First-Order Quantifiers
and the Syntactic Monoid
of Height Fragments of Picture Languages

Oliver Matz
Institut für Informatik, Universität Kiel, Germany
matz@ti.informatik.uni-kiel.de

May 10, 2014

Abstract

We investigate the expressive power of first-order quantifications in the context of monadic second-order logic over pictures. We show that $k + 1$ set quantifier alternations allow to define a picture language that cannot be defined using $k$ set quantifier alternations preceded by arbitrarily many first-order quantifier alternations.

The approach uses, for a given picture language $L$ and an integer $m \geq 1$, the height- $m$ fragment of $L$, which is defined as the word language obtained by considering each picture $p$ of height $m$ in $L$ as a word, where the letters of that word are the columns of $p$.

A key idea is to measure the complexity of a regular word language by the group complexity of its syntactic monoid. Given a picture language $L$, such a word language measure may be applied to each of its height fragments, so that the complexity of the picture language is a function that maps each $m$ to the complexity of the height- $m$ fragment of $L$. The asymptotic growth rate of that function may be bounded based on the structure of a monadic second-order formula that defines $L$.

The core argument for that lower bound proof is based on Straubing’s algebraic characterization of the effect of first-order quantifiers on the syntactic monoid of word languages by means of Rhodes’ and Tilson’s block product.

Keywords: Picture languages, monadic second-order logic, quantifier alternation, syntactic monoid, group complexity
## Contents

1 Introduction

2 Basic Notions
   2.1 Pictures
   2.2 Pictures over Attributes Alphabets
   2.3 Monadic Second-Order Formulas
   2.4 Pictures as Models
   2.5 Quantifier Alternation Classes
   2.6 Syntactic Congruence and Syntactic Monoid
   2.7 Pseudovarieties and Group Complexity
   2.8 Height Fragment Technique and Results

3 Expressibility Result
   3.1 Iterated Matrix Multiplication
   3.2 Picture Languages Defined by a Regular Top-Row Language
   3.3 Relativization and Closure Under Concatenation
   3.4 Assembling the Picture Language

4 Non-Expressibility Result
   4.1 Some More Notation
   4.2 Transition Monoid of an NFA
   4.3 A Semantic Equivalent to First-Order Quantification
   4.4 The Block Product
   4.5 Using the Group Complexity

5 Conclusion
   5.1 Remarks on the Height Fragment Technique
   5.2 Open Questions

6 Acknowledgments
1 Introduction

In monadic second-order logic (MSO) over finite structures, formulas use first-order quantifications (ranging over elements of the universe) as well as set quantifications (ranging over sets thereof). \cite{MT97, Sch97, Mat99, MST02, Mat02} investigate the effect of the alternation of existential and universal set quantification and show that the depth of this alternation cannot be bounded without loss of expressive power. The proofs are done for a specific class of structures, namely pictures.

The upper bound proofs in those papers show that very little use of set quantification is needed. The quantifiers that actually alternate are all first-order. Set quantification is needed for two purposes: The outermost set quantification establishes a specific, uniquely determined coloring, and the innermost set quantification is needed only to replace the horizontal ordering, which itself is not present in the logic. Thus all the formulas constructed in the upper bound proofs can be written in prenex normal form with a quantifier prefix of the form

\[ \exists^* \{\exists, \forall\}^* \exists^* \{\exists, \forall\}^* \]

where \( \exists^* \) denotes a block of existential set quantifiers, and \( \forall \) and \( \exists \) denote universal (or existential, respectively) first-order quantifiers. The question whether every MSO formula can be written in this form remains open, see Problem 5.2.

This motivates the interest in the power of first-order quantification in the context of MSO. It has been studied in \cite{AFS00, JM01} in the context of graphs. In \cite{AFS00}, the authors suggest the closed MSO alternation hierarchy, which is coarser and more robust than the ordinary MSO alternation hierarchy of \cite{MT97} because it allows to intersperse first-order quantifiers “for free” between set quantifiers. The authors ask whether this hierarchy is strict—a question that is still open.

In \cite{JM01}, the authors develop a technique to infer new separation results dealing with the first-order closure. Specifically, they show the following:

**Theorem 1.1** (\cite{JM01}) Let \( V, W \subseteq \{\exists, \forall, \exists, \forall\}^* \). Let \( S \) be a graph property definable with a quantifier prefix of a form in \( V \) but not with one of a form in \( W \). Then there is another property definable with a quantifier prefix of a form in \( \exists \forall V \) but not with one of a form in \( \{\exists, \forall\}^* W \).

The authors of \cite{JM01} apply that theorem to show the following corollary (previously shown directly in \cite{AFS00}).

**Corollary 1.2** There exists a graph property definable by a prenex normal form of type \( \exists^* \{\exists, \forall\}^* \exists^* \{\exists, \forall\}^* \) but not with one of type \( \{\exists, \forall\}^* \exists^* \{\exists, \forall\}^* \).

