L(u) \in M_q$. When combined with closure under modulo transfer this yield the following interesting property (known as quasi aperiodicity [19]):

$$\forall x \in \Sigma^*, |x| \equiv 0[q] \text{ implies } x^\omega =_L x^{\omega+1} \quad (11)$$

Indeed, consider x such that $|x| \equiv 0[q]$. By the remark above we have $\mu_L(x^\omega) \in M_q$. Hence there exist z of length

q such that $z =_L x^\omega$. By closure under modulo transfer we have $x^\omega x z^\omega =_L x^\omega z^\omega z$. By definition of ω we have $x^\omega x z^\omega =_L x^{\omega+1}$ and $x^\omega z^\omega z =_L x^\omega$ and (11) is proved.

Hence for any string u and any $j \in \mathbb{N}$, we have

$$j|u| \equiv 0 \ [q] \quad \text{implies} \quad u^\omega =_L u^{\omega+j} \qquad (12)$$

because $u^\omega =_L (u^j)^\omega$ and by (11) $(u^j)^\omega =_L (u^j)^{\omega+1} =_L u^{\omega+j}$.

In particular, by taking $j = q$ in (12), in the proof below, we can assume we have enough copies of v_i^q available, so that any negative integer that may occur is treated as its positive counterpart modulo q.

We now show that q has the desired property by induction on k.

If $k = 1$, hypothesis (4) yields $\delta_1|v_1| \equiv 0 \ [q]$. Therefore, from (12), we obtain

$$X_1 v_1^\omega X_2 \in L \quad \text{iff} \quad X_1 v_1^{\omega+\delta_1} X_2 \in L,$$

as required.

Assume now that $k > 1$. Set $\alpha_i = |v_i|$ for $1 \leqslant i \leqslant k$. Let d be the greatest common divisor (gcd), of $q, \alpha_2, \cdots, \alpha_k$. Then we have by equation (4) that d also divides $\delta_1 \alpha_1$. Let $q' = q/d$ and, for $j > 1$, $\alpha_j' = \alpha_j/d$. Because of $\delta_1 \cdot q' \cdot \alpha_1 = \delta_1 \cdot \alpha_1' \cdot q \equiv 0 \ [q]$, by the observation above we have

$$v_1^\omega =_L v_1^\omega v_1^{\delta_1 q'}. \qquad (13)$$

By the closure of L under modulo transfers, applied with $x = v_1^{\delta_1 \cdot \alpha_j'}$, $z = v_j^{\delta_1 \cdot \alpha_1'}$ (notice that $|x| = |z|$), we also have for all $x' \in \Sigma^*$:

$$v_1^\omega v_1^{\delta_1 \alpha_j'} x' v_j^\omega =_L v_1^\omega x' v_j^\omega v_j^{\delta_1 \alpha_1'}. \qquad (14)$$

By Bézout's identity[3] there exist $\beta_1, \ldots, \beta_k \in \mathbb{Z}$ such that $1 = \beta_1 q' + \beta_2 \alpha_2' + \cdots + \beta_k \alpha_k'$. Thus, we have

$$\delta_1 = \beta_1 \delta_1 q' + \beta_2 \delta_1 \alpha_2' + \cdots + \beta_k \delta_1 \alpha_k'. \qquad (15)$$

By replacing in $x_1 v_1^\omega v_1^{\delta_1} x_2 v_2^\omega v_2^{\delta_2} \cdots x_k v_k^\omega v_k^{\delta_k} x_{k+1}$, δ_1 by the value provided by (15) and applying equations (13) and (14) to each of the terms $v_1^{\beta_1 \delta_1 q'}, v_1^{\beta_2 \delta_1 \alpha_2'}, \ldots, v_1^{\beta_k \delta_1 \alpha_k'}$, we obtain:

$$x_1 v_1^\omega v_1^{\delta_1} x_2 v_2^\omega v_2^{\delta_2} \cdots x_k v_k^\omega v_k^{\delta_k} x_{k+1}$$
$$=_L x_1 v_1^\omega x_2 v_2^\omega v_2^{\delta_2'} \cdots x_k v_k^\omega v_k^{\delta_k'} x_{k+1} \qquad (16)$$

where, for $j > 1$, $\delta_j' = \delta_j + \delta_1 \alpha_j' \beta_j$.

Consider now $\Delta = \delta_2' \alpha_2 + \cdots + \delta_k' \alpha_k = \delta_2 \alpha_2 + \cdots + \delta_k \alpha_k + \delta_1 \alpha_1'(\beta_2 \alpha_2 + \cdots + \beta_k \alpha_k)$. Notice that $(\beta_2 \alpha_2 + \cdots + \beta_k \alpha_k) = d(1 - \beta_1 q') \equiv d \ [q]$ and recall that $\delta_1 \alpha_1' d = $

[3]Recall that Bézout's identity states that the greatest common divisor of non-zero integers $z_1, \ldots, z_n$ can be written as a linear combination of $z_1, \ldots, z_n$ with integer coefficients.

$\delta_1 \alpha_1$. Thus $\Delta \equiv \delta_1 \alpha_1 + \cdots + \delta_k \alpha_k \equiv 0 \ [q]$, and we can conclude by induction that

$$x_2 v_2^\omega v_2^{\delta_2'} \cdots x_k v_k^\omega v_k^{\delta_k'} x_{k+1}$$
$$=_L x_2 v_2^\omega \cdots x_k v_k^\omega x_{k+1}. \qquad (17)$$

Combining (16) and (17) yields the desired result. □

Proof of part (b) of Proposition 3.11:
Let $N_0 = q^2$. The following claim will be useful in the proof.

Claim B.1. *If w is accepted by B, in the decomposition $w_1 \cdots w_n$ given by Lemma 3.10 such that $w_1 u_1^{\delta_1} w_2 u_2^{\delta_2} \cdots w_n$ is accepted by A, we can assume without loss of generality that $n \leqslant N_0$.*

Proof. Assume that $n > N_0$, and let $\alpha_i < q$ such that $\alpha_i \equiv \delta_i \cdot |u_i| \ [q]$. From the choice of n we can find $j_1, \ldots, j_q$ such that $\alpha_{j_m} = \alpha_{j_1}$ for all $m \leqslant q$. Hence, we have $\sum_m \delta_{j_m} |u_{j_m}| \equiv q \cdot \alpha_{j_1} \equiv 0 \ [q]$. We can therefore apply Proposition 3.8 and remove those $u_{j_m}^{\delta_{j_m}}$ without affecting membership in $\mathcal{L}(A)$. By Lemma 3.10 this yields a new decomposition $w = w_1' \cdots w_{n'}'$ with $n' = n - q$. □

For the proof of part (b) of Proposition 3.11, let us assume v and P form a counter for the minimal deterministic automaton B' equivalent to B. Recall that this means that $|P| > 1$. Assume for the sake of a contradiction that v is not a counter for A. Hence there exists some m such that $v^m =_{\mathcal{L}(A)} v^{m+1}$.

Let X be a string such that the run of B' on that string gives a state of P, and consider a string Y such that XY is accepted by B'. Because (v, P) is a counter for B', the string $Xv^\delta Y$ is accepted by B' for any δ that is a multiple of $|P|$. By applying Lemma 3.10 with $w := Xv^\delta Y$, we obtain appropriate *extensions* (in the sense of the lemma) X', Y' of X, Y, and numbers n_j, α_j and strings v_{1j}, v_{2j} such that $v = v_{1j} v_{2j}$, for all $j \in J$, where J is a suitable finite set, such that the string

$$X' \left(v^{n_j} v_{1j} u^{\alpha_j} v_{2j} \right)_{j \in J} Y'$$

is accepted by A.

By Claim B.1 we can assume that $|J| \leqslant N_0$. By taking for δ any multiple of $|P|$ larger than mN_0, we can make sure that one of the n_j is bigger than m. Because $v^m =_{\mathcal{L}(A)} v^{m+1}$, we can insert there one extra copy of v while still being accepted by A. By Lemma 3.10 this implies that $Xv^{\delta+1} Y$ is accepted by B'. Because δ is a multiple of $|P|$, this implies that XvY is accepted by B'.

As all implications above can be reversed, we also have that if XvY is accepted by B', then also XV is accepted by B'. Therefore, we have shown that for all Y, XY is

accepted by B' iff XvY is accepted by B'. Hence, since B' is minimal, the state reached by B' after evaluating Xv is the same as the state reached by B' after evaluating X. This contradicts the fact that $|P| > 1$.

Altogether, we have shown that if (v, P) is a counter of B', then v is a counter of A. It remains to show that if v was a counter for A, then v is no longer a counter for B'. This is essentially a consequence of the construction of B, which is designed for removing the counters of A.

Let v be a counter of A and assume that for some P, (v, P) is a counter for B'. Consider again a string X such that the run of B' on that string gives a state of P, and consider a string Y such that XY is accepted by B. Because (v, P) is a counter for B', we also have that $Xv^\delta Y$ is accepted by B', for any δ that is a multiple of $|P|$. Consider now an accepting run of B on $Xv^{\omega q|P|}Y$, and consider the states reached by B at the end of each of the last lq copies of v in the sequence between X and Y. Some state p must repeat. There are two cases.

In the first one, a different state q occurs between the two occurrences of p. Then we have a non-trivial loop and p is part of a counter for v. In this case, B could therefore make a non-deterministic move and accept also the string $Xv^{\omega q|P|+1}Y$ and therefore XvY.

In the second case, from p, after reading v, B returns to state p, and therefore B could read one more copy of v and accept $Xv^{\omega q|P|+1}Y$.

In both cases, B' accepts XvY. Similarly, one can show that if XvY is accepted by B' then XY is also accepted by B'. As this is true for all Y, the state reached by B' after evaluating Xv is the same as the state reached by B' after evaluating X. This contradicts the fact that $|P| > 1$ and concludes the proof of part (b) of Proposition 3.11. $\qquad\square$

B.2 Proof of Theorem 3.13

Proof of Theorem 3.13:
Let $L \subseteq \Sigma^*$ be a regular language definable in $+$-inv-FO$(+1)$. Let S_L be the syntactic monoid of L, i.e., S_L is the set of equivalence classes of the syntactic congruence $=_L$.

For showing that L is closed under swaps, we let e, f, x, y, z be elements of S_L such that e and f are idempotent. Furthermore, we let $E, F, X, Y, Z \in \Sigma^*$ be shortest strings in e, f, x, y, z, respectively.

Our goal is to prove that $exfyezf = ezfyexf$. For showing this, let A and B be arbitrary stings in Σ^*. It should be clear that, in order to prove the theorem, it suffices to find natural numbers n_V, n'_V, n_W, and n'_W for which we

can show that

$$\underbrace{A\, E^{n_V}\, X\, F^{n_V}\, Y\, E^{n'_V}\, Z\, F^{n'_V}\, B}_{=:\, V''} \in L$$

$$\iff \underbrace{A\, E^{n_W}\, Z\, F^{n_W}\, Y\, E^{n'_W}\, X\, F^{n'_W}\, B}_{=:\, W''} \in L$$

(18)

Aiming at applying Lemma A.2 we let Δ be the alphabet

$$\Sigma \times \{A, B, E, F, X, Y, Z\} \times \{start, -\} \times \{end, -\}.$$

With each of the words A, B, E, F, X, Y, Z, we associate words $\tilde{A}, \tilde{B}, \tilde{E}, \tilde{F}, \tilde{X}, \tilde{Y}, \tilde{Z}$ in Δ^* as follows:

- If $A = A_1 A_2 \cdots A_\ell$ with $A_j \in \Sigma$, then $\tilde{A} := \tilde{A}_1 \tilde{A}_2 \cdots \tilde{A}_\ell$ with $\tilde{A}_j := (A_j, A, \mu, \nu)$, where $(\mu = start \iff j = 1)$ and $(\nu = end \iff j = \ell)$.

- The words $\tilde{B}, \tilde{E}, \tilde{F}, \tilde{X}, \tilde{Y}, \tilde{Z}$ are defined analogously.

Furthermore, let $\Gamma := \{\mathbf{1}\}$, and let $k' := k + 7$, where k is the quantifier rank of the $+$-inv-FO$(+1)$-sentence φ that, by assumption, defines L. Furthermore, we let

$$H := \tilde{A}\tilde{X}\tilde{Y}\tilde{Z}\tilde{B}, \qquad U := \tilde{E}\tilde{F}\tilde{E}\tilde{F},$$
$$G := \tilde{E}\tilde{F}\tilde{E}\tilde{F}\,\tilde{E}\tilde{F}\tilde{E}\tilde{F}, \quad U_\mathbf{1} := U.$$

We choose $m := |U|$ and let h, g, k'' and $r := r(m, h, g, k'')$ and $P = \{p_1, p_2, ...\} \subseteq \mathbb{N}$ and i_j (for $j \in \mathbb{N}$) be chosen as in Lemma A.2. We let $d \in \mathbb{N}$ be a large enough *even* number such that $(\underline{v}, <) \approx_r (\underline{w}, <)$ for $v = \mathbf{1}^{d-1}$ and $w = \mathbf{1}^d$ (an easy EF-game argument shows that any $d > 2^r + 1$ will do, see e.g. [11]).

Let V and W be chosen as in Lemma A.2. I.e., V is

$$\tilde{A}\tilde{X}\tilde{Y}\tilde{Z}\tilde{B}\, (\tilde{E}\tilde{F}\tilde{E}\tilde{F})^{i_0} \left((\tilde{E}\tilde{F}\tilde{E}\tilde{F})^{1+i_j} \right)_{j=1}^{d-1} \tilde{E}\tilde{F}\tilde{E}\tilde{F}\; \tilde{E}\tilde{F}\tilde{E}\tilde{F}$$

and W is

$$\tilde{A}\tilde{X}\tilde{Y}\tilde{Z}\tilde{B}\, (\tilde{E}\tilde{F}\tilde{E}\tilde{F})^{i_0} \left((\tilde{E}\tilde{F}\tilde{E}\tilde{F})^{1+i_j} \right)_{j=1}^{d} \tilde{E}\tilde{F}\tilde{E}\tilde{F}\; \tilde{E}\tilde{F}\tilde{E}\tilde{F}.$$

Aiming at applying part (b) of Lemma A.2 we let, for each $a \in \Sigma$, $\psi_a(x)$ be a (quantifier-free) formula that states that there exist $(j_1, j_2, j_3) \in \{A, B, E, F, X, Y, Z\} \times \{start, -\} \times \{end, -\}$ such that the letter at position x is $(a, j_1, j_2, j_3) \in \Delta$: the formula $\psi_a(x)$ is simply the disjunction of the formulas $P_{(a,j_1,j_2,j_3)}(x)$ for all $(j_1, j_2, j_3) \in \{A, B, E, F, X, Y, Z\} \times \{start, -\} \times \{end, -\}$. Then, the words V' and W' defined in Lemma A.2 are identical to the words V and W, where each letter in Δ is restricted to its first component.