In this paper, we focus on pictures (as opposed to arbitrary finite graphs). We show that the above corollary is true for pictures, too, thereby giving yet another proof for it (see Corollary 2.12 for the case \( k = 1 \)). Besides we consider (as in \cite{Mat99}) formulas that have a quantifier prefix of the form

\[ \{\exists, \forall\}^* \{\exists, \forall\}^* \{\exists, \forall\}^* \]
Hasse diagram of the monadic second-order alternation hierarchy and the first-order closures hierarchy over pictures ($k \geq 1$). All inclusions are trivial. The dashed line indicates that the two classes are incomparable.

The non-inclusions (1) (from [Sch97]) and (2) (from [Mat99]) are re-proved here (for non-trivial alphabets), see Corollary 2.11. That corollary shows also the non-inclusion (3), which is new. Non-inclusion (4) has been shown for directed graphs in [AFS00, JM01] and is here re-proved (for pictures over a non-trivial alphabet) as Corollary 2.12.

where the set quantifier block in the middle contains only $k$ alternations, and compare their expressive power to formulas with a quantifier prefix of the form

$$\{ \exists, \forall \}^* \{ \exists, \forall \}^* ,$$

where the set quantifier block contains only $k + 1$ alternations. The main result of this paper (Corollary 2.11) is that there is a formula of the latter kind that is not equivalent to any of the former kind. Once again, the formula constructed in the proof does not actually use $k + 1$ set quantifier alternations; it has only two set quantifier blocks—the $k + 1$ alternations stem from the first-order quantifier blocks in between these.

The lower bound proof is based on the block product introduced in [RT89], which, by [Str94], allows to characterize the effect of first-order quantifiers on the syntactic monoid of word languages, see Lemma 4.3. The application to pictures (as opposed to words) follows the same approach as [MT97, MST02, Mat99, Mat02]: The common essential idea to show that a picture language $L$ cannot be defined by a formula class $\mathcal{F}$ is the following: We consider the family $(L[m])_{m \geq 1}$, where $L[m]$ contains the pictures of height $m$. That so-called height-$m$ fragment $L[m]$ may be regarded as a word language over the $m$-fold Cartesian product of the alphabet. Then we show that, for a sufficiently large $m$, the complexity of that height-$m$ fragment (wrt. some suitable complexity measure of word languages) is too high, so that $L$ cannot be defined by a $\mathcal{F}$-formula.
Typical complexity measures used in [MT97, MST02, Mat99] are firstly the number of states needed for a recognizing non-deterministic finite automaton and, secondly, the length of the shortest word of a (unary) word language. This paper is the first one in which the used complexity measure is the group complexity of the syntactic monoid.

2 Basic Notions

2.1 Pictures

Let $\Gamma$ be a finite alphabet. A non-empty picture of size $(m,n)$ over $\Gamma$ (where $m,n \geq 1$) is an $m \times n$-matrix over $\Gamma$. If $p$ is a non-empty picture of size $(m,n)$, we denote the length $n$ (i.e., the number of columns) by $|p|$, the height $m$ (i.e., the number of rows) by $\overline{p}$, and the domain $\{1,..,m\} \times \{1,..,n\}$ by $\text{dom}(p)$. The component at position $(i,j) \in \text{dom}(p)$ is denoted $p_{\langle i,j \rangle}$.

The set of non-empty pictures over $\Gamma$ is denoted $\Gamma^+$. A set of non-empty pictures is called a picture language.

If $p$ and $q$ are non-empty pictures with $\overline{p} = \overline{q}$, then the non-empty picture that results by appending $q$ to the right of $p$ is denoted $pq$. This partial operation is called the column concatenation.

Picture languages must not contain the empty picture. Nevertheless, when we assemble picture languages by column concatenation, it is often convenient to have a neutral element. That is why we consider a special, distinct empty picture which we denote $\varepsilon$ and for which height, width, domain, and size are not defined. For every (empty or non-empty) picture $p$, we define $p\varepsilon = \varepsilon p = p$.

Column concatenation is lifted to sets of pictures as usual. For every set $L$ of pictures, the iterated column concatenation is defined by $L^0 = \{\varepsilon\}$ and $L^{i+1} = L^i L$ and every $i \geq 0$.

The set of all non-empty pictures of height $m$ over alphabet $\Gamma$ is denoted $\Gamma^{m,+}$, and $\Gamma^{m,*}$ abbreviates $\Gamma^{m,+} \cup \{\varepsilon\}$.

Let $p$ be a non-empty picture over $\Gamma$ and $m = \overline{p}$. We frequently consider each column of $p$ as a letter of the new alphabet $\Gamma^m$. This way, we identify every non-empty picture $p$ with a word of length $|p|$ over alphabet $\Gamma^m$. For a set of pictures $L$ and $m \geq 1$ we define the height-$m$ fragment (denoted $L[m]$) as the set of these words over alphabet $\Gamma^m$.

2.2 Pictures over Attributes Alphabets

While in general the nature of an alphabet $\Gamma$ is indifferent, it will be technically convenient to have certain notions for the case that $\Gamma$ is of the form $\{0,1\}^I$ for a finite set of so-called attributes. That means that each letter $a \in \Gamma$ is a mapping $I \rightarrow \{0,1\}$.

If $a \in \{0,1\}^I$ and $J \subseteq I$, then $\text{restr}_J(a) = a \upharpoonright J$ is the restriction of $a$ to a $J$-indexed family. The mapping $\text{restr}_J$ is an alphabet projection from $\{0,1\}^I \rightarrow \{0,1\}^J$, which is lifted to pictures and picture languages the usual way.

The alphabet projection $\text{ex}_J : \{0,1\}^I \rightarrow \{0,1\}^{I \setminus J}$ is defined by $\text{ex}_J = \text{restr}_{I \setminus J}$. 
Furthermore, we define for every $\mu \in I$ the mapping 

$$\text{pr}_\mu : \{0, 1\}^I \rightarrow \{0, 1\}, \ a \mapsto a(\mu).$$

It is an alphabet projection, too, and it is lifted to pictures and picture languages the usual way.

Typically, each attribute corresponds to a free variable in a formula (see next section). With regard to sentences (i.e., formulas without free variables), it is therefore consequent to allow also the empty attribute set, so by convention, $\{0, 1\}^\emptyset$ is some fixed singleton alphabet, and $\text{restr}_\emptyset$ denotes the alphabet projection to that singleton alphabet.

### 2.3 Monadic Second-Order Formulas

We describe our conventions for formulas. We will be concerned with a fixed signature with two binary successor predicates $S_1$, $S_2$ and with the specific class of structures associated to non-empty pictures.

Let $J, K$ be two disjoint sets of attributes, which we use as indices of variables. We use first-order variables $x_\nu$ with $\nu \in K$ and set variables $X_\mu$ with $\mu \in J$. Atomic formulas are of the form $X_\mu x_\nu$ (for $\mu \in J$ and $\nu \in K$), or $S_1 x_\mu x_\nu$, or $S_2 x_\mu x_\nu$, or $x_\mu = x_\nu$ (for $\mu, \nu \in K$). Formulas are assembled in the usual way using the boolean connectives as well as first-order quantification ($\exists x_\nu \phi$ or $\forall x_\nu \phi$) and set quantification ($\exists X_\mu \phi$ or $\forall X_\mu \phi$).

### 2.4 Pictures as Models

Let $J, K$ be two disjoint attribute sets. Set $I = J \cup K$. Let $\text{Unique}_{I,K}$ be the set of those non-empty pictures $p$ over alphabet $\{0, 1\}^I$ such that for all $\nu \in K$ there is exactly one position $(i, j) \in \text{dom}(p)$ with $p(i, j)(\nu) = 1$.

Let $p \in \text{Unique}_{I,K}$, say with size $(m, n)$. Let $\phi$ be a formula with free set variables in $\{X_\mu \mid \mu \in J\}$ and free first-order variables in $\{x_\nu \mid \nu \in K\}$. To $p$, we associate the grid structure with universe $\{1, .., m\} \times \{1, .., n\}$ and an assignment $(X^p_\mu)_{\mu \in J}, (x^p_\nu)_{\nu \in K}$ to the free variables in the following way:

- $X^p_\mu = \{(i, j) \in \text{dom}(p) \mid p(i, j)(\mu) = 1\}$,
- $x^p_\nu$ is the unique $(i, j) \in \text{dom}(p)$ with $p(i, j)(\nu) = 1$.

We write

$$p \models \phi$$

iff this assignment makes $\phi$ true in the structure with universe $\{1, .., m\} \times \{1, .., n\}$, where the predicates $S_1$ and $S_2$ are interpreted as the vertical and horizontal successor relation, respectively, i.e., $S_2 x_1 x_2$ asserts that $x_2$ is the horizontal successor of $x_1$. That means, $p \models S_2 x_1 x_2$ iff there exist $(i, j), (i, j + 1) \in \text{dom}(p)$ such that $x^p_1 = \langle i, j \rangle$ and $x^p_2 = \langle i, j + 1 \rangle$.

Another notation convention will be convenient. Let $\phi$ and $p$ be as above. Suppose that $\nu_1, \ldots, \nu_n \in K$ are attributes of first-order variables. If $a_1, \ldots, a_n \in \text{dom}(p)$, then, by abuse of notation, we write

$$p, \frac{a_1}{x_{\nu_1}} \ldots \frac{a_n}{x_{\nu_n}} \models \phi$$
iff $\varphi$ is made true in the structure from above, where the assignment for the attributes $\{\nu_1, \ldots, \nu_n\}$ is provided by setting $x_{\nu_j}^p = a_j$ for every $j \in \{1, \ldots, n\}$.