We let

$$\ell_V := i_0 + \left(\sum_{j=1}^{d-1} (1 + i_j) \right) + 2,$$

$$\ell_W := i_0 + \left(\sum_{j=1}^{d-1} (1 + i_j) \right) + (1 + i_d) + 2.$$

16

Note that

$$V' = AXYZB \left(EFEF \right)^{\ell_V},$$
$$W' = AXYZB \left(EFEF \right)^{\ell_W}.$$

We choose

$$n_V := n_V' := \ell_V, \qquad \begin{matrix} n_W := \ell_W + 1, \\ n_W' := \ell_W - 1, \end{matrix} \qquad (19)$$

and let

$$V'' := A E^{n_V} X F^{n_V} Y E^{n_V'} Z F^{n_V'} B,$$
$$W'' := A E^{n_W} Z F^{n_W} Y E^{n_W'} X F^{n_W'} B.$$

Claim B.2. *There is a* $\mathrm{FO}(\tau_\Delta \cup \{<, +, P\})$-*formula* $\psi_{Succ}(x, y)$ *of quantifier rank at most* 7^4 *which, when interpreted in* $(\underline{V}, <, +, P)$ *and* $(\underline{W}, <, +, P)$, *defines a successor relation on the domain such that, when reading the letters of* V' *and* W' *according to this particular successor relation, one obtains the words* V'' *and* W''.

Before proving this claim, let us first note that part (b) (i) of Lemma A.2 then tells us that V'' and W'' satisfy the same $+$-inv-FO($+1$)-sentences of quantifier rank at most $k = k' - 7$. Since k is the quantifier rank of the $+$-inv-FO($+1$)-sentence φ which, by assumption, defines L, we conclude that $V'' \in L \iff W'' \in L$. Recalling equation (18), the proof of Theorem 3.13 therefore is complete after having proved Claim B.2.

Proof of Claim B.2: Note that V' and W' are "permutations" of V'' and W'' in the following sense: V' — as well as V'' — contains one occurrence of each of the substrings A, X, Y, Z, B, and $n_V + n_V' = 2\ell_V$ occurrences of each of the substrings E and F (and the analogous statement holds for W' and W'').

Furthermore, when making the convention that the leftmost position of $\tilde{A}$ is the position 0, we have the following situation: the $\tilde{E}$ directly right to the prefix

$$\tilde{A}\tilde{X}\tilde{Y}\tilde{Z}\tilde{B} \left(\tilde{E}\tilde{F}\tilde{E}\tilde{F} \right)^{i_0}$$

starts at position p_1. Similarly, for every $j' \in \{1, .., d\}$, we have that the $\tilde{E}$ directly right to the prefix

$$\tilde{A}\tilde{X}\tilde{Y}\tilde{Z}\tilde{B} \left(\tilde{E}\tilde{F}\tilde{E}\tilde{F} \right)^{i_0} \left(\left(\tilde{E}\tilde{F}\tilde{E}\tilde{F} \right)^{1+i_j} \right)_{j=1}^{j'}$$

starts at position $p_{j'+1}$.

The formula $\psi_{Succ}(x, y)$ defines the following successor relation *Succ* (where "leftmost", "rightmost", "first", and "last" always corresponds to the natural linear order $<$ available in the schema):

---

[4] 7 is just an upper bound here; when writing down the formulas in detail, one will most probably end up with formulas of quantifier rank smaller than 7.

1. The first position of *Succ* is the first position of the natural linear order $<$.

2. Within each substring of the form $\tilde{A}$, $\tilde{X}$, $\tilde{Y}$, $\tilde{Z}$, $\tilde{B}$, $\tilde{E}$, $\tilde{F}$, *Succ* corresponds to the successor associated with the natural linear order $<$. Note that because we use $\tilde{A}, \tilde{X}, \tilde{Y}, ...$ instead of $A, X, Y, ...$, it is definable in FO whether we are in this case.

3. The *Succ*-successor of the last position in $\tilde{A}$ (i.e., the unique position that carries a letter of the form (a, A, j, end) with $a \in \Sigma$ and $j \in \{start, -\}$) is the first position of the first occurrence, relative to $<$, of $\tilde{E}$.

4. The *Succ*-successor of the last position of the last-but-one occurrence, relative to $<$, of $\tilde{E}$ is the first position of $\tilde{X}$.

5. The *Succ*-successor of the last position in $\tilde{X}$ is the first position of the last-but-one occurrence, relative to $<$, of $\tilde{F}$.

6. The *Succ*-successor of the last position of the first occurrence, relative to $<$, of $\tilde{F}$ is the first position of $\tilde{Y}$.

7. The *Succ*-successor of the last position of $\tilde{Y}$ is the first position of the second occurrence, relative to $<$, of $\tilde{E}$.

8. The *Succ*-successor of the last position of the last occurrence, relative to $<$, of $\tilde{E}$ is the first position of $\tilde{Z}$.

9. The *Succ*-successor of the last position of $\tilde{Z}$ is the first position, relative to $<$, of the last occurrence of $\tilde{F}$.

10. The *Succ*-successor of the last position of the second occurrence, relative to $<$, of $\tilde{F}$ is the first position of $\tilde{B}$.

11. The last position in $\tilde{B}$ is the last position of *Succ*.

12. The *Succ*-successor of the last position (denoted x in the following) of an occurrence, relative to $<$, of $\tilde{E}$ that is neither the last nor the last-but-one occurrence, relative to $<$, of $\tilde{E}$, is chosen as follows:

    - If this particular $\tilde{E}$ starts at a position that belongs to P, then the *Succ*-successor of x is the first position of the next (relative to $<$) occurrence of $\tilde{E}$.

    - If the next (relative to $<$) occurrence of $\tilde{E}$ starts at a position that belongs to P, then the *Succ*-successor of x is the first position (denoted y in the following) of the next-but-next-but-one occurrence of $\tilde{E}$. (I.e., between x and y there are 2 occurrences of $\tilde{E}$.)

    - In all other cases, the *Succ*-successor of x is the first position of the next-but-one (relative to $<$) occurrence of $\tilde{E}$.

13. The *Succ*-successor of the last position (denoted x in the following) of an occurrence of $\tilde{F}$ that is neither the first nor the second occurrence, relative to $<$, of $\tilde{F}$, is chosen as follows: Let x' be the starting position of the particular occurrence of $\tilde{E}$ that ends directly to the left of x, and let y' be such that x' is the *Succ*-successor of y' (note that this y' is uniquely defined in item 12, and y' is the last position of a particular occurrence of $\tilde{E}$). Then, the *Succ*-successor of x is the first position of the first occurrence of $\tilde{F}$ to the right of y'. (Thus, in some sense, the *Succ*-successors corresponding to $\tilde{F}$s are the "reversed"-versions of the *Succ*-successors corresponding to $\tilde{E}$s.)

Note that in $(\underline{V}, <, +, P)$, the predicate P is interpreted by the set $P^V = \{p_1, \ldots, p_d\}$. In $(\underline{W}, <, +, P)$, the predicate P is interpreted by the set $P^W = \{p_1, \ldots, p_d, p_{d+1}\}$. Recall that d is even. Note that the *Succ* relation that is defined through 1–13 forms a path that connects the first position of the first occurrence of $\tilde{E}$ with the first position of the occurrence of $\tilde{E}$ that starts at position p_1, from there on, the path leads to the first positions of the occurrences of $\tilde{E}$ that start at positions p_3, p_5, p_7, etc. Since d is even, the unique *Succ*-path in V that only visits $\tilde{E}$s and starts at the first position of the leftmost $\tilde{E}$ in V, ends at the last position of the last-but-one $\tilde{E}$ in V. Continuing this kind of reasoning, it is not difficult to see that the string obtained by reading the letters of V in the order specified by the relation *Succ*, is exactly the word

$$\tilde{A}\,\tilde{E}^{n_V}\,\tilde{X}\,\tilde{F}^{n_V}\,\tilde{Y}\,\tilde{E}^{n'_V}\,\tilde{Z}\,\tilde{F}^{n'_V}\,\tilde{B}.$$

Similarly, since $d+1$ is odd, the unique *Succ*-path in W that only visits $\tilde{E}$s and starts at the first position of the leftmost $\tilde{E}$ in W, ends at the last position of the last $\tilde{E}$ in W. Continuing this kind of reasoning, it again is not difficult to see that the string obtained by reading the letters of W in the order specified by the relation *Succ*, is exactly the string

$$\tilde{A}\,\tilde{E}^{n_W}\,\tilde{Z}\,\tilde{F}^{n_W}\,\tilde{Y}\,\tilde{E}^{n'_W}\,\tilde{X}\,\tilde{F}^{n'_W}\,\tilde{B}.$$

Finally, it is straightforward to formalize items 1–13 by a first-order formula $\psi_{Succ}(x, y)$ over the signature of $(\underline{V}, <, +, P)$ and $(\underline{W}, <, +, P)$ (which even does not need to make use of the addition predicate $+$).
This completes the proof of Claim B.2 and thus also the proof of Theorem 3.13. $\square$

B.3 Proof of Theorem 3.14

Proof of Theorem 3.14:
Let L be a regular language definable in FO$(+1, lm)$. Then, L is also definable in $+$-inv-FO$(<)$ and therefore is closed under modulo transfers. By Theorem 3.13, it is also closed under swaps. This proves one direction of the theorem.

For the opposite direction, we follow the lines of the proof of Theorem 3.6. Let L be a regular language closed under modulo transfers and under swaps.

Let q be the number given by Proposition 3.8. For $0 \leqslant i < q$, let L_i be the restriction of L to strings of length i modulo q. We show that L_i is definable in FO$(+1, lm)$. This will conclude the proof, as $L = \bigcup_i L_i$. Our goal is to show that $L_i = M \cap Z_i^q$ for some regular language M definable in FO$(+1)$. This implies that M is definable in FO$(+1)$, and therefore L_i is definable in FO$(+1, lm)$.

Let A be the minimal deterministic automaton for L_i. Let B be the automaton constructed from A as in the proof of Theorem 3.6. By Proposition 3.11, B defines an aperiodic language (i.e., the minimal deterministic automaton equivalent to B has no counters). We now use the fact that L_i is closed under swaps to show that also $\mathcal{L}(B)$ is closed under swaps.

Consider a string $XE^nUF^nVE^nWF^nY$ in $\mathcal{L}(B)$, where E and F are idempotents for $\mathcal{L}(B)$. We want to show that $XE^nWF^nVE^nUF^nY$ also belongs to $\mathcal{L}(B)$. By Lemma 3.10 we have that $X'E'U'F'V'E''W'F''Y'$ is accepted by A, where E' is of the form

$$\left(E^{n_j}\, E_{1j}\, u_j^{\delta_j}\, E_{2j} \right)_{j \in J}$$

and similarly for E'', F' and F''. By Claim B.1, we can further assume that $|J| \leqslant N_0$. Hence, by taking $n > \omega q N_0$, we are sure that one of the $n_j > \omega q$. This also holds for E'', F' and F'', hence each of them contains a segment $E^{q\omega}$ or $F^{q\omega}$, which are idempotent for $\mathcal{L}(A)$. We can therefore use that fact that $\mathcal{L}(A)$ is closed under swaps for swapping the corresponding segments, one containing U, the other containing W. Applying Lemma 3.10 again on the resulting string yields the desired result that $\mathcal{L}(B)$ is closed under swaps.

We can now conclude that $\mathcal{L}(B)$ is definable in FO$(+1)$ by using the following well-known theorem.

Theorem B.3 ([2]). *A regular language is definable in* FO$(+1)$ *iff it is aperiodic and closed under swaps.*

Applying this theorem, we obtain that $\mathcal{L}(B)$ is definable in FO$(+1)$. From Proposition 3.11 we know that $L_i = \mathcal{L}(B) \cap Z_i^q$. Thus, L_i (and therefore also $\bigcup_i L_i$) is definable in FO$(+1, lm)$. $\square$

B.4 Proof of Theorem 3.16

Proof of Theorem 3.16:
Obviously, every language definable in $+$-inv-FO$(=)$ has to be commutative. All that remains to show is that a commutative regular language closed under modulo transfers is definable in FO$(=, lm)$. This follows from a simple counting argument:

Fix such a language L, and let q be the number derived from Proposition 3.8. Assume $\Sigma = \{a_1, \dots, a_k\}$. Let f be the function that associates to a string $w \in \Sigma^*$ a tuple $f(w) = (\alpha_1, \cdots, \alpha_k, \beta)$, where α_i is the number of occurrences of a_i in w up to threshold $q \cdot \omega$, while β is the length of w modulo $q \cdot \omega$. Let S be the image of f. Notice that S is a finite set and that for each $\tau \in S$, the language $L_\tau = \{w \mid f(w) = \tau\}$ is definable in $\mathrm{FO}(=, lm)$.

The result then follows from the next lemma, showing that L is of the form $\bigcup_{\tau \in S_L} L_\tau$, for a suitable $S_L \subseteq S$.

Lemma B.4. *For all $w, w' \in \Sigma^*$ with $f(w) = f(w')$ we have: $w \in L$ iff $w' \in L$.*

Proof. For any string u, let $\bar{u}$ be the string $a_1^{i_1} \cdots a_k^{i_k}$, where, for any j, i_j is the number of occurrences of a_j in u. Obviously, $f(u) = f(\bar{u})$. Furthermore, by commutativity of L, we have $u \in L$ iff $\bar{u} \in L$.

Now let w, w' be strings with $f(w) = f(w')$. Our aim is to show that $w \in L$ iff $w' \in L$.

To this end, let $\tau := f(w) = f(w')$. For each $j \in \{1, \dots, k+1\}$, by $\tau[j]$ we refer to the jth element of τ. If all the components in τ are strictly smaller than $q \cdot \omega$, then $\bar{w} = \bar{w}'$ and the lemma is proved.

From now on we assume without loss of generality that $\tau[1] = q \cdot \omega$.

Assume that $\tau[2] = q \cdot \omega$ and that the number of occurrences of a_2 in w is $q \cdot \omega + \alpha$. Then, by modulo transfers, we can, in $\bar{w}$, transfer α occurrences of a_2 into α occurrences of a_1. By repeating this argument for all letters of Σ, we end up in a string $\hat{w}$ such that $f(\hat{w}) = \tau$, $\hat{w} \in L$ iff $\bar{w} \in L$, and a_1 is the only letter occurring strictly more than $q \cdot \omega$ times in $\hat{w}$.

Analogously, we construct $\hat{w}'$ from w'. Notice that $\hat{w}$ and $\hat{w}'$ are identical, except maybe for their number of occurrences of a_1. It remains to show that $\hat{w} \in L$ iff $\hat{w}' \in L$.

Let α be the number of occurrences of a_1 in $\hat{w}$, and let α' be the corresponding number for $\hat{w}'$. By construction, $\alpha > q \cdot \omega$ and, as $f(\hat{w}) = f(\hat{w}')$, we have $\alpha \equiv \alpha' \ [q \cdot \omega]$. From (11) we have, for any $k > 0$, that $a_1^{q\omega} =_L a_1^{kq\omega}$. Therefore, $\hat{w} \in L$ iff $\hat{w}' \in L$, and $w \in L$ iff $w' \in L$.

This completes the proof of Lemma B.4 and the proof of Theorem 3.16. $\square$

C Proofs omitted in Section 4

C.1 Proof of Lemma 4.4

Proof of Lemma 4.4:
According to Theorem 4.3, it suffices to show that the set $S := \mathscr{S}_{\bar{\alpha}}^{\overline{w}}(L)$ is first-order definable in $(\mathbb{N}, <, +)$.

For showing this, it will be convenient to use the following notation. For any (transitive) string u over Σ we write

$\hat{u}$ to denote the $\sigma'[+]$-expansion of u in which the predicate $\prec$ is interpreted by the natural linear order of u (i.e., by E^+, cf. Section 2), and $+$ is interpreted by the addition induced by $\prec$.

For proving Lemma 4.4, we do not really need the assumption that L is $+$-inv-$\mathrm{FO}(<)$-definable. In fact, the following assumption will suffice (note that this assumption is met, in particular, by languages definable in $+$-inv-$\mathrm{FO}(<)$):

> *There is a $\mathrm{FO}(<, \prec, +)$-sentence φ such that for every string $u \in M_{\bar{\alpha}}^{\overline{w}}$ we have: $u \in L$ iff $\hat{u} \models \varphi$.*

Let $S := \mathscr{S}_{\bar{\alpha}}^{\overline{w}}(L)$. Our aim is to find a $\mathrm{FO}(<, +)$-formula φ' with n free variables such that

$$S = \{(x_1, \dots, x_n) \in \mathbb{N}^n : (\mathbb{N}, <, +) \models \varphi'(x_1, \dots, x_n)\}.$$

The straightforward idea is to construct φ' in such a way that, when interpreted in $(\mathbb{N}, <, +)$ for a tuple $(x_1, \dots, x_n) \in \mathbb{N}^n$, it simulates φ when evaluated on $\hat{u}$, for

$$u := \alpha_1 w_1^{x_1} \alpha_2 w_2^{x_2} \cdots \alpha_n w_n^{x_n} \alpha_{n+1}. \qquad (20)$$

To this end, note that the strings $\alpha_1, \dots, \alpha_{n+1}$ and $w_1, \dots, w_n$ are fixed and thus can be "hard-coded" in the formula φ'. In particular, e.g., there is a formula $\psi_i(v, x_i)$ ensuring that $v = |w_i| \cdot x_i$ by stating that

$$v = \underbrace{x_i + \cdots + x_i}_{|w_i|}.$$

Similarly, for every j with $0 \leqslant j < |w_i|$ there is a formula $\chi_{i,j}(v)$ ensuring that v is congruent j modulo $|w_i|$ by stating that there exists a v' such that

$$v = j + \underbrace{v' + \cdots + v'}_{|w_i|}.$$

We choose the formula φ' defining S in $(\mathbb{N}, <, +)$ as

$$\varphi' = \exists y_1 \cdots \exists y_{n+1} \exists z_1 \cdots \exists z_{n+1} (\varphi_1' \wedge \varphi_2'),$$

where φ_1' and φ_2' are defined as follows:

The formula φ_1' ensures that the variables $y_1, \dots, y_{n+1}$ and $z_1, \dots, z_{n+1}$ are interpreted by the following natural numbers:

- $y_1 = 0$,

- for each $i \in \{1, \dots, n\}$, $z_i = y_i + |\alpha_i|$,
$$y_{i+1} = z_i + |w_i| \cdot x_i, \quad \text{and}$$

- $z_{n+1} = y_{n+1} + |\alpha_{n+1}|$.

19

Thus, when identifying the positions of the string u from (20) with the numbers $0, 1, \ldots, |u|-1$, then y_i denotes the first position of α_i in u, z_i denotes the first position of $w_i^{x_i}$ in u (for $i \leqslant n$), and z_{n+1} denotes the first position to the right of u.

The formula φ_2' is obtained from the $\mathrm{FO}(<, \prec, +)$-sentence φ that, by assumption, defines the language L, by

(1) relativizing all quantifications to numbers $< z_{n+1}$,

(2) replacing every atomic subformula of φ of the form $E^+(v_1, v_2)$ or $v_1 \prec v_2$ by the formula $v_1 < v_2$,

(3) replacing every atomic subformula of φ of the form $E(v_1, v_2)$ by the formula
$$\big(v_1 < v_2 \ \wedge \ \neg \exists v_3 (v_1 < v_3 \wedge v_3 < v_2)\big), \quad \text{and}$$

(4) replacing every atomic subformula of φ of the form $P_a(v)$ (for $a \in \Sigma$) by a formula stating that

- either, there is an $i \in \{1, \ldots, n{+}1\}$ such that $y_i \leqslant v < z_i$, and there is a j with $0 \leqslant j < |\alpha_i|$ such that the $(j{+}1)^{\text{st}}$ position of α_i carries the letter a, and $v = y_i + j$,

- or, there is a number $i \in \{1, \ldots, n\}$ such that $z_i \leqslant v < y_{i+1}$, and there is a number j with $0 \leqslant j < |w_i|$ such that the $(j{+}1)^{\text{st}}$ position of w_i carries the letter a, and $v - z_i$ is congruent j modulo $|w_i|$.

It is straightforward to formalize this in $\mathrm{FO}(<, +)$. Furthermore, it can easily be seen that for any $(x_1, \ldots, x_n) \in \mathbb{N}^n$ and the associated string

$$u \ := \ \alpha_1 \, w_1^{x_1} \, \alpha_2 \, w_2^{x_2} \, \cdots \, \alpha_n \, w_n^{x_n} \, \alpha_{n+1}$$

we have:

$$
\begin{aligned}
(\mathbb{N}, <, +) \models \varphi'(x_1, \ldots, x_n) &\iff \hat{u} \models \varphi \\
&\iff u \in L \\
&\iff (x_1, \ldots, x_n) \in S.
\end{aligned}
$$

Thus, S is first-order definable in $(\mathbb{N}, <, +)$ and hence, by Theorem 4.3, S is semi-linear. This completes the proof of Lemma 4.4. $\qquad \square$

C.2 Proof of Theorem 4.5

Proof of Theorem 4.5:
The proof makes use of the following result of Ginsburg and Spanier [8].

Theorem C.1 ([8]). *Let Σ be a finite alphabet, $n \in \mathbb{N}_{\geqslant 1}$, $v_1, \ldots, v_n \in \Sigma^*$, and $L \subseteq v_1^* v_2^* \cdots v_n^*$. Then, L is regular iff the set $\{(x_1, \ldots, x_n) \in \mathbb{N}^n \ : \ v_1^{x_1} v_2^{x_2} \cdots v_n^{x_n} \in L\}$ is semi-diced.*

Now, let $T := \{y = (y_1, \ldots, y_{2n+1}) \in \mathbb{N}^{2n+1} : \alpha_1^{y_1} w_1^{y_2} \alpha_2^{y_3} \cdots \alpha_n^{2n-1} w_n^{y_{2n}} \alpha_{n+1}^{y_{2n+1}} \in L\}$, and let $S := \mathscr{S}_{\alpha}^{\overline{w}}(L) \subseteq \mathbb{N}^n$. By Theorem C.1 we know that L is regular if and only if T is semi-diced. Clearly, $S = \pi_{2,4,6,\ldots,2n}(T)$, where $\pi_{2,4,6,\ldots,2n} : \mathbb{N}^{2n+1} \to \mathbb{N}^n$ denotes the projection onto the "even" components. Our aim is to show that L is regular if and only if S is semi-diced.

For the "only if" direction, assume that L is regular. Then, by Theorem C.1, T is semi-diced. It is straightforward to see that the class of semi-diced sets is closed under projections. Thus, $S = \pi_{2,4,6,\ldots,2n}(T)$ is semi-diced.

For the "if" direction, assume that S is semi-diced. Let $\sigma_1, \ldots, \sigma_n$ be n pairwise distinct letters that do not belong to Σ. Since S is semi-diced, we obtain from Theorem C.1 that the language $L_1 := \{\sigma_1^{x_1} \sigma_2^{x_2} \cdots \sigma_n^{x_n} : (x_1, \ldots, x_n) \in S\}$ is regular. It is then straightforward to see that also the language $L_2 := \{\alpha_1 \sigma_1^{x_1} \alpha_2 \cdots \alpha_n \sigma_n^{x_n} \alpha_{n+1} : (x_1, \ldots, x_n) \in S\}$ is regular. Let $h : \{\sigma_1, \ldots, \sigma_n\} \to \Sigma^*$ be the mapping that substitutes, for every $i \in \{1, \ldots, n\}$, the letter σ_i by the word $h(\sigma_i) := w_i$. Since L_2 is regular, we obtain that also the language $h(L_2) = \{\alpha_1 w_1^{x_1} \alpha_2 \cdots \alpha_n w_n^{x_n} \alpha_{n+1} : (x_1, \ldots, x_n) \in S\}$ is regular. Note that $h(L_2) = L$. Thus, L is regular, and the proof of Theorem 4.5 is complete. $\qquad \square$

C.3 Proof of Lemma 4.6

Proof of Lemma 4.6:
For the proof, we use the following lemma that is implicit in [7] (see the proof of Theorem 6.1 in [7]).

Lemma C.2 ([7]). *Let T be a finite set of linear sets $L \subseteq \mathbb{N}^n$. For each $L \in T$, let $t_L \in \mathbb{N}$ and $v_0^L, \ldots, v_{t_L}^L \in \mathbb{N}^n$ such that $L = v_0^L + \mathbb{N}v_1^L + \cdots + \mathbb{N}v_{t_L}^L$. For the set*

$$M_T := \bigcap_{L \in T} \Big(\mathbb{N}v_1^L + \cdots + \mathbb{N}v_{t_L}^L\Big),$$

the following is true:

(a) *Either $M_T = \{\mathbf{0}\}$, or there exists a number $t_T \in \mathbb{N}_{\geqslant 1}$ and vectors $v_1^T, \ldots, v_{t_T}^T \in \mathbb{N}^n \setminus \{\mathbf{0}\}$ such that $M_T = \mathbb{N}v_1^T + \cdots + \mathbb{N}v_{t_T}^T$.*

(b) *There exists a finite set $C_T \subseteq \mathbb{N}^n$ such that*

$$\bigcap_{L \in T} L \ = \ \bigcup_{c \in C_T} c + M_T.$$

We will use this lemma for proving Lemma 4.6. Obviously, Lemma 4.6 holds if $S = \emptyset$ or $S = \mathbb{N}^n$. Let us thus assume that $\emptyset \neq S \neq \mathbb{N}^n$. Since S is semi-linear, there exists an $r \in \mathbb{N}_{\geqslant 1}$ and linear sets $L_1, \ldots, L_r$ such that

$$S \ = \ L_1 \cup \cdots \cup L_r.$$

The class of semi-linear sets is closed under complementation (cf., Theorem 4.3). Therefore, for each $i \in \{1, \dots, r\}$, the set $\overline{L_i} := \mathbb{N}^n \setminus L_i$ is semi-linear, and there exists an $r_i \in \mathbb{N}_{\geqslant 1}$ and linear sets $L_{i,1}, \dots, L_{i,r_i}$ such that

$$\overline{L_i} = L_{i,1} \cup \cdots \cup L_{i,r_i}.$$

We let $L_{i,0} := L_i$ and consider the collection

$$\mathcal{L} := \{L_{i,j} : i \in \{1, \dots, r\} \text{ and } j \in \{0, \dots, r_i\}\}$$

of the linear sets that all the L_i and $\overline{L_i}$ are composed of.

Every $L \in \mathcal{L}$ is linear, thus there exists a number $t_L \in \mathbb{N}$ and vectors $v_0^L, \dots, v_{t_L}^L \in \mathbb{N}^n$ such that

$$L = v_0^L + \mathbb{N}v_1^L + \cdots + \mathbb{N}v_{t_L}^L.$$

For every $T \subseteq \mathcal{L}$ we let

$$M_T := \bigcap_{L \in T} \left(\mathbb{N}v_1^L + \cdots + \mathbb{N}v_{t_L}^L \right).$$

From Lemma C.2 (a) we know that either $M_T = \{\mathbf{0}\}$, or there exists a number $t_T \in \mathbb{N}_{\geqslant 1}$ and vectors $v_1^T, \dots, v_{t_T}^T \in \mathbb{N}^n \setminus \{\mathbf{0}\}$ such that

$$M_T = \mathbb{N}v_1^T + \cdots + \mathbb{N}v_{t_T}^T.$$

We choose

$$U := \{v_1^T, \dots, v_{t_T}^T : T \subseteq \mathcal{L} \text{ such that } M_T \neq \{\mathbf{0}\}\}.$$

Clearly, U is a finite subset of $\mathbb{N}^n \setminus \{\mathbf{0}\}$.

For each $x \in \mathbb{Z}^n$ let

$$type(x) := \{L \in \mathcal{L} : x \in L\}.$$

Let

$$\mathcal{T} := \{type(x) : x \in \mathbb{Z}^n\}$$

be the set of types that are realizable in $\mathbb{Z}^n$. Note that for every $\tau \in \mathcal{T}$ and every $i \in \{1, \dots, r\}$, the following is true:

$$L_{i,0} \in \tau \iff \text{for all } j \in \{1, \dots, r_i\}, \ L_{i,j} \notin \tau.$$

Therefore, for any $\tau \in \mathcal{T}$ and the set

$$L_\tau := \bigcap_{L \in \tau} L,$$

the following is true:

(1) for all $x, y \in L_\tau$ we have $x \in S \iff y \in S$, and

(2) for all $x \in \mathbb{Z}^n$ with $type(x) = \tau$ we have $x \in L_\tau$.

Now let K be an arbitrary number with $K \in \mathbb{N}$. We let the K-type of x be the mapping

$$type_K(x) : N_K(\mathbf{0}) \to \mathcal{T}$$

which associates with every vector $w \in N_K(\mathbf{0})$ the set $type(x + w)$, i.e.,

$$type_K(x)(w) := type(x + w), \text{ for each } w \in N_K(\mathbf{0}).$$

Let

$$\mathcal{T}_K := \{type_K(x) : x \in \mathbb{Z}^n\}$$

be the set of all realizable K-types. For each $\tau \in \mathcal{T}_K$ let

$$R_\tau := \{ x \in \mathbb{Z}^n :$$
$$\text{for each } w \in N_K(\mathbf{0}) \text{ we have } x + w \in L_{\tau(w)}\}.$$

Note that the following is true for every $\tau \in \mathcal{T}_K$:

(I) for all vectors $x, y \in R_\tau$ and all $w \in N_K(\mathbf{0})$ we have
$$x + w \in S \iff y + w \in S, \quad \text{and}$$

(II) for all vectors $x \in \mathbb{Z}^n$ with $type_K(x) = \tau$ we have
$$x \in R_\tau.$$

Furthermore, $R_\tau =$

$$\bigcap_{\substack{w \in N_K(\mathbf{0}), \\ L \in \tau(w)}} (-w) + L = \bigcap_{\substack{w \in N_K(\mathbf{0}), \\ L \in \tau(w)}} (v_0^L - w) + \mathbb{N}v_1^L + \cdots + \mathbb{N}v_{t_L}^L.$$

For each $\tau \in \mathcal{T}_K$ let $T_\tau :=$

$$\{L \in \mathcal{L} : \text{there is a } w \in N_K(\mathbf{0}) \text{ such that } L \in \tau(w)\}.$$

Recall that for the set

$$M_{T_\tau} = \bigcap_{L \in T_\tau} \mathbb{N}v_1^L + \cdots + \mathbb{N}v_{t_L}^L$$

we know that either $M_{T_\tau} = \{\mathbf{0}\}$ or $M_{T_\tau} = \mathbb{N}v_1^{T_\tau} + \cdots + \mathbb{N}v_{t_{T_\tau}}^{T_\tau}$. Furthermore, from Lemma C.2 (b) we obtain that there is a finite set $C_\tau \subseteq \mathbb{N}^n$ such that

$$R_\tau = \bigcup_{c \in C_\tau} c + M_{T_\tau}.$$

We choose $\ell \in \mathbb{N}$ to be bigger than the norm $|| \cdot ||$ of any element in C_τ for any realizable K-type τ, i.e.,

$$\ell := 1 + \max\{||c|| : c \in \bigcup_{\tau \in \mathcal{T}_K} C_\tau\}.$$

Now let $x \in \mathbb{N}^n$ be an arbitrary vector with $||x|| \geqslant \ell$. Let $\tau := type_K(x)$. Clearly, $x \in R_\tau$. Furthermore, since $||x|| \geqslant \ell$ we know that $M_{T_\tau} \neq \{\mathbf{0}\}$ and thus $M_{T_\tau} = \mathbb{N}v_1^{T_\tau} + \cdots + \mathbb{N}v_{t_{T_\tau}}^{T_\tau}$. In particular, $u := v_1^{T_\tau} \in U$, and $x^{(j)} \in R_\tau$ for every $j \in \mathbb{N}$ and $x^{(j)} := x + ju$. From observation (I) we thus obtain that for any $j \in \mathbb{N}$ and any $w \in N_K(\mathbf{0})$ we have $x + w \in S \iff x^{(j)} + w \in S$. I.e., $N_K(x)$ and $N_K(x^{(j)})$ are identical with respect to S. This completes the proof of Lemma 4.6. $\qquad \square$

C.4 Proof of Theorem 4.7

This section is devoted to the proof of Theorem 4.7. We start with some basic observations on the structure of semi-diced sets.