Let $\text{Mod}_{I,K}(\varphi) = \{p \in \text{Unique}_{I,K} \mid p \models \varphi\}$. We write $\text{Mod}(\varphi)$ rather than $\text{Mod}_{I,K}(\varphi)$ if $I, K$ are clear from the context; typically $I$ (or $K$) is the set of those attributes that may appear as indices of free variables (or free first-order variables, respectively) of $\varphi$, or any superset thereof. Indeed we have the following remark, which shows that adding an element to the attribute set does not make that much of a difference:

**Remark 2.1** Let $I$ be an attribute set, $K \subseteq I$, and $\mu \in I \setminus K$. If $\varphi$ is a formula with indexes of free variables in $I \setminus \{\mu\}$, then

$$\text{Mod}_{I,K}(\varphi) = \text{ex}^{-1}_{\{\mu\}}(\text{Mod}_{I \setminus \{\mu\}, K}(\varphi)).$$

The concept of existential set quantification is captured by the alphabet projection on picture languages in the following sense, motivating the notation $\text{ex}_{\{\mu\}}$ for the alphabet projection.

**Remark 2.2** Let $I$ be an attribute set, $K \subseteq I$, and $\mu \in I \setminus K$. If $\varphi$ is a formula with indexes of free variables in $I$, then

$$\text{Mod}_{I \setminus \{\mu\}, K}(\exists_\mu \varphi) = \text{ex}_{\{\mu\}}(\text{Mod}_{I,K}(\varphi)).$$

Two formulas $\varphi, \psi$ are **equivalent** iff $\text{Mod}(\varphi) = \text{Mod}(\psi)$. Note that our notion of equivalence implicitly refers to the class of pictures and is thus coarser than logical equivalence. A formula $\varphi$ defines a picture language $L$ over alphabet $\{0, 1\}^I$ if $\varphi$ has no free first-order variables, the free set variables of $\varphi$ are among $(X_\mu)_{\mu \in J}$, and $\text{Mod}_{I,\emptyset}(\varphi) = L$.

We use the following convention for variable substitution. Let $\varphi$ be a formula. Let $X_1, \ldots, X_m$ (and $x_1, \ldots, x_n$) be set variables (or first-order variables, respectively). Note that we do not require that all free variables of $\varphi$ are among these, but typically, this is the case.

We may write $\varphi(X_1, \ldots, X_m, x_1, \ldots, x_n)$ instead of $\varphi$ in order to pick these variables for a later substitution. If we later write $\varphi(X'_1, \ldots, X'_m, x'_1, \ldots, x'_n)$, for other variables $X'_1, \ldots, X'_m, x'_1, \ldots, x'_n$, then this denotes the formula that results from $\varphi$ by replacing each indicated variable from the first variable tuple by the respective variable from the latter. For example, if we introduce the formula $\varphi$ as $\varphi(x_1, x_2)$, then by $\varphi(x_2, x_1)$ we mean the formula that results from $\varphi$ by exchanging the occurrences of $x_1$ and $x_2$.

**Example 2.3** The first-order formula $\text{top}(x) := \neg \exists y(S_1 yx)$ asserts for a position $x$ that it is in the top row. Similarly, $\text{left}(x) := \neg \exists y(S_2 yx)$ and $\text{right}(x) := \neg \exists y(S_2 xy)$ assert that $x$ is in the leftmost (or rightmost, respectively) column.

**Example 2.4** Let

$$\psi = \forall x_1 \forall x_2 ((S_2 x_1 x_2 \land X_{\text{cl}d} x_1) \rightarrow X_{\text{cl}d} x_2).$$
Then $X_{\text{cld}}$ is the only free set variable of $\psi$. The formula $\psi$ asserts that $X_{\text{cld}}$ is closed under horizontal successors. In other words, for a non-empty picture $p$ over alphabet $\{0, 1\}^{\text{cld}}$ we have that $p \models \psi$ iff every row of the picture $\text{pr}_{\text{cld}}(p)$ is in $0^*1^*$. Let

$$\varphi = \forall X_{\text{cld}}(X_{\text{cld}}x \land \psi \rightarrow X_{\text{cld}}x').$$

Then $\psi$ asserts that position $x'$ is right to $x$. More precisely: for a non-empty picture $p$ and two positions $\langle i, j \rangle, \langle i', j' \rangle \in \text{dom}(p)$ we have $p, \langle i, j \rangle \models \varphi$ iff $i = i'$ and $j \leq j'$.

Consider the formula $\text{right}(x)$ from the preceding example. Let

$$\varphi' = \exists X_{\text{cld}} \left(X_{\text{cld}}x \land \forall x_1 (\text{right}(x_1) \land x_1 \neq x' \rightarrow \neg X_{\text{cld}}x_1) \land \forall x_1 x_2 (S_2 x_1 x_2 \land x_1 \neq x' \land X_{\text{cld}}x_1 \rightarrow X_{\text{cld}}x_2) \right).$$

Then $\varphi'$ is equivalent to $\varphi$. \hfill \Box

The formula $\varphi$ from Example 2.4 will be abbreviated as $x \leq_2 x'$ and will be needed later. The above is a standard example of how to use set quantification to express the horizontal ordering, which we do not have in the signature.

### 2.5 Quantifier Alternation Classes

In this section we define the formula classes that are characterized by the structure of their prenex normal form wrt. blocks of existential or universal set quantifiers or first-order quantifiers.

A first-order formula is a formula that does not make use of set quantification. The class of first-order formulas is denoted $\text{FO}$. For a class $\mathcal{F}$ of formulas, let $\text{co-}\mathcal{F}$ be the class of formulas $\neg \varphi$ with $\varphi \in \mathcal{F}$.

Let $\mathcal{F}$ be a class of formulas. The

1. **boolean closure** of $\mathcal{F}$, denoted $\text{B}(\mathcal{F})$,
2. **existential first-order closure** of $\mathcal{F}$, denoted $\Sigma^0_1(\mathcal{F})$,
3. **existential monadic closure** of $\mathcal{F}$, denoted $\Sigma^\text{mon}_1(\mathcal{F})$,
4. **first-order closure** of $\mathcal{F}$, denoted $\text{FO}(\mathcal{F})$,

respectively, are defined as the smallest superclass of $\mathcal{F}$ that is closed under

1. boolean combinations,
2. existential first-order quantifications and positive boolean combinations,
3. existential set quantifications and positive boolean combinations,
4. first-order quantifications and boolean combinations,

respectively.
We define \( \Sigma_0^{\text{mon}}(\mathcal{F}) = \mathcal{F} \) and \( \Sigma_{k+1}^{\text{mon}}(\mathcal{F}) = \Sigma_1^{\text{mon}}(B(\Sigma_k^{\text{mon}}(\mathcal{F}))) \) for every \( k \geq 0 \). Let \( \Pi_k^{\text{mon}}(\mathcal{F}) = \text{co}-\Sigma_k^{\text{mon}}(\text{co-}\mathcal{F}) \) for every \( k \). We write \( \Sigma_k^{\text{mon}} \) and \( \Pi_k^{\text{mon}} \) instead of \( \Sigma_k^{\text{mon}}(\text{FO}) \) and \( \Pi_k^{\text{mon}}(\text{FO}) \), respectively.

The formula classes \( \Sigma_k^{\text{mon}}(\mathcal{F}) \) and \( \Pi_k^{\text{mon}}(\mathcal{F}) \) are defined analogously but for first-order rather than set quantification.

In the sequence, every formula that is equivalent to a formula in \( \mathcal{F} \) will be called an \( \mathcal{F} \)-formula, too.

\( \Delta_k^{\text{mon}} \) is the class of formulas that are both a \( \Sigma_k^{\text{mon}} \)-formula and a \( \Pi_k^{\text{mon}} \)-formula.

Some of the quantifier alternation classes can be characterized very succinctly by giving their formulas in prenex normal form, as we did in the introduction. For example, \( \Sigma \Delta F \)

The situation is more difficult for classes that involve the boolean closure, the first-order closure, or \( \Delta \)-formula, too.

For example, \( \{\forall, \exists\} \exists^+ \{\exists, \forall\}^* \)

Remark 2.7 Let \( \mathcal{F} \supseteq \text{FO} \) be a class of formulas closed under conjunction and \( \varphi \in \mathcal{F} \). Then there is a formula \( \varphi' \in \mathcal{F} \) such that \( \exists x_{\mu} \varphi \) is equivalent to \( \exists X_{\mu} \varphi' \).

By the standard calculation rules of predicate logic and by the above remark, we have the following.

Remark 2.6 Let \( \mathcal{F} \supseteq \text{FO} \) is a class of formulas closed under conjunction and \( \varphi \in \mathcal{F} \). Then there is a formula \( \varphi' \in \mathcal{F} \) such that \( \exists x_{\mu} \varphi \) is equivalent to \( \exists X_{\mu} \varphi' \).

Every boolean combination of \( \Delta_1^{\text{mon}} \)-formulas is a \( \Delta_1^{\text{mon}} \)-formula. By a standard argument, first-order quantification may be expressed by a suitable set quantification in the following sense:

Example 2.5 In Example 2.4 we have seen that \( x \leq_2 x' \) is a \( \Sigma_1^{\text{mon}} \)-formula and also a \( \Pi_1^{\text{mon}} \)-formula. Hence it is a \( \Delta_1^{\text{mon}} \)-formula. \( \square \)

2.6 Syntactic Congruence and Syntactic Monoid

Let \( L \) be a word language over alphabet \( \Gamma \). The syntactic congruence \( \equiv_L \) is defined as follows: For two words \( x, y \in \Gamma^* \) we define \( x \equiv_L y \) if for all \( u, v \in \Gamma^* \) we have \( uxv \in L \Leftrightarrow uyv \in L \). The syntactic monoid \( M(L) \) of \( L \) is the quotient of \( \Gamma^* \) by this congruence, i.e., \( M(L) \) consists of all congruence classes of the syntactic congruence of \( L \).