By using Theorem C.1 (cf., Section C.2), one easily obtains the following closure properties of the class of semi-diced subsets of $\mathbb{N}^n$.

Lemma C.3 (closure properties of semi-diced sets).
The class of all semi-diced sets contains the empty set and every finite subset of $\mathbb{N}^n$ and is closed under union, intersection, complement, taking sections, projection, and cartesian product. In other words: $\emptyset$ is semi-diced, every finite set $F \subseteq \mathbb{N}^n$ is semi-diced, and if $S, T \subseteq \mathbb{N}^n$ are semi-diced, then also $S \cup T$, $S \cap T$ and $\overline{S} := \mathbb{N}^n \setminus S$ are semi-diced. Furthermore, if $S \subseteq \mathbb{N}^n$ is semi-diced, $i \in \{1, \ldots, n\}$, $\ell \in \mathbb{N}$, then $S_{i,\ell}$ is semi-diced. If $S \subseteq \mathbb{N}^n$ and $T \subseteq \mathbb{N}^m$ are semi-diced, then $S \times T \subseteq \mathbb{N}^{n+m}$ is semi-diced. If $S \subseteq \mathbb{N}^n$ is semi-diced, $r \leqslant n$ and $j_1, \ldots, j_r$ are pairwise distinct elements in $\{1, \ldots, n\}$, then and $\pi_{j_1,\ldots,j_r}(S) := \{(x_{j_1}, \ldots, x_{j_r}) : (x_1, \ldots, x_n) \in S\}$ is semi-diced.

Proof. From the definition of semi-diced sets, one immediately obtains the following:

- The empty set $\emptyset$ is semi-diced

- every finite set $F \subseteq \mathbb{N}^n$ is semi-diced,

- the union of two semi-diced sets is semi-diced, and

- if $S \subseteq \mathbb{N}^n$ is semi-diced and $j_1, \ldots, j_r$ are pairwise distinct elements in $\{1, \ldots, n\}$, then $\pi_{j_1,\ldots,j_r}(S)$ is semi-diced.

For proving the remaining closure properties, we apply Theorem C.1 for the special case where the alphabet Σ consists of n pairwise distinct letters $\sigma_1, \ldots, \sigma_n$, with $v_i := \sigma_i$ for every $i \in \{1, \ldots, n\}$.

We use the following notation: For a string w and a letter σ_i we write $|w|_{\sigma_i}$ to denote the number of occurrences of the letter σ_i in w. For a set $S \subseteq \mathbb{N}^n$ we let $\mathscr{L}(S) := \{\sigma_1^{x_1} \sigma_2^{x_2} \cdots \sigma_n^{x_n} : x = (x_1, \ldots, x_n) \in S\}$. For a language $L \subseteq \sigma_1^* \sigma_2^* \cdots \sigma_n^*$ we let $\mathscr{S}(L) := \{x = (x_1, \ldots, x_n) \in \mathbb{N}^n : \sigma_1^{x_1} \sigma_2^{x_2} \cdots \sigma_n^{x_n} \in L\}$. Note that for each $S \subseteq \mathbb{N}^n$ we have $\mathscr{S}(\mathscr{L}(S)) = S$. Similarly, for each $L \subseteq \sigma_1^* \sigma_2^* \cdots \sigma_n^*$ we have $\mathscr{L}(\mathscr{S}(L)) = L$. Theorem C.1 states that $L \subseteq \sigma_1^* \sigma_2^* \cdots \sigma_n^*$ is regular if and only if $\mathscr{S}(L)$ is semi-diced.

For showing closure under intersection, complement, and taking sections let $S, T \subseteq \mathbb{N}^n$ be semi-diced sets. Theorem C.1 tells us that in order to show that $S \cap T$, $\overline{S}$, and $S_{i,\ell}$ are semi-diced, it suffices to show that $\mathscr{L}(S \cap T)$, $\mathscr{L}(\overline{S})$, and $\mathscr{L}(S_{i,\ell})$ are regular. Note that $\mathscr{L}(S \cap T) = \mathscr{L}(S) \cap$

$\mathscr{L}(T)$, $\mathscr{L}(\overline{S}) = \sigma_1^* \sigma_2^* \cdots \sigma_n^* \setminus \mathscr{L}(S)$, and $\mathscr{L}(S_{i,\ell}) = \mathscr{L}(S) \cap \{w \in \sigma_1^* \sigma_2^* \cdots \sigma_n^* : |w|_{\sigma_i} = \ell\}$.

Since S and T are semi-diced, we obtain from Theorem C.1 that $\mathscr{L}(S)$ and $\mathscr{L}(T)$ are regular. Furthermore, the languages $\sigma_1^* \sigma_2^* \cdots \sigma_n^*$ and $\{w \in \sigma_1^* \sigma_2^* \cdots \sigma_n^* : |w|_{\sigma_i} = \ell\}$ are regular. Since the class of regular languages is closed under intersection and complement, the languages $\mathscr{L}(S) \cap \mathscr{L}(T)$, $\sigma_1^* \sigma_2^* \cdots \sigma_n^* \setminus \mathscr{L}(S)$, and $\mathscr{L}(S) \cap \{w \in \sigma_1^* \sigma_2^* \cdots \sigma_n^* : |w|_{\sigma_i} = \ell\}$ are regular. Therefore, $S \cap T, \overline{S}$, and $S_{i,\ell}$ are semi-diced.

For showing closure under cartesian product, let $S \subseteq \mathbb{N}^n$ and $T \subseteq \mathbb{N}^m$ be semi-diced. We view $\mathscr{L}(S)$ as a regular subset of $\sigma_1^* \sigma_2^* \cdots \sigma_n^*$, and we view $\mathscr{L}(T)$ as a regular subset of $\sigma_{n+1}^* \cdots \sigma_{n+m}^*$. Clearly, the concatenation L of $\mathscr{L}(S)$ and $\mathscr{L}(T)$ is regular, and $L = \mathscr{L}(S \times T)$. Due to Theorem C.1, thus $S \times T$ is semi-diced. □

For reasoning about semi-diced sets, it is convenient to note that every semi-diced set is a finite union of *uniformly diced* sets, defined as follows.

Definition C.4 (uniformly diced). A set S is called *uniformly diced* iff there are a vector $v_0 \in \mathbb{N}^n$, a number $q \in \mathbb{N}_{\geqslant 1}$, and a set $I \subseteq \{1, \ldots, n\}$, such that

$$S = v_0 + \sum_{i \in I} \mathbb{N}q e_i .$$

The number q is called the *period* of S.

Lemma C.5. *Every nonempty semi-diced set is a union of a finite number of uniformly diced sets, each with the same period.*

Proof. Let us start with a straightforward observation: For all $a, b \in \mathbb{N}_{\geqslant 1}$,

$$\mathbb{N}a + \mathbb{N}b = \bigcup_{\substack{0 \leqslant a' < b, \\ 0 \leqslant b' < a}} aa' + bb' + \mathbb{N}ab ,$$

and in general, for arbitrary $k \in \mathbb{N}_{\geqslant 1}$, $a_1, \ldots, a_k \in \mathbb{N}_{\geqslant 1}$, $\ell := \mathrm{lcm}\{a_1, \ldots, a_k\}$, and q any multiple of ℓ,

$$\sum_{j=1}^{k} \mathbb{N}a_j = \bigcup_{(0 \leqslant a'_j < q/a_j)_{j=1,\ldots,k}} \left(\sum_{j=1}^{k} a_j a'_j\right) + \mathbb{N}q. \quad (21)$$

Now, let $S = v_0 + \mathbb{N}v_1 + \cdots + \mathbb{N}v_t$ be an arbitrary diced subset of $\mathbb{N}^n$. For each coordinate $i \in \{1, \ldots, n\}$ let J_i be the set of all those $j \in \{1, \ldots, t\}$ such that v_j is a multiple of the i-th unit vector e_i, and let $a_j \in \mathbb{N}_{\geqslant 1}$ such that $v_j = a_j e_i$. Let I be the set of all those $i \in \{1, \ldots, n\}$ such that $J_i \neq \emptyset$. Let $q \in \mathbb{N}_{\geqslant 1}$ be any mulitple of $\mathrm{lcm}\{a_j : j \in \{1, \ldots, t\}\}$. For each $i \in I$ we apply equation (21) to obtain a finite set K_i and numbers $b_{i,k} \in \mathbb{N}$ for all $k \in K_i$ such that

$$\sum_{j \in J_i} \mathbb{N}a_j = \bigcup_{k \in K_i} b_{i,k} + \mathbb{N}q.$$

Now it is easy to see that

$$
\begin{aligned}
S &= v_0 + \sum_{i \in I} \left(\sum_{j \in J_i} \mathbb{N} v_j \right) \\
&= v_0 + \sum_{i \in I} \left(\sum_{j \in J_i} \mathbb{N} a_j e_i \right) \\
&= v_0 + \sum_{i \in I} \left(\bigcup_{k \in K_i} b_{i,k} e_i + \mathbb{N} q e_i \right) \\
&= v_0 + \sum_{i \in I} \left\{ b_{i,k} e_i \ : \ k \in K_i \right\} + \sum_{i \in I} \mathbb{N} q e_i.
\end{aligned}
$$

Thus, every diced set S is a finite union of uniformly diced sets, each with the same period q. From this, one easily obtains that every semi-diced set is the finite union of uniformly diced sets, each with the same period q. □

For proving Theorem 4.7, it will be convenient to use the following notation.

Definition C.6. Let $S, N \subseteq \mathbb{N}^n$, and let $v \in \mathbb{Z}^n$. We say that *v is a period of S in N* if the equivalence

$$
y \in S \iff y + v \in S
$$

is true for all $y \in \mathbb{N}^n$ such that $y \in N$ and $y + v \in N$.

Definition C.7. Let $S, V \subseteq \mathbb{N}^n$.

(a) We say that *S has property $(*)$ with respect to V* if the following is true:

$\forall K \in \mathbb{N}, \exists \ell \in \mathbb{N}$ such that the following is true:
$\forall x \in \mathbb{N}^n$ with $||x|| \geqslant \ell, \exists v \in V$ such that
v is a period of S in $N_K(x)$.

(b) We say that *S has property $(**)$ with respect to V* if the following is true:

$\forall K \in \mathbb{N}, \exists \ell \in \mathbb{N}$ such that the following is true:
$\forall x \in \mathbb{N}^n$ with $||x|| \geqslant \ell, \exists v \in V$ such that
$N_K(x)$ and $N_K(x + v)$ are identical w.r.t. S.

Note that property $(**)$ is used in the formulation of Theorem 4.7. The next lemma is an easy observation showing that, for finite V, property $(*)$ is equivalent to property $(**)$.

Lemma C.8. *Let $S, V \subseteq \mathbb{N}^n$ such that V is finite. Then, S has property $(*)$ w.r.t. V iff S has property $(**)$ w.r.t. V.*

Proof. For the "if" direction it suffices to show the following: If $N_K(x)$ and $N_K(x + v)$ are identical w.r.t. S, then v is a period of S in $N_K(x)$.

Let us therefore assume that $N_K(x)$ and $N_K(x + v)$ are identical w.r.t. S. In order to show that v is a period of S in $N_K(x)$, consider an arbitrary $y \in \mathbb{N}^n$ with $y \in N_K(x)$

and $y + v \in N_K(x)$. Our goal is to show that $y \in S$ iff $y + v \in S$.

Since $y \in N_K(x)$, we have for $z := y - x$, $||z|| \leqslant K$. Since $N_K(x)$ and $N_K(x + v)$ are identical w.r.t. S, we therefore know that $x + z \in S$ iff $x + v + z \in S$. I.e., $y \in S$ iff $y + v \in S$. Thus, v is a period of S in $N_K(x)$.

For the "only if" direction let $K_0 := \max\{||v|| \ : \ v \in V\}$, and note that it suffices to show the following: If v is a period of S in $N_{K+K_0}(x)$, then $N_K(x)$ and $N_K(x + v)$ are identical w.r.t. S.

Let us now assume that v is a period of S in $N_{K+K_0}(x)$. In order to show that $N_K(x)$ and $N_K(x + v)$ are identical w.r.t. S, consider an arbitrary $z \in \mathbb{Z}^n$ with $||z|| \leqslant K$. Our goal is to show that $x + z \in S$ iff $x + v + z \in S$.

Since $||z|| \leqslant K \leqslant K + K_0$ and $||v + z|| \leqslant K + K_0$, we have $x + z \in N_{K+K_0}(x)$ and $x + v + z \in N_{K+K_0}(x)$. Thus, for $y := x + z$ we have $y \in N_{K+K_0}(x)$ and $y + v \in N_{K+K_0}(x)$. Since v is a period of S in $N_{K+K_0}(x)$, we therefore know that $y \in S$ iff $y + v \in S$. Thus, $x + z \in S$ iff $x + v + z \in S$. Hence, $N_K(x)$ and $N_K(x + v)$ are identical w.r.t. S. □

Our proof of Theorem 4.7 will proceed by induction on the size of the set V. The induction base is established by the following lemma.

Lemma C.9. *Let $S \subseteq \mathbb{N}^n$ be a set for which the following is true: (1) There exists a vector v of the form $k \cdot e_i$ (with $k \in \mathbb{N}_{\geqslant 1}$ and $i \in \{1, \ldots, n\}$) such that S has property $(*)$ with respect to the set $V := \{v\}$, and (2) every section $S_{i,\ell}$ (for every $\ell \in \mathbb{N}$) of S is semi-diced. Then, S is semi-diced.*

Proof. For simplicity in notation we assume that $i = 1$, i.e., $v = k \cdot e_1 = (k, 0, \ldots, 0)$. By assumption, S has property $(*)$ with respect to $\{v\}$. Thus, there exists an $\ell \geqslant 0$ such that for every $x \in \mathbb{N}^n$ with $||x|| \geqslant \ell$, v is a period of S in $N_k(x)$. Since x and $x + v$ belong to $N_k(x)$, we therefore know for all $x \in \mathbb{N}^n$ with $||x|| \geqslant \ell$ that $x \in S \iff x + v \in S$. Thus, $v = (k, 0, \ldots, 0)$ is a period of S in the set $\mathbb{N}^n_{\geqslant \ell} := \{x \in \mathbb{N}^n \ : \ ||x|| \geqslant \ell\}$.

Therefore, for an arbitrary $x = (x_1, x_2, \ldots, x_n) \in \mathbb{N}^n$ with $x_1 \geqslant \ell$ the following is true: If $r \in \{0, \ldots, k - 1\}$ and $q \in \mathbb{N}$ such that $x_1 = \ell + r + qk$, then

$$
(x_1, x_2, \ldots, x_n) \in S \iff (\ell + r, x_2, \ldots, x_n) \in S.
$$

By assumption, the section $S_{1,\ell+r}$ is semi-diced, i.e., a finite union of diced sets of the form $v_0 + \mathbb{N} v_1 + \cdots + \mathbb{N} v_t$. Now let $\tilde{S}_{1,\ell+r}$ be the union of the according sets $v_0 + \mathbb{N} v_1 + \cdots + \mathbb{N} v_t + \mathbb{N} v$. Clearly, $\tilde{S}_{1,\ell+r}$ is semi-diced, and $\tilde{S}_{1,\ell+r} =$

$$
\{x = (x_1, x_2, \ldots, x_n) \in S \ : \ x_1 \geqslant \ell \text{ and } x_1 \equiv \ell + r \ [k]\}.
$$

Therefore,

$$
S_{1,\geqslant \ell} := \{x = (x_1, x_2, \ldots, x_n) \in S \ : \ x_1 \geqslant \ell\}
$$

23

is equal to $\bigcup_{r=0}^{k-1} \tilde{S}_{1,\ell+r}$, and thus $S_{1,\geqslant\ell}$ is semi-diced. Furthermore, by assumption we know that each of the sections $S_{1,0}, S_{1,1}, \ldots, S_{1,\ell-1}$ is semi-diced. Since

$$S = S_{1,0} \cup S_{1,1} \cup \cdots \cup S_{1,\ell-1} \cup S_{1,\geqslant\ell},$$

we therefore obtain that S is semi-diced. This concludes the proof of Lemma C.9. $\qquad\square$

For the induction step in our proof of Theorem 4.7, the following notion is convenient.

Definition C.10. Let $S \subseteq \mathbb{N}^n$ and $v \in \mathbb{Z}^n$. The *boundary* $Bd(S, v)$ *of S in the direction v* is the set

$$Bd(S, v) := \{x \in S : x + v \notin S\}.$$

The next two lemmas are analogues of lemmas given in [15]; they will be used for the induction step in our proof of Theorem 4.7.

Lemma C.11. *Let $S \subseteq \mathbb{N}^n$ and let $v \in \mathbb{N}^n$ such that v has exactly one non-zero coordinate. If all sections of S are semi-diced, then all sections of $Bd(S, v)$ and all sections of $Bd(S, -v)$ are semi-diced.*

Proof. For simplicity in notation we assume w.l.o.g. that $v = k \cdot e_1$ for some $k \in \mathbb{N}_{\geqslant 1}$. Consider the (i, ℓ)-section of $Bd(S, v)$ and $Bd(S, -v)$, i.e., the sets $Bd(S, v)_{i,\ell}$ and $Bd(S, -v)_{i,\ell}$. Let $v' \in \{v, -v\}$ and let k' be the first component of v' (i.e., k' is either k or $-k$).

Case 1: $i = 1$. Then, $Bd(S, v')_{1,\ell} =$

$$\{ x = (\ell, x_2, \ldots, x_n) \in S_{1,\ell} :$$
$$(\ell + k', x_2, \ldots, x_n) \notin S_{1,\ell+k'} \}.$$

By assumption, $S_{1,\ell}$ and $S_{1,\ell+k'}$ are semi-diced. Due to Lemma C.3, also the projections of $S_{1,\ell}$ and $S_{1,\ell+k'}$ to the coordinates $2, \ldots, n$ are semi-diced. From Lemma C.3 we know that the class of semi-diced sets is closed under intersection and complement. Therefore, also the set

$$T := \{ (x_2, \ldots, x_n) : (\ell, x_2, \ldots, x_n) \in S_{1,\ell}$$
$$\text{and } (\ell + k', x_2, \ldots, x_n) \notin S_{1,\ell+k'} \}$$

is semi-diced.
  Due to the closure under cartesian product and since the finite set $\{(\ell)\} \subseteq \mathbb{N}^1$ is semi-diced, we obtain that also the set $\{(\ell)\} \times T =$

$$\{(\ell, x_2, \ldots, x_n) : (x_2, \ldots, x_n) \in T\} = Bd(S, v')_{1,\ell}$$

is semi-diced.
  Case 2: $i \geqslant 2$. Then, $Bd(S, v')_{i,\ell} =$

$$\{ x = (x_1, x_2, \ldots, x_n) \in S_{i,\ell} :$$
$$(x_1 + k', x_2, \ldots, x_n) \notin S_{i,\ell} \}.$$

By assumption we know that $S_{i,\ell}$ is semi-diced. From the definition of semi-diced sets it is straightforward to see that also the set

$$S'_{i,\ell} := \{(x_1, x_2, \ldots, x_n) : (x_1 + k', x_2, \ldots, x_n) \in S_{i,\ell}\}$$

is semi-diced. From Lemma C.3 we know that the class of semi-diced subsets is closed under intersection and complement. Therefore, also the set

$$Bd(S, v')_{i,\ell} = S_{i,\ell} \cap \overline{S'_{i,\ell}}$$

is semi-diced. This completes the proof of Lemma C.11. $\qquad\square$

Lemma C.12. *Let $S, V \subseteq \mathbb{N}^n$ such that S has property $(*)$ with respect to V, V is finite with $|V| \geqslant 2$, and every $v \in V$ has exactly one non-zero coordinate. Then for every $v \in V$ the following is true: $Bd(S, v)$ and $Bd(S, -v)$ have property $(*)$ with respect to $V \setminus \{v\}$.*

Proof. For simplicity in notation we assume w.l.o.g. that $v = k \cdot e_1$ for some $k \in \mathbb{N}_{\geqslant 1}$. Let $v' \in \{v, -v\}$. We have to show that $Bd(S, v')$ has property $(*)$ with respect to $V \setminus \{v\}$. To this end, let $k' \geqslant 0$ be an arbitrary size of a neighborhood.
  By assumption, S has property $(*)$ with respect to V. In particular, for $k' + k$ there exists an $\ell \geqslant 0$ such that for every $x \in \mathbb{N}^n$ with $||x|| \geqslant \ell$ there is a $\tilde{v} \in V$ such that $\tilde{v}$ is a period of S in $N_{k'+k}(x)$.
  If $\tilde{v} = v$, then v is a period of S in $N_{k'+k}(x)$. Note that for each $y \in N_{k'}(x)$, $N_{k'+k}(x)$ contains each of the vectors y and $y + v'$. Therefore, $Bd(S, v') \cap N_{k'}(x) = \emptyset$, and thus any element in $V \setminus \{v\}$ is a period of $Bd(S, v')$ in $N_{k'}(x)$.
  If $\tilde{v} \neq v$, then $\tilde{v}$ is a period of $Bd(S, v')$ in $N_{k'}(x)$: To see this, let $y \in N_{k'}(x)$ such that $y + \tilde{v} \in N_{k'}(x)$ and note that $y \in Bd(S, v') \iff y \in S$ and $y + v' \notin S \iff y + \tilde{v} \in S$ and $y + v' + \tilde{v} \notin S \iff y + \tilde{v} \in Bd(S, v')$.
  In summary, we have shown that $Bd(S, v')$ has property $(*)$ with respect to $V \setminus \{v\}$. This completes the proof of Lemma C.12. $\qquad\square$

We are now ready for the proof of Theorem 4.7.

Proof of Theorem 4.7:
Due to Lemma C.8, it suffices to show the following:

  A set $S \subseteq \mathbb{N}^n$ is semi-diced iff the following is true:

  (a) every section of S is semi-diced, and

  (b) there exists a finite set $V \subseteq \mathbb{N}^n \setminus \{\mathbf{0}\}$ such that every element in V has exactly one non-zero coordinate and S has property $(*)$ w.r.t. V.

The "only if" direction follows easily from Lemma C.5 along with the definition of semi-diced sets. The proof of

the "if" direction proceeds by induction on $|V|$. The *induction base* for $|V| = 1$ is established by Lemma C.9.

For the *induction step*, assume that $|V| \geqslant 2$, and let v be an arbitrary element in V. By assumption we know that $V \subseteq \mathbb{N}^n$ is finite, that every element in V has exactly one non-zero coordinate, that all sections of S are semi-diced, and that S has property $(*)$ with respect to V.

Lemma C.11 tells us that all sections of $Bd(S, v)$ and all sections of $Bd(S, -v)$ are semi-diced. From Lemma C.12 we obtain that $Bd(S, v)$ and $Bd(S, -v)$ have property $(*)$ with respect to $V \setminus \{v\}$. The induction hypothesis thus tells us that $Bd(S, v)$ and $Bd(S, -v)$ are semi-diced.

Our aim is to show that S is semi-diced. For simplicity in notation we assume w.l.o.g. that

$$v \;=\; k \cdot e_1 \;=\; (k, 0, \dots, 0)$$

for some $k \in \mathbb{N}_{\geqslant 1}$. Furthermore, we write

$$B^+ := Bd(S, v) \quad \text{and} \quad B^- := Bd(S, -v).$$

We already know that B^+ and B^- are semi-diced. Using the construction from the proof of Lemma C.5, we obtain that there exists a period $q \in \mathbb{N}_{\geqslant 1}$ such that the following is true: q is a multiple of k, and for each $\Diamond \in \{+, -\}$ there exists a finite set $J^\Diamond$ such that for each $j \in J^\Diamond$ there is a vector $v_j^\Diamond \in \mathbb{N}^n$ and a set $I_j^\Diamond \subseteq \{1, \dots, n\}$ such that

$$B^\Diamond \;=\; \bigcup_{j \in J^\Diamond} \Big(v_j^\Diamond + \sum_{i \in I_j^\Diamond} \mathbb{N} q e_i \Big).$$

Let d be the smallest integer that is bigger than any component in any vector in

$$\{ v_j^\Diamond \;:\; \Diamond \in \{+, -\}, \; j \in J^\Diamond \}.$$

From the particular choice of d and q we immediately obtain the following:

Claim C.13. *For every $\Diamond \in \{+, -\}$ and for every $x \in \mathbb{N}^n$ such that each component of x is $\geqslant d$, the following is true: If $x \in B^\Diamond$, then $x + \sum_{i=1}^{n} \mathbb{N} q e_i \subseteq B^\Diamond$. If $x \notin B^\Diamond$, then $x + \sum_{i=1}^{n} \mathbb{N} q e_i \subseteq \mathbb{N}^n \setminus B^\Diamond$.*

Let $c := d + q$. Furthermore, let

$$\mathbb{N}^n_{\geqslant c} := \{ x \in \mathbb{N}^n \;:\; \text{each component of } x \text{ is } \geqslant c \}$$

and $S_{\geqslant c} := S \cap \mathbb{N}^n_{\geqslant c}$. Note that

$$S \;=\; S_{\geqslant c} \cup \bigcup_{i=1}^{n} \bigcup_{\ell=0}^{c-1} S_{i,\ell}.$$

Since, by assumption, all sections $S_{i,\ell}$ of S are semi-diced, in order to show that S is semi-diced it suffices to show that

$S_{\geqslant c}$ is semi-diced. The remainder of the proof is devoted to showing that $S_{\geqslant c}$ is semi-diced.

Recall that $v = k \cdot e_1$. For $x = (x_1, \dots, x_n) \in \mathbb{N}^n$ let

$$\langle x \rangle^v_{\geqslant d} \;:=\; \{ x + j \cdot v \;:\; j \in \mathbb{Z} \text{ such that } x_1 + j \cdot k \geqslant d \}$$

Let

$$S^{(1)} \quad := \quad \{ x \in S_{\geqslant c} \;:\; \langle x \rangle^v_{\geqslant d} \subseteq S \} \qquad \text{and}$$

$$S^{(2)} \quad := \quad S_{\geqslant c} \setminus S^{(1)}.$$

Note that $S_{\geqslant c} = S^{(1)} \cup S^{(2)}$. In order to show that $S_{\geqslant c}$ is semi-diced, it therefore suffices to show that $S^{(1)}$ is semi-diced and to find a semi-diced set S' such that $S^{(2)} \subseteq S' \subseteq S_{\geqslant c}$. To this end let us consider the set

$$T \;:=\; \{ x \in \mathbb{N}^n_{\geqslant c} \;:\; \langle x \rangle^v_{\geqslant d} \subseteq S \text{ or } \langle x \rangle^v_{\geqslant d} \subseteq \mathbb{N}^n \setminus S \}$$

and the cube

$$C \;:=\; \{ \, x = (x_1, \dots, x_n) \in \mathbb{N}^n \;:\; $$
$$c \leqslant x_i < c + q, \text{ for each } i \in \{1, \dots, n\} \, \}.$$

Note that $T \supseteq S^{(1)}$.

Claim C.14. *For all $x \in C \setminus T$, the following is true: If $x \in S$, then $x + \sum_{i=1}^{n} \mathbb{N} q e_i \subseteq S$. If $x \notin S$, then $x + \sum_{i=1}^{n} \mathbb{N} q e_i \subseteq \mathbb{N}^n \setminus S$.*

Proof. Let $x \in C \setminus T$. Since $x \notin T$, there exist $x', x'' \in \langle x \rangle^v_{\geqslant d}$ with $x' \in S$ and $x'' \notin S$. By choice of C and q we obtain that there must exist integers j^+ and j^- that have the following three properties:

- $0 \leqslant j^+ < \frac{q}{k}$ and $0 \geqslant j^- > \frac{q}{k}$,

- $x \in S \iff x + j^+ \cdot v \in S$
  $\qquad \iff x + (j^+ + 1) \cdot v \notin S,$

- $x \in S \iff x + j^- \cdot v \in S$
  $\qquad \iff x + (j^- - 1) \cdot v \notin S.$

Let j^+ and j^- be chosen such that these conditions are met and $|j^+|$ and $|j^-|$ is as small as possible. Clearly, for any j with $j^- \leqslant j \leqslant j^+$ we have that $x + j \cdot v \in S \iff x \in S$.

Now let y be an arbitrary element in $x + \sum_{i=1}^{n} \mathbb{N} q e_i$. It suffices to show that $x \in S \iff y \in S$.