A comprehensive introduction to the concept of syntactic monoids of word languages can be found in many text books, see e.g. [Pin86] (especially Section 2.4.) or [Str94] (especially Theorem V.1.3).

A group contained in a semigroup \( S \) is a subsemigroup of \( S \) that is a group. If \( G \) is a group contained in a monoid \( M \), the neutral element of \( G \) may or may not be the same as
that of $M$. A submonoid of a monoid $M$ is a subsemigroup of $M$ that contains the neutral element of $M$.

Let $S, T$ be semigroups. Then $S$ divides $T$ (written $S \prec T$) iff $S$ is a homomorphic image of a subsemigroup of $T$. Then $\prec$ is transitive.

### 2.7 Pseudovarieties and Group Complexity

The group complexity was introduced in [KR65] and assigns a non-negative integer $c(S)$ to every semigroup $S$. We briefly introduce the related notions, see e.g. [Eil76, RS09].

A class $V$ of finite semigroups is a pseudovariety (see [RS09], Definition 1.2.30) if the following properties hold:

- $V$ contains a one-element semigroup;
- For all semigroups $S_1, S_2 \in V$ we have $S_1 \times S_2 \in V$, where $S_1 \times S_2$ is the direct product;
- For all semigroups $S, T$ with $S \prec T$ and $T \in V$ we have $S \in V$.

The following are pseudovarieties:

- the class $G$ of finite groups, and
- the class $A$ of finite aperiodic semigroups.

**Definition 2.8** Let $S, T$ be finite semigroups, and let us write $S$ additively. A left action of $T$ on $S$ is a map $T \times S \rightarrow S$, where the image of $(t, s)$ is denoted $ts$, that satisfies the following two properties:

- $t(s + s') = ts + ts'$ for every $t \in T$ and every $s, s' \in S$,
- $(tt')s = t(t's)$ for every $t, t' \in T$ and every $s \in S$.

For two semigroups $S$ and $T$, the semidirect product $S \rtimes T$ wrt. a given left action is defined as the set $S \times T$ with multiplication given by

$$(s, t)(s', t') = (s + ts', tt').$$

For two pseudovarieties $V$ and $W$, the semidirect product $V \rtimes W$ is the pseudovariety generated by the semigroups of the form $V \rtimes W$ with $V \in V$ and $W \in W$.

We define (cf. [RS09], Definition 4.3.10):

$$C_0 = A,$$
$$C_{n+1} = A \ast (G \ast C_n) = C_n \ast (A \ast G), \text{ for every } n \geq 0.$$ 

The famous “prime decomposition theorem” of [KR65] asserts that every finite semigroup is in $\bigcup_{n \geq 1} C_n$. Thus for every finite semigroup $S$, the group complexity $c(S) := \min \{n \mid S \in C_n\}$ is well defined.

For a regular word language $L$, the group complexity of $L$ is defined as $c(L) = c(M(L))$. 
2.8 Height Fragment Technique and Results

Let $\mathcal{P}$ be a class of picture languages over a fixed alphabet $\Gamma$ and let $\alpha$ be a function that assigns to every regular word language an element from $\mathbb{N}$. We say that

- $\mathcal{P}$ is at most $k$-fold exponential wrt. $\alpha$ if for every $L \in \mathcal{P}$ we have that $\alpha(L[m])$ is at most $k$-fold exponential in $m$.
- $\mathcal{P}$ is at least $k$-fold exponential wrt. $\alpha$ if there exists $L \in \mathcal{P}$ such that $\alpha(L[m])$ is at least $k$-fold exponential in $m$.

The following remark is immediate. Its contraposition provides a technique to separate two classes of picture languages, given a complexity measure $\alpha$ as above.

**Remark 2.9 (Height Fragment Technique)** Let $\mathcal{P}, \mathcal{P}'$ be picture language classes. If $\mathcal{P}' \subseteq \mathcal{P}$ and $\mathcal{P}$ is at most $k$-fold exponential wrt. $\alpha$, then so is $\mathcal{P}'$.

We say that a formula class $\mathcal{F}$ is at most (or at least, respectively) $k$-fold exponential wrt. $\alpha$ if the class $\{\text{Mod}(\varphi) \mid \varphi \in \mathcal{F}\}$ is.

The following is the main result of this paper and will be proved in Section 4.

**Theorem 2.10** Let $k \geq 1$. The formula classes $\Sigma_{1}^{\text{mon}}(\Pi_{k-1}^{0}(\Delta_{1}^{\text{mon}}))$, $\text{FO}(\Sigma_{k}^{\text{mon}})$, and $\Sigma_{k}^{\text{mon}}$ are both at most and at least $k$-fold exponential wrt. group complexity.