The proof of "$\implies$" proceeds as follows. If $x \in S$, then the following is true: $x + j^+ \cdot v \in B^+$, $x + j^- \cdot v \in B^-$, and $x + jv \notin B^+ \cup B^-$ for any j with $j^- < j < j^+$. By Claim C.13 we obtain that $y + j^+ \cdot v \in B^+$, $y + j^- \cdot v \in B^-$, and $y + jv \notin B^+ \cup B^-$ for any j with $j^- < j < j^+$. Thus, Definition C.10 tells us that $y + j \cdot v \in S$ for all j with $j^- \leqslant j \leqslant j^+$. In particular, $y \in S$.

25

The proof of "⟸" proceeds as follows. If $x \notin S$, then the following is true: $x + (j^+ + 1) \cdot v \in B^-$, $x + (j^- - 1) \cdot v \in B^+$, and $x + j \cdot v \notin B^+ \cup B^-$ for any j with $j^- \leqslant j \leqslant j^+$. By Claim C.13 we obtain that $y + (j^+ + 1) \cdot v \in B^-$, $y + (j^- - 1) \cdot v \in B^+$, and $y + j \cdot v \notin B^+ \cup B^-$ for any j with $j^- \leqslant j \leqslant j^+$. Thus, Definition C.10 tells us that $y + j \cdot v \notin S$ for any j with $j^- \leqslant j \leqslant j^+$. In particular, $y \notin S$. This completes the proof of Claim C.14. $\square$

Claim C.15. $T = \bigcup_{x \in C \cap T} x + \sum_{i=1}^{n} \mathbb{N} q e_i$. *In particular, T is semi-diced.*

Proof. Let $y = (y_1, \ldots, y_n) \in \mathbb{N}^n_{\geqslant c}$. Consider the particular element $x = (x_1, \ldots, x_n) \in C$ where $x_i \equiv y_i$ $[q]$, for every $i \in \{1, \ldots, n\}$. Obviously,

$$y \in x + \sum_{i=1}^{n} \mathbb{N} q e_i.$$

It suffices to show that $x \in T \iff y \in T$.

The proof of "⟹" proceeds as follows: If $x \in T$, then (by definition of T), we have $\langle x \rangle^v_{\geqslant d} \subseteq S$ or $\langle x \rangle^v_{\geqslant d} \subseteq \mathbb{N}^n \setminus S$. In particular, this implies that $\langle x \rangle^v_{\geqslant d} \subseteq \mathbb{N}^n \setminus B^\Diamond$, for any $\Diamond \in \{+, -\}$. By Claim C.13 we obtain that $\langle y \rangle^v_{\geqslant d} \subseteq \mathbb{N}^n \setminus B^\Diamond$, for any $\Diamond \in \{+, -\}$. Thus, either $\langle y \rangle^v_{\geqslant d} \subseteq S$ or $\langle y \rangle^v_{\geqslant d} \subseteq \mathbb{N}^n \setminus S$. I.e., $y \in T$.

The proof of "⟸" follows analogously. $\square$

Claim C.16. $S^{(1)}$ *is semi-diced.*

Proof. It is straighforward to verify that $S^{(1)}$ has property (∗) with respect to the set $\{v\}$. Lemma C.9 thus tells us that in order to show that $S^{(1)}$ is semi-diced, it suffices to show that every section $S^{(1)}_{1,\ell}$ (for any $\ell \in \mathbb{N}$) is semi-diced.

Note that $S^{(1)}_{1,\ell} = S_{1,\ell} \cap T$. By assumption we know that every section $S_{1,\ell}$ of S is semi-diced, and by Claim C.15 we know that T is semi-diced. Since the class of semi-diced sets is closed under intersection (cf., Lemma C.3), we therefore obtain that $S^{(1)}_{1,\ell}$ is semi-diced. $\square$

Claim C.17. *The set*

$$S' := \bigcup_{x \in S \cap (C \setminus T)} x + \sum_{i=1}^{n} \mathbb{N} q e_i$$

is semi-diced, and $S^{(2)} \subseteq S' \subseteq S$.

Proof. S' is semi-diced by definition. Due to Claim C.14, $S' \subseteq S$. It remains to show that $S^{(2)} \subseteq S'$. To this end, consider an arbitrary $y \in S^{(2)} = S_{\geqslant c} \setminus S^{(1)}$. In particular, $y \notin T$.

Consider the particular element $x = (x_1, \ldots, x_n) \in C$ where $x_i \equiv y_i$ $[q]$, for every $i \in \{1, \ldots, n\}$. Obviously, $y \in x + \sum_{i=1}^{n} \mathbb{N} q e_i$.

Since $y \notin T$, Claim C.15 tells us that $x \notin T$. Thus, Claim C.14 (together with the fact that $y \in S$) tells us that $x \in S$. By definition of S', we then have that $x + \sum_{i=1}^{n} \mathbb{N} q e_i \subseteq S'$, and hence $y \in S'$. $\square$

In summary, we know that $S_{\geqslant c} = S^{(1)} \cup S'$, and $S^{(1)}$ and S' are semi-diced. Thus, $S_{\geqslant c}$ is semi-diced, and the proof of Theorem 4.7 is complete. $\square$

C.5   Proof of Proposition 4.2

We actually prove a result slightly stronger than Proposition 4.2. For formulating this result in the next lemma, we need the following notation.

Definition C.18. A language L is called +-inv-FO($<$)-definable in a language M iff if there exists a sentence φ of FO($<, \prec, +$) such that for any string $u \in M$ and any two $\sigma[+]$-expansions u_1 and u_2 of u we have $u_1 \models \varphi$ iff $u_2 \models \varphi$.

Note that Proposition 4.2 is an immediate consequence of the following lemma.

Lemma C.19. *Let $n \in \mathbb{N}_{\geqslant 1}$, let $w_1, \ldots, w_n \in \Sigma^*$ such that $|w_1| = \cdots = |w_n| \geqslant 1$, let $\alpha_1, \ldots, \alpha_{n+1} \in \Sigma^*$, and let $M := \alpha_1 w_1^* \alpha_2 w_2^* \cdots \alpha_n w_n^* \alpha_{n+1}$. Every language $L \subseteq M$ that is +-inv-FO($<$)-definable in M is regular.*

The proof of Lemma C.19 follows the line sketched in Section 4.2. We recall here the main steps and provide the missing details.

Recall that for $\overline{\alpha} := (\alpha_1, \ldots, \alpha_{n+1})$ and $\overline{w} := (w_1, \ldots, w_n)$ we use the following notation:

- $M^{\overline{w}}_{\overline{\alpha}} = \alpha_1 w_1^* \alpha_2 w_2^* \cdots \alpha_n w_n^* \alpha_{n+1}$.

- For $L \subseteq M^{\overline{w}}_{\overline{\alpha}}$, the set $\mathscr{S}^{\overline{w}}_{\overline{\alpha}}(L) \subseteq \mathbb{N}^n$ consists of all vectors $x = (x_1, \ldots, x_n) \in \mathbb{N}^n$ such that the string $\alpha_1 w_1^{x_1} \alpha_2 w_2^{x_2} \cdots \alpha_n w_n^{x_n} \alpha_{n+1}$ associated to x belongs to L.

Proof of Lemma C.19:
Let $M := M^{\overline{w}}_{\overline{\alpha}}$. Fix a language $L \subseteq M$ that is +-inv-FO($<$)-definable in M. Let $S \subseteq \mathbb{N}^n$ be $\mathscr{S}^{\overline{w}}_{\overline{\alpha}}(L)$.

Our goal is to show that L is regular. By Theorem 4.5, it suffices to show that S is semi-diced. By Theorem 4.7 it suffices to show that S has the properties (a) and (b) stated in Theorem 4.7. I.e., it suffices to show that

(a) every section of S is semi-diced, and

(b) there is a finite set $V \subseteq \mathbb{N}^n \setminus \{\mathbf{0}\}$ such that every element in V has exactly one non-zero coordinate and $\forall K \in \mathbb{N}, \exists \ell \in \mathbb{N}$ such that the following is true: $\forall x \in \mathbb{N}^n$ with $||x|| \geqslant \ell, \exists v \in V$ such that $N_K(x)$ and $N_K(x + v)$ are identical with respect to S.

26

The most difficult part is to show property (b). Property (a) then follows essentially by induction on n. We split the proof of (b) and (a) into two claims.

Claim C.20. *S has property (b).*

Proof. By Lemma 4.4, S is semi-linear. Let $U \subseteq \mathbb{N}^n \setminus \{\mathbf{0}\}$ be the finite set given by Lemma 4.6 for S.

Let V be defined as in (7), i.e.,

$$V := \{\,\|u\| \cdot e_i \;:\; u \in U \text{ and } i \in supp(u)\,\},$$

where e_i is the unit vector of $\mathbb{N}^n$ which has a 1 in its i-th component and 0s in all other components. Clearly, V is a finite subset of $\mathbb{N}^n$, and every element in V has exactly one non-zero coordinate.

All we need to show is that V has the following property:

  $\forall K \in \mathbb{N}$, $\exists \ell \in \mathbb{N}$ such that the following is true: $\forall x \in \mathbb{N}^n$ with $\|x\| \geqslant \ell$, $\exists v \in V$ such that $N_K(x)$ and $N_K(x + v)$ are identical with respect to S.

Let $K_0 := \max\{\|v\| : v \in V\}$. Now let $K \in \mathbb{N}$ be an arbitrary number. Let $\hat{K} := K + K_0$. Choose $\ell := \hat{\ell}$ to be the number obtained from Lemma 4.6 for the number $\hat{K}$.

Now let $x \in \mathbb{N}^n$ be an arbitrary vector with $\|x\| \geqslant \ell$. By Lemma 4.6 we obtain an $u \in U$ such that for all $j \in \mathbb{N}$ and for $x^{(j)} := x + ju$, $N_{\hat{K}}(x)$ and $N_{\hat{K}}(x^{(j)})$ are identical with respect to S.

If $|supp(u)| = 1$, then $u \in V$, and by choosing $v := u$ we obtain that $x + v = x^{(1)}$, and thus $N_K(x)$ and $N_K(x+v)$ are identical with respect to S.

For the remainder of this proof we consider the case that $|supp(u)| \geqslant 2$. For simplicity in notation we assume w.l.o.g. that $supp(u) = \{1, \ldots, t\}$ for some $t \in \mathbb{N}$ with $2 \leqslant t \leqslant n$.

We choose $v := \|u\| \cdot e_1$. By (7) we have $v \in V$. Our goal is to prove that $N_K(x)$ and $N_K(x + v)$ are identical with respect to S. To this end, let us fix an arbitrary $z \in \mathbb{Z}^n$ with $\|z\| \leqslant K$. We need to show that $x + z \in S \iff x + v + z \in S$. We will see that this is a consequence of:

Claim 4.8. *There exists a $J \in \mathbb{N}$ such that*
$x + Ju + u + z \in S \iff x + Ju + v + z \in S$.

Before proving this claim, let us point out how to use the claim in order to show that $x + z \in S \iff x + v + z \in S$.

Let J be chosen according to Claim 4.8. We know that $N_{\hat{K}}(x)$, $N_{\hat{K}}(x^{(J)})$, and $N_{\hat{K}}(x^{(J+1)})$ are identical with respect to S. Furthermore, $\|z\| \leqslant K$ and $\|v\| \leqslant K_0$, thus $\|z+v\| \leqslant K + K_0 = \hat{K}$. Therefore,

$$
\begin{array}{rcll}
x + z \in S & \iff & x^{(J+1)} + z \in S & (1) \\
& \iff & x^{(J)} + u + z \in S & (2) \\
& \iff & x^{(J)} + v + z \in S & (3) \\
& \iff & x + v + z \in S & (4).
\end{array}
$$

Here, equivalence (1) holds since $N_{\hat{K}}(x)$ and $N_{\hat{K}}(x^{(J+1)})$ are identical w.r.t. S. Equivalence (2) holds since $x^{(J+1)} = x^{(J)} + u$. Equivalence (3) holds due to Claim 4.8. Equivalence (4) holds since $N_{\hat{K}}(x^{(J)})$ and $N_{\hat{K}}(x)$ are identical w.r.t. S.

In summary, we obtain that $N_K(x)$ and $N_K(x + v)$ are identical with respect to S. Therefore, in order to finish the proof of Claim C.20, it suffices to prove Claim 4.8.

Proof of Claim 4.8:
By the assumption of Lemma C.19 we are given strings $\alpha_1, \ldots, \alpha_{n+1} \in \Sigma^*$ and strings $w_1, \ldots, w_n \in \Sigma^*$ such that $|w_1| = \cdots = |w_n| \geqslant 1$.

Let $\ell := \max\{|w_1|, |\alpha_1|, \ldots, |\alpha_{n+1}|\}$. We consider the alphabet

$$\Delta := \Sigma \times \{w, \alpha\} \times \{1, \ldots, n{+}1\} \times \{1, \ldots, \ell\}. \quad (22)$$

With each of the strings w_i (resp., α_i) we associate a string $\tilde{w}_i$ (resp., $\tilde{\alpha}_i$) in Δ^* as follows:

- If $w_i = w_{i,1}w_{i,2}\cdots w_{i,\ell_i}$ with $w_{i,j} \in \Sigma$, then $\tilde{w}_i := \tilde{w}_{i,1}\tilde{w}_{i,2}\cdots\tilde{w}_{i,\ell_i}$ with $\tilde{w}_{i,j} := (w_{i,j}, w, i, j)$.

- If $\alpha_i = \alpha_{i,1}\alpha_{i,2}\cdots\alpha_{i,s_i}$ with $\alpha_{i,j} \in \Sigma$, then $\tilde{\alpha}_i := \tilde{\alpha}_{i,1}\tilde{\alpha}_{i,2}\cdots\tilde{\alpha}_{i,s_i}$ with $\tilde{\alpha}_{i,j} := (\alpha_{i,j}, \alpha, i, j)$.

For each $x = (x_1, \ldots, x_n) \in \mathbb{N}^n$ let

$$\tilde{\mathcal{W}}(x) := \tilde{w}_1^{x_1}\,\tilde{w}_2^{x_2}\,\cdots\,\tilde{w}_n^{x_n} \in \Delta^*.$$

Aiming at applying Lemma A.2 we choose Δ as in equation (22), and $\Gamma := \{\mathbf{0}_i, \mathbf{1}_i, \mathbf{2}_i : i \in \{2, \ldots, t\}\}$. We let $k' := 1 + qr(\varphi)$, where φ is the +-inv-FO($<$)-sentence that, by assumption, defines language L in M. Furthermore, we let

$$
\begin{array}{rcl}
H & := & \tilde{\alpha}_1\,\tilde{\alpha}_2\,\cdots\,\tilde{\alpha}_{n+1}\,\tilde{\mathcal{W}}(x + z), \\
G & := & \varepsilon, \\
U & := & \tilde{\mathcal{W}}(u).
\end{array}
$$

Note that $|U| \geqslant 1$. For each $\gamma \in \Gamma$, the string U_γ is defined as follows: For every $i \in \{2, \ldots, t\}$,

$$
\begin{array}{rcl}
U_{\mathbf{0}_i} & := & U, \\
U_{\mathbf{1}_i} & := & \tilde{\mathcal{W}}(u + e_1 - e_i), \\
U_{\mathbf{2}_i} & := & \tilde{\mathcal{W}}(u - e_1 + e_i).
\end{array}
$$

Note that $|U_\gamma| = |U|$ for every $\gamma \in \Gamma$ (since $|\tilde{w}_1| = \cdots = |\tilde{w}_n|$).