By Remark 2.9 this implies.

**Corollary 2.11** Let $k \geq 1$. There is a picture language definable by a $\Sigma_{k+1}^{\text{mon}}$-formula but not by an $\text{FO}(\Sigma_{k}^{\text{mon}})$-formula. In particular, there is a picture language definable by a $\text{FO}(\Sigma_{k+1}^{\text{mon}})$-formula but not by an $\text{FO}(\Sigma_{k}^{\text{mon}})$-formula.

The first statement of the above corollary is a new result. The second statement has already been proved in [Mat99, Corollary 2.31]. The proof in this paper is simpler but requires at least four (or, with standard encoding arguments, at least two) symbols in the alphabet, whereas the proof in [Mat99] applies also to singleton alphabets.

Theorem 2.10 also provides new witnesses for the strictness of the alternation hierarchy of MSO over pictures, i.e., the result of [Sch97] that $\Sigma_{k+1}^{\text{mon}}$ is more expressive than $\Sigma_{k}^{\text{mon}}$. Unlike the witnesses in [Sch97, MST02, Mat99], these witnesses are not over a singleton alphabet, so the result is formally weaker.

Another consequence of Theorem 2.10 is the following:

**Corollary 2.12** Let $k \geq 1$. There is picture language definable by a $\Sigma_{1}^{\text{mon}}(\text{FO}(\Sigma_{1}^{\text{mon}}))$-formula but not by a $\text{FO}(\Sigma_{k}^{\text{mon}})$-formula.

For the case $k = 1$, this is the generalization of Corollary 1.2 to picture languages.
3 Expressibility Result

In this section we will prove the upper bound part of Theorem 2.10. For this aim, we will construct a picture language whose height-$m$ fragment has group complexity $k$-fold exponential in $m$ and that is definable in the respective formula classes.

The idea is to code large Boolean square matrices with pictures of small height. The picture language then consists of pictures of the form $p_1\ldots p_n$, where $p_1,\ldots, p_n$ encode square matrices whose matrix product over the Boolean semiring is not the zero matrix. This way, the syntactic monoid contains the monoid of binary relations, established by the syntactic congruence classes of the encoded matrices. By a result of Rhodes (see Theorem 3.18), that monoid has high group complexity.

3.1 Iterated Matrix Multiplication

Let us consider the semiring of $m \times m$-Matrices over the Boolean semiring. Its product $\cdot$ is the standard matrix product.

**Lemma 3.1** Let $m \geq 1$. Then for every $n \geq 0$ and all matrices $A_1,\ldots, A_n \in \{0,1\}^{m \times m}$, we have the following equivalence:

\[\prod_{h=1}^{n} A_h \neq 0 \iff \exists i_1,\ldots, i_{n+1} \leq m : \forall h \leq n : A_h(i_h, i_{h+1}) = 1.\]

**Proof** First, we show by induction on $n$ that the following equivalence holds for every $n$, every $k, l \in \{1, \ldots, n\}$ and all matrices $A_1,\ldots, A_n \in \{0,1\}^{m \times m}$:

\[(\prod_{h=1}^{n} A_h)(k, l) = 1 \iff \exists i_1,\ldots, i_{n+1} \leq m : i_1 = k \land i_{n+1} = l \land (\forall h \leq n : A_h(i_h, i_{h+1}) = 1).\]

This equivalence is immediate for $n = 0$. Assume that the equivalence holds for some $n \geq 0$, and let $A_1,\ldots, A_{n+1} \in \{0,1\}^{m \times m}$. Let $k, l \leq m$. Then \((\prod_{h=1}^{n+1} A_h)(k, l) = (\prod_{h=1}^{n} A_h) \cdot A_{n+1})(k, l)\). Thus the following equivalence chain holds:

\[(\prod_{h=1}^{n+1} A_h)(k, l) = 1 \iff \exists i_1,\ldots, i_{n+2} \leq m : i_1 = k \land (\forall h \leq n : A_h(i_h, i_{h+1}) = 1) \land A_{n+1}(i_{n+1}, l) = 1 \iff \exists i_1,\ldots, i_{n+2} \leq m : i_1 = k \land (\forall h \leq n + 1 : A_h(i_h, i_{h+1}) = 1).\]

This completes the induction. The lemma is now immediate. □
3.2 Picture Languages Defined by a Regular Top-Row Language

For a non-empty picture \( p \), we define \( \text{top}(p) \) to be the word of length \( |p| \) in the top row, i.e., \( \text{top}(p) = p(1,1) \ldots p(1,|p|) \).

We observe the following.