We choose $m := |U|$. Let h, g, k'' and $r := r(m, h, g, k'')$ and $P \subseteq \mathbb{N}$ and i_j (for $j \in \mathbb{N}$) be chosen as in Lemma A.2.

We let $d \in \mathbb{N}$ be large enough such that $(\underline{v}, <) \approx_r (\underline{w}, <)$ for the strings

$$v := \mathbf{0}_2^d\,\mathbf{0}_2^{u_2}\,\mathbf{1}_2^d\,\mathbf{2}_2^d \quad \mathbf{0}_3^d\,\mathbf{0}_3^{u_3}\,\mathbf{1}_3^d\,\mathbf{2}_3^d \quad \cdots \quad \mathbf{0}_t^d\,\mathbf{0}_t^{u_t}\,\mathbf{1}_t^d\,\mathbf{2}_t^d$$

and

$$w \quad := \quad \mathbf{0}_2^d \, \mathbf{1}_2^{u_2} \, \mathbf{1}_2^d \, \mathbf{2}_2^d \quad \mathbf{0}_3^d \, \mathbf{1}_3^{u_3} \, \mathbf{1}_3^d \, \mathbf{2}_3^d \quad \cdots \quad \mathbf{0}_t^d \, \mathbf{1}_t^{u_t} \, \mathbf{1}_t^d \, \mathbf{2}_t^d$$

(an easy EF-game argument shows that any $d > 2^r$ will do, see e.g. [11]). Let $D = d_v = d_w$ be the length of each of these strings, i.e., $D = 3d \cdot (t-1) + \sum_{i=2}^{t} u_i$.

Let V and W be chosen as in Lemma A.2, i.e., (recall that $G = \varepsilon$)

$$V \;=\; H \, U^{i_0} \left(Q_j \, U^{i_j} \right)_{j=1,\dots,D} \qquad \text{and}$$

$$W \;=\; H \, U^{i_0} \left(R_j \, U^{i_j} \right)_{j=1,\dots,D}$$

where, for each $j \geqslant 1$ and each $\gamma \in \Gamma$ the following is true: If γ is the j-th letter in v (respectively, w), then $Q_j = U_\gamma$ (respectively, $R_j = U_\gamma$).

Aiming at applying part (b) of Lemma A.2, we let, for each $a \in \Sigma$, $\psi_a(x)$ be a (quantifier-free) formula that states that there exists $(j_1, j_2, j_3) \in \{w, \alpha\} \times \{1, \dots, n+1\} \times \{1, \dots, \ell\}$ such that the letter at position x is $(a, j_1, j_2, j_3) \in \Delta$: The formula $\psi_a(x)$ is simply the disjunction of the formulas $P_{(a, j_1, j_2, j_3)}(x)$ for all $(j_1, j_2, j_3) \in \{w, \alpha\} \times \{1, \dots, n+1\} \times \{1, \dots, \ell\}$.

Then, the strings V' and W' defined in Lemma A.2 are identical to the strings V and W, where each letter in Δ is restricted to its first component.

We let $\psi_{Ord}(x, y)$ be a formula which, when interpreted in $(\underline{V}, <, +, P)$ and $(\underline{W}, <, +, P)$, defines a linear order on the domain of $\underline{V}$ and $\underline{W}$ such that when reading the letters of $\underline{V}$ and $\underline{W}$ according to this particular linear order, one obtains strings that belong to

$$\tilde{\alpha}_1 \, \tilde{w}_1^* \, \tilde{\alpha}_2 \, \tilde{w}_2^* \, \cdots \, \tilde{\alpha}_n \, \tilde{w}_n^* \, \tilde{\alpha}_{n+1}.$$

By our particular choice of the alphabet Δ, it is straightforward to see that this can be formalized by a *quantifier-free* formula $\psi_{Ord}(x, y)$.

Furthermore, we let $\psi_{Succ}(x, y)$ be a first-order formula (of quantifier rank 1) that defines the successor relation that corresponds to the linear order defined by $\psi_{Ord}(x, y)$.

Let V'' and W'' be chosen as in Lemma A.2 (b). I.e., V'' and W'' are the strings obtained from reading the letters of V' and W' according to the successor relation defined by ψ_{Succ}. It is straightforward to see that V'' and W'' both belong to $M = M_{\overline{\alpha}}^{\overline{w}} = \alpha_1 \, w_1^* \, \alpha_2 \, w_2^* \, \cdots \, \alpha_n \, w_n^* \, \alpha_{n+1}$.

From Lemma A.2 (b) (ii) we obtain that V'' and W'' satisfy the same $+$-inv-FO$(<)$-sentences of quantifier rank at most $k := k' - 1$. Since, by assumption, φ is a $+$-inv-FO$(<)$-sentence of quantifier rank k that defines the language L in M, we obtain that $V'' \in L \iff W'' \in L$. Thus, if y_V and y_W are elements in $\mathbb{N}^n$ such that

$$V'' \;=\; \alpha_1 \, w_1^{y_{V,1}} \, \alpha_2 \, w_2^{y_{V,2}} \, \cdots \, \alpha_n \, w_n^{y_{V,n}} \, \alpha_{n+1},$$
$$W'' \;=\; \alpha_1 \, w_1^{y_{W,1}} \, \alpha_2 \, w_2^{y_{W,2}} \, \cdots \, \alpha_n \, w_n^{y_{W,n}} \, \alpha_{n+1},$$

then we have

$$y_V \in S \iff y_W \in S. \tag{23}$$

Now let $\tilde{y}_V$ and $\tilde{y}_W$ be the vectors in $\mathbb{N}^n$ which, for each $i \in \{1, \dots, n\}$, indicate in their i-th component the number of copies of $\tilde{w}_i$ that occur in V and W, respectively. Note that

$$V'' \;=\; \alpha_1 \, w_1^{\tilde{y}_{V,1}} \, \alpha_2 \, w_2^{\tilde{y}_{V,2}} \, \cdots \, \alpha_n \, w_n^{\tilde{y}_{V,n}} \, \alpha_{n+1},$$
$$W'' \;=\; \alpha_1 \, w_1^{\tilde{y}_{W,1}} \, \alpha_2 \, w_2^{\tilde{y}_{W,2}} \, \cdots \, \alpha_n \, w_n^{\tilde{y}_{W,n}} \, \alpha_{n+1}.$$

Therefore, from equation (23) we obtain that $\tilde{y}_V \in S \iff \tilde{y}_W \in S$. To finish the proof of Claim 4.8, it thus suffices to show that there exists a $J \in \mathbb{N}$ such that

$$\tilde{y}_V \;=\; x^{(J)} + u + z \quad \text{and} \quad \tilde{y}_V \;=\; x^{(J)} + v + z.$$

To this end, note that

$$\tilde{y}_V =$$
$$\underbrace{x \,+\, z \,+\, \left(\sum_{j=0}^{D} i_j \right) \cdot u \,+\, 3d(t-1) \cdot u \,+\, \left(\sum_{i=2}^{t} u_i \right) \cdot u}_{=: \; y'}$$

and

$$\tilde{y}_W \;=\; y' \,+\, \sum_{i=2}^{t} \left(u_i \cdot (u + e_1 - e_i) \right).$$

Note that $v = \|u\| \cdot e_1 = u + \sum_{i=2}^{t} \left(u_i \cdot (e_1 - e_i) \right)$. Therefore,

$$\sum_{i=2}^{t} \left(u_i \cdot (u + e_1 - e_i) \right) \;=\; \left(\left(\sum_{i=2}^{t} u_i \right) - 1 \right) \cdot u \,+\, v.$$

For

$$J \;:=\; \left(\sum_{j=0}^{D} i_j \right) \,+\, 3d(t-1) \,+\, \left(\left(\sum_{i=2}^{t} u_i \right) - 1 \right)$$

we thus obtain that $\tilde{y}_V = x + z + J \cdot u + u$ and $\tilde{y}_W = x + z + J \cdot u + v$. I.e.,

$$\tilde{y}_V \;=\; x^{(J)} + u + z \qquad \text{and} \qquad \tilde{y}_W \;=\; x^{(J)} + v + z.$$

Thus, the proof of Claim 4.8 — and hence also the proof of Claim C.20 — is complete. $\qquad\square$

We are now ready to finish the proof of Lemma C.19, i.e., to show the following:

Claim C.21. *S has property (a) and (b), i.e., S is semi-diced.*

Proof. We proceed by induction on n. From Lemma 4.4, we know that the set $S = \mathscr{S}_{\overline{\alpha}}^{\overline{w}}(L) \subseteq \mathbb{N}^n$ is semi-linear.

For the *induction base* $n = 1$ note that every semi-linear set is a finite union of sets of the form $m + \mathbb{N}p$, where $m, p \in \mathbb{N}$. Note that since $n = 1$, each of these sets is *diced*, and thus S is semi-diced. Theorem 4.7 therefore tells us that S has property (a) and (b).

For the *induction step* let $n \geqslant 2$. Let $w_1, \dots, w_n$, $\alpha_1, \dots, \alpha_{n+1}$, and M be chosen as in the assumption of Lemma C.19, and let $\overline{\alpha} := (\alpha_1, \dots, \alpha_{n+1})$ and $\overline{w} := (w_1, \dots, w_n)$. Let $L \subseteq M$ be a language that is +-inv-FO($<$)-definable in M. Our aim is to show that the set $S = \mathscr{S}_{\overline{\alpha}}^{\overline{w}}(L) \subseteq \mathbb{N}^n$ has property (a) and (b) (i.e., by Theorem 4.7, S is semi-diced).

From Claim C.20 we already know that S has property (b). For showing that S also has property (a), we choose $i \in \{1, \dots, n\}$ and $\ell \in \mathbb{N}$, and show that the set $S_{i,\ell}$ is semi-diced. For simplicity in notation, we only consider the case where $i = n$ (the proof for $i < n$ is analogous). Let $\overline{w}' := (w_1, \dots, w_{n-1})$ and $\overline{\alpha}' := (\alpha_1, \dots, \alpha_{n-1}, \alpha'_n)$ where $\alpha'_n := \alpha_n w_n^\ell \alpha_{n+1}$.

Clearly, for every $x = (x_1, \dots, x_{n-1}) \in \mathbb{N}^{n-1}$ we have $\mathcal{W}_{\overline{\alpha}'}^{\overline{w}'}(x) = \mathcal{W}_{\overline{\alpha}}^{\overline{w}}(x, \ell)$, where

$$\mathcal{W}_{\overline{\alpha}'}^{\overline{w}'}(x) \ := \ \alpha_1 w_1^{x_1} \alpha_2 w_2^{x_2} \cdots \alpha_{n-1} w_{n-1}^{x_{n-1}} \alpha'_n,$$

$$\mathcal{W}_{\overline{\alpha}}^{\overline{w}}(x, \ell) \ := \ \alpha_1 w_1^{x_1} \alpha_2 w_2^{x_2} \cdots \alpha_{n-1} w_{n-1}^{n-1} \alpha_n w_n^\ell \alpha_{n+1}.$$

Let us consider the set $S_{n,\ell} = \{y = (y_1, \dots, y_{n-1}, \ell) : y \in S\}$ and the language $L' :=$

$$\{\mathcal{W}_{\overline{\alpha}}^{\overline{w}}(y) : y \in S_{n,\ell}\} = \{\mathcal{W}_{\overline{\alpha}'}^{\overline{w}'}(x) : (x, \ell) \in S_{n,\ell}\}. \quad (24)$$

Clearly, $L' \subseteq M' := M_{\overline{\alpha}'}^{\overline{w}'}$, and L' is +-inv-FO($<$)-definable in M' (by the same +-inv-FO($<$)-sentence that, by assumption, defines L in M).

From the induction hypothesis we obtain that the set $S' := \mathscr{S}_{\overline{\alpha}'}^{\overline{w}'}(L') \subseteq \mathbb{N}^{n-1}$ has property (a) and (b), i.e., S' is semi-diced. Note that

$$
\begin{aligned}
S' \ &= \ \{x \in \mathbb{N}^{n-1} : \mathcal{W}_{\overline{\alpha}'}^{\overline{w}'}(x) \in L'\} \\
&\overset{\text{eq. (24)}}{=} \ \{x \in \mathbb{N}^{n-1} : (x, \ell) \in S\}.
\end{aligned}
$$

Thus, $S_{n,\ell} = S' \times \{(\ell)\}$. We already know that S' is semi-diced. Consequently, also $S_{n,\ell}$ is semi-diced. This completes the proof Claim C.21 and thus also the proof of Lemma C.19. $\qquad\square$

C.6   Proof of Theorem 4.1

In fact, we even get a result slightly stronger than Theorem 4.1. The following formulation of this result uses the notation introduced in Definition C.18.

Theorem C.22. *Let $n \in \mathbb{N}_{\geqslant 1}$, and let $w_1, \dots, w_n \in \Sigma^*$. Every language $L \subseteq w_1^* w_2^* \cdots w_n^*$ that is +-inv-FO($<$)-definable in $w_1^* w_2^* \cdots w_n^*$ is regular.*

Note that Theorem 4.1 is an immediate consequence of Theorem C.22. The proof of Theorem C.22 can be obtained as an easy consequence of Lemma C.19 from Section C.5:

Proof of Theorem C.22:
Let $L \subseteq w_1^* w_2^* \cdots w_n^*$ be +-inv-FO($<$)-definable in $w_1^* w_2^* \cdots w_n^*$ by a +-inv-FO($<$)-sentence φ. W.l.o.g. we can assume that each w_i is nonempty, i.e, $|w_i| \geqslant 1$.

Let $\ell := \text{lcm}\{|w_1|, \dots, |w_n|\}$. For each $i \in \{1, \dots, n\}$ let $\ell_i := \frac{\ell}{|w_i|}$, let $\hat{w}_i := w_i^{\ell_i}$, and for each $j \in [\ell_i] = \{0, \dots, \ell_i - 1\}$ let $\alpha_{i,j} := w_i^j$.
Clearly, for $J := [\ell_1] \times \cdots \times [\ell_n]$ we have $w_1^* w_2^* \cdots w_n^* =$

$$\bigcup_{(j_1, \dots, j_n) \in J} \underbrace{\alpha_{1,j_1} \hat{w}_1^* \alpha_{2,j_2} \hat{w}_2^* \cdots \alpha_{n,j_n} \hat{w}_n^*}_{=:\ M_j \ \text{for}\ j := (j_1, \dots, j_n)}. \quad (25)$$

For each $j \in J$ let $L_j := L \cap M_j$. Note that for every word $w \in M_j$ we have $w \in L_j \iff w \models \varphi$. Thus, L_j is +-inv-FO($<$)-definable in M_j. Furthermore, $|\hat{w}_1| = \cdots = |\hat{w}_n| \geqslant 1$. Thus, we obtain from Lemma C.19 (with α_{n+1} being the empty word) that L_j is regular. Since $L = \bigcup_{j \in J} L_j$ and since the class of regular languages is closed under union, we obtain that L is regular. Thus, the proof of Theorem C.22 is complete. $\qquad\square$

D   Proofs omitted in Section 5

D.1   Proof of Theorem 5.1

Proof of Theorem 5.1 (continued):
Let L be a commutative language that is definable in +-inv-FO($<$). Let Σ be the alphabet of L, let $n := |\Sigma|$, and let $\sigma_1, \dots \sigma_n$ be an enumeration of all letters in Σ.

Let $L' := L \cap \sigma_1^* \sigma_2^* \cdots \sigma_n^*$. Clearly, L' is +-inv-FO($<$)-definable (since, by assumption, L is definable in +-inv-FO($<$) and, obviously, $\sigma_1^* \sigma_2^* \cdots \sigma_n^*$ is definable in FO($<$)). By Theorem 4.1 we obtain that L' is regular. Since L is commutative, we know that $L = c(L')$. From Theorem 5.2 we obtain that L is regular. $\qquad\square$

D.2   Proof of Theorem 5.4

We will make use of the following pumping lemma for languages definable in +-inv-FO($<$).

Lemma D.1. *Let L be a language definable in +-inv-FO($<$). Let u, v, w_1, w_2, w_3 be five words of Σ^*. Let*

$$\delta_u \ = \ |v| \cdot (|u| + |v|) \quad \text{and} \quad \delta_v \ = \ |u| \cdot (|u| + |v|).$$

Then we have: $\forall l \in \mathbb{N}, \exists \nu \in \mathbb{N}$ *such that*

$$w_1 u^{\nu + l\delta_u} w_2 v^{\nu - l\delta_v} w_3 \in L \text{ iff } w_1 u^\nu w_2 v^\nu w_3 \in L. \quad (26)$$

Proof. We assume w.l.o.g. that $|u| \geqslant 1$ and $|v| \geqslant 1$ (note that the lemma's statement is trivial if $|u| = 0$ or $|v| = 0$).

Let $\alpha = |u|$, $\beta = |v|$, and $z = \alpha\beta$. Let k be the quantifier rank of the $+\text{-inv-FO}(<)$ formula defining L, and choose $k' := k + 1$.

Aiming at applying Lemma A.2, we let $\Gamma := \{\mathbf{0}, \mathbf{1}\}$ and

$$\begin{aligned}
\Delta := \Sigma \; &\cup \; \{(a, u) \mid a \in \Sigma\} \\
&\cup \; \{(a, v) \mid a \in \Sigma\} \\
&\cup \; \{(a, w_1) \mid a \in \Sigma\} \\
&\cup \; \{(a, w_2) \mid a \in \Sigma\} \\
&\cup \; \{(a, w_3) \mid a \in \Sigma\}.
\end{aligned}$$

With each of the strings u, v, w_1, w_2, w_3 we associate a string $\tilde{u}, \tilde{v}, \tilde{w}_1, \tilde{w}_2, \tilde{w}_3$ of Δ^* by using the letters marking the string it belongs to.

We further let

$$\begin{aligned}
H &:= \tilde{w}_1 \tilde{w}_2 \tilde{w}_3, \quad G := \varepsilon, \\
U &:= (\tilde{u}\tilde{v})^z, \quad U_{\mathbf{0}} := \tilde{u}^{\delta_u}, \quad U_{\mathbf{1}} = \tilde{v}^{\delta_v}.
\end{aligned} \quad (27)$$

We choose $m := |U|$ and note that $m \geqslant 1$ and $|U| = |U_{\mathbf{0}}| = |U_{\mathbf{1}}|$. We let h, g, k'' and $r := r(m, h, g, k'')$ and $P = \{p_1, p_2, ...\} \subseteq \mathbb{N}$ and i_j (for $j \in \mathbb{N}$) be chosen according to Lemma A.2.

Now fix an arbitrary $l \in \mathbb{N}$, and let $d \in \mathbb{N}$ be a large enough number such that for all $d_0, d_1 > d$,

$$\mathbf{0}^{d_0} \mathbf{1}^{d_1} \approx_r \mathbf{0}^{d_0 + l} \mathbf{1}^{d_1 - l}. \quad (28)$$

An easy EF-game argument shows that any $d > 2^{r+l}$ will do, see e.g. [11].

We choose

$$d_0 := d \cdot \alpha, \quad d_1 := d \cdot \beta, \quad d' := d_0 + d_1. \quad (29)$$

Notice that $\delta_u \cdot d_0 = \delta_v \cdot d_1 = d \cdot \alpha \cdot \beta \cdot (\alpha + \beta)$, and that both d_0 and d_1 are greater than d (since $\alpha \neq 0$ and $\beta \neq 0$).

Recall that according to Lemma A.2, $i_0, i_1, ..., i_{d'}$ are the following numbers: $i_0 = \frac{p_1 - h}{m}$, and $i_j = \frac{p_{j+1} - p_j}{m} - 1$ for all $1 \leqslant j \leqslant d'$. We set

$$\nu = z \cdot (i_0 + i_1 + \cdots + i_{d'}) + \delta_u \cdot d_0. \quad (30)$$

Now let V and W be chosen according to Lemma A.2 i.e.,

$$V = \tilde{w}_1 \tilde{w}_2 \tilde{w}_3 (\tilde{u}\tilde{v})^{z i_0} \left(\tilde{u}^{\delta_u} (\tilde{u}\tilde{v})^{z i_j} \right)_{j=1}^{d_0} \left(\tilde{v}^{\delta_v} (\tilde{u}\tilde{v})^{z i_j} \right)_{j=d_0+1}^{d'}$$

$$W = \tilde{w}_1 \tilde{w}_2 \tilde{w}_3 (\tilde{u}\tilde{v})^{z i_0} \left(\tilde{u}^{\delta_u} (\tilde{u}\tilde{v})^{z i_j} \right)_{j=1}^{d_0+l} \left(\tilde{v}^{\delta_v} (\tilde{u}\tilde{v})^{z i_j} \right)_{j=d_0+l+1}^{d'}$$

Note that the number of occurences of $\tilde{u}$ in V is ν, and the number of occurrences of $\tilde{v}$ in V is ν, while the number of occurrences of $\tilde{u}$ and $\tilde{v}$ in W is, respectively, $\nu + \delta_u l$ and $\nu - \delta_v l$.

Aiming at applying part (b) of Lemma A.2 we let, for each $a \in \Sigma$, $\psi_a(x)$ be the quantifier-free formula satisfied by all positions x whose label is either a or (a, u) or (a, v) or (a, w_i) for $i \in \{1, 2, 3\}$.

We let $\psi_{Ord}(x, y)$ be a formula which, when interpreted in $(\underline{V}, <, +, P)$ and $(\underline{W}, <, +, P)$, defines a linear order on the domain of $\underline{V}$ and $\underline{W}$ such that, when reading the letters of $\underline{V}$ and $\underline{W}$ according to this particular linear order, one obtains strings that belong to

$$\tilde{w}_1 \tilde{u}^* \tilde{w}_2 \tilde{v}^* \tilde{w}_3.$$

By our particular choice of the alphabet Δ, it is straightforward to see that this can be formalized by a *quantifier-free* formula $\psi_{Ord}(x, y)$.

Furthermore, we let $\psi_{Succ}(x, y)$ be a first-order formula (of quantifier-rank 1) that defines the successor relation that corresponds to the linear order defined by $\psi_{Ord}(x, y)$.

Then, the strings V'' and W'' defined in Lemma A.2 are:

$$\begin{aligned}
V'' &= w_1 u^\nu w_2 v^\nu w_3, \\
W'' &= w_1 u^{\nu + \delta_u l} w_2 v^{\nu - \delta_v l} w_3.
\end{aligned} \quad (31)$$

Now, by Lemma A.2 we know that V'' and W'' satisfy the same $+\text{-inv-FO}(<)$-sentences of quantifier-rank at most $k' - 1$. Thus, by our choice of k' we obtain that $V'' \in L$ iff $W'' \in L$. This completes the proof of Lemma D.1. $\square$

The following notation will be useful for our proof of Theorem 5.4.

Let A be a deterministic pushdown-automaton (DPDA, for short) whose set of states is Q, and whose stack alphabet is Γ. A *configuration* of A is a pair (q, γ) where $q \in Q$ and $\gamma \in \Gamma^*$ is the content of the stack. The *type* of a configuration (q, γ) is the pair (q, S) where S is the top symbol of the stack γ. Because A is deterministic, for each $w \in \Sigma^*$ there is a unique type reached by A after reading w, denoted by $\tau_A(w)$. Given a string $w \in \Sigma^*$ we say that w *is a loop for the type* (q, S) if, when starting in the configuration (q, S) (where the stack contains only the symbol S), A ends in the same configuration (q, S) after reading w.

Definition D.2. Let A be a DPDA, and let L be the language accepted by A. A tuple (u, v, w_1, w_2) is a *pumping pair* for L if

1. w_2 is a loop for $\tau_A(w_1 u)$,

2. $u w_2 v$ is a loop for $\tau_A(w_1)$,

3. $\tau_A(w_1) = \tau_A(w_1 u)$, and

4. $\tau_A(w_1 u w_2) = \tau_A(w_1 u w_2 v)$.

Note that if (u, v, w_1, w_2) is a pumping pair for L, then also $(u, v, w_1 u, w_2)$ is a pumping pair for L.

We will make use of the following pumping lemma for deterministic context-free languages:

Lemma D.3. *Let L be a deterministic context-free language recognized by a DPDA A. Let (u, v, w_1, w_2) be a pumping pair for L. Then, for all $w_3 \in \Sigma^*$ and all $k, l \in \mathbb{N}$ we have:*

$$w_1 u^k u^l w_2 v^l w_3 \in L \quad \textit{iff} \quad w_1 u^k w_2 w_3 \in L. \quad (32)$$

Proof. By induction on l, using Definition D.2, one easily sees that $u^l w_2 v^l$ is a loop for $\tau_A(w_1)$. By induction on k, using Definition D.2 we also obtain that $\tau_A(w_1) = \tau_A(w_1 u^k)$. The lemma then follows easily. $\square$

We are now ready to prove a pumping lemma for deterministic context-free languages definable in $+$-inv-FO$(<)$.

Lemma D.4. *Let L be a deterministic context-free language definable in $+$-inv-FO$(<)$. Let (u, v, w_1, w_2) be a pumping pair for L, and let $\delta = (|u| + |v|)^2$.*
Then, for all $w_3 \in \Sigma^*$ and for all $l \in \mathbb{N}$ we have:

$$w_1 u w_2 v w_3 \in L \quad \textit{iff} \quad w_1 u u^{l\delta} w_2 v w_3 \in L. \quad (33)$$

Proof. Fix w_3 and l.

Since L is definable in $+$-inv-FO$(<)$, we can apply Lemma D.1 with l, and we get a number $\nu \in \mathbb{N}$ such that

$$w_1 u^{\nu + l\delta_u} w_2 v^{\nu - l\delta_v} w_3 \in L \text{ iff } w_1 u^{\nu} w_2 v^{\nu} w_3 \in L. \quad (34)$$

Notice that $\delta = \delta_u + \delta_v$. Since L is deterministic context-free, applying Lemma D.3 to the left hand side of (34) yields:

$$w_1 u^{\nu + l\delta_u} w_2 v^{\nu - l\delta_v} w_3 \in L \text{ iff } w_1 u^{\nu + l\delta} w_2 v^{\nu} w_3 \in L$$
$$\text{iff } w_1 u u^{l\delta} w_2 v w_3 \in L. \quad (35)$$

Applying Lemma D.3 to the right hand side of (34) yields:

$$w_1 u^{\nu} w_2 v^{\nu} w_3 \in L \quad \text{iff} \quad w_1 u w_2 v w_3 \in L. \quad (36)$$

Now, combining (34), (35), and (36) concludes the proof of Lemma D.4. $\square$

For the proof of Theorem 5.4 we use the following notation:

If L is a language, then two words w and w' are said to be *L-equivalent* if $\forall \gamma, w\gamma \in L$ iff $w'\gamma \in L$. We are now ready to conclude the proof of Theorem 5.4.

The next notation is taken from [20]. A word u is said to be *null-transparent for L* if it satisfies the following:

$$\forall x, y \in \Sigma^*, \quad \forall m, n \in \mathbb{N},$$
$$\text{if} \quad |y| < min\{m, n\} \quad (37)$$
$$\text{then} \quad xu^m y \in L \text{ iff } xu^n y \in L.$$

We will use the next lemma, proved by Valiant in [20] (there, the lemma was used in order to show the decidability of the problem whether a given deterministic context-free language is regular).

Lemma D.5 (Implicit in [20]). *If L is a deterministic context-free language that is not regular, then there exist strings w_1, u, w_2, v such that:*

1. *(u, v, w_1, w_2) is a pumping pair for L,*

2. *$w_1 u^2 w_2 v$ is not L-equivalent to $w_1 u w_2 v$, and*

3. *u is null-transparent for L.*

We are finally ready for the proof of Theorem 5.4.

Proof of Theorem 5.4:
Let L be a deterministic context-free language definable in $+$-inv-FO$(<)$.

Aiming at a contradiction, let us assume that L is not regular. Then, let w_1, u, w_2, v be the strings given by Lemma D.5.

Since (u, v, w_1, w_2) is a pumping pair for L, by Lemma D.4 we have for all w_3 and all $l \in \mathbb{N}$:

$$w_1 u w_2 v w_3 \in L \quad \text{iff} \quad w_1 u u^{l\delta} w_2 v w_3 \in L. \quad (38)$$

For a given w_3, fix l such that $l\delta > |w_2 v w_3|$. Since u is null-transparent for L, using (37) we obtain:

$$w_1 u u^{l\delta} w_2 v w_3 \in L \quad \text{iff} \quad w_1 u u^{l\delta + 1} w_2 v w_3 \in L. \quad (39)$$

Applying, again, Lemma D.4, gives:

$$w_1 u u^{l\delta + 1} w_2 v w_3 \in L \quad \text{iff} \quad w_1 u^2 w_2 v w_3 \in L. \quad (40)$$

By combining equations (38), (39), and (40) we obtain that for all strings w_3:

$$w_1 u w_2 v w_3 \in L \quad \text{iff} \quad w_1 u^2 w_2 v w_3 \in L. \quad (41)$$

Therefore, $w_1 u w_2 v$ is L-equivalent to $w_1 u^2 w_2 v$, contradiction Item 2 of Lemma D.5. Thus, L is regular, and the proof of Theorem 5.4 is complete. $\square$

E Proof omitted in Section 6

Proof of Proposition 6.1:
Let us first show that $\bar{L}$ is context-free: A non-deterministic pushdown automaton (PDA) recognizing $\bar{L}$ first guesses why the input string w is not in L, and then verifies that its guess is correct.

In the following, by *block* we mean a factor of w between two consecutive $\#$ symbols.

A string w is not in L because either (i) two consecutive blocks do not have the same length or (ii) they correspond to non-consecutive numbers. In the case of (i) the PDA guesses the corresponding blocks and compares their respective length using the stack. In the case of (ii), the PDA guesses the corresponding block while maintaining in its state whether the corresponding number is coded with least or most significant bit first. It is then not too hard to use the stack for performing an increment.

It is not difficult to see that $\bar{L}$ is in $\mathrm{FO}(<,+)$: The position of the leftmost $\#$ provides the length n of the blocks and can then be used with addition to test whether all blocks have the same length. Testing that two consecutive blocks represent consecutive numbers is done bit by bit using the fact that the ith bit of a number represented by some block is at distance exactly $n-i+2$ from the ith bit of the number represented by the following block.

That $\bar{L}$ is expressible in $(+,*)$-inv-$\mathrm{FO}(<)$ follows along the same lines as Lemma 5.4 in [1]. □