**Proposition 3.2** Let \( \Gamma = \{0,1\}^I \) be an attributed alphabet. Let \( L \subseteq \Gamma^+ \) be a regular word language. Then \( \text{top}^{-1}(L) := \{ p \in \Gamma^+ \mid \text{top}(p) \in L \} \) is definable by a \( \Delta^{\mon}_1 \)-formula.

**Proof** Let \( \mathfrak{A} \) be a deterministic finite automaton that recognizes \( L \). We may assume w.l.o.g. that the state set \( Q \) of \( \mathfrak{A} \) is of the form \( \{0,1\}^J \) for some index set \( J \) disjoint from \( I \). Let \( q_0 \in Q \) be the initial state of \( \mathfrak{A} \) and \( F \subseteq Q \) be the set of final states of \( \mathfrak{A} \). Let \( \Delta \subseteq Q \times \Gamma \times Q \) be the transition relation of \( \mathfrak{A} \).

We will construct a \( \Delta^{\mon}_1 \)-formula that asserts that the uniquely determined run of \( \mathfrak{A} \) on the top row of a non-empty input picture is accepting. For this aim, we encode the run into an assignment to free variables \( (X_\mu)_{\mu \in J} \) in the obvious way.

Recall the formulas \( \text{top}(x) \), \( \text{left}(x) \), and \( \text{right}(x) \) from Example 2.3.

For every \( a : I \rightarrow \{0,1\} \), set

\[
\text{letter}_a(x) := \bigwedge_{\mu \in a^{-1}(1)} X_\mu x \land \bigwedge_{\mu \in a^{-1}(0)} \neg X_\mu x.
\]

Similarly, for every \( q : J \rightarrow \{0,1\} \), set

\[
\text{state}_q(x) := \bigwedge_{\mu \in q^{-1}(1)} X_\mu x \land \bigwedge_{\mu \in q^{-1}(0)} \neg X_\mu x.
\]

Let

\[
\varphi = \forall x \left( \text{left}(x) \land \text{top}(x) \rightarrow \text{state}_{q_0}(x) \right)
\land \bigwedge_{(q,a,q') \in \Delta} \forall x \forall x' \left( \text{state}_q(x) \land \text{letter}_a(x) \land S_2xx' \land \text{top}(x) \rightarrow \text{state}_{q'}(x') \right).
\]

Then \( \varphi \) asserts, for a non-empty input picture \( p \) over alphabet \( \{0,1\}^{I \cup J} \), that \( \text{top}(\text{restr}_I(p)) \) encodes (in the obvious way) the unique run of \( \mathfrak{A} \) on the input word \( \text{top}(\text{restr}_I(p)) \).

Let

\[
\psi = \exists x \left( \text{top}(x) \land \text{right}(x) \land \bigvee_{f \in F} \text{state}_f(x) \right).
\]

Then \( \psi \) asserts that for a non-empty input picture over alphabet \( \{0,1\}^J \) that the state encoded in the top right corner is final. Consider the formulas

\[
\sigma = \exists (X_\mu)_{\mu \in J} (\varphi \land \psi),
\]

\[
\pi = \forall (X_\mu)_{\mu \in J} (\varphi \rightarrow \psi).
\]

Both \( \sigma \) and \( \pi \) assert for a non-empty picture \( p \) over alphabet \( \{0,1\}^J \) that the unique run of \( \mathfrak{A} \) on the top row of \( p \) reaches a final state, i.e., that its top row is in \( L \). Thus \( \sigma \) and \( \pi \) are equivalent and define \( \text{top}^{-1}(L) \). This completes the proof. \( \square \)
Corollary 3.3 Let \( L \subseteq \{0,1\}^+ \) be a regular language of non-empty words. Let \( \Gamma = \{0,1\}^I \) be some attributed alphabet, let \( \mu \in I \) be an attribute. Define \( \text{top}^{-1}_\mu(L) := \{ p \in \Gamma^{+,+} \mid \text{top}(\text{pr}_\mu(p)) \in L \} \). There exists a \( \Delta^\text{mon}_1 \)-formula \( \text{top-in}_{\mu}(L) \) such that \( \text{Mod}(\text{top-in}_{\mu}(L)) = \text{top}^{-1}_\mu(L) \).

Proof For every picture \( p \in \Gamma^{+,+} \) we have the equivalence chain \( p \in \text{top}^{-1}_\mu(L) \) iff \( \text{top}(\text{pr}_\mu(p)) \in L \) iff \( \text{pr}_\mu(\text{top}(p)) \in L \) iff \( p \in \text{top}^{-1}(\text{pr}_\mu^{-1}(L)) \). Now apply Proposition 3.2 to the regular word language \( \text{pr}_\mu^{-1}(L) \).

When we write \( \text{top}^{-1}_\mu(L) \) in the following, the alphabet \( \Gamma \) must be clear from the context.

3.3 Relativization and Closure Under Concatenation

In this section, we will show the following result:

Proposition 3.4 For every \( k \geq 0 \), the class of \( \Sigma^\text{mon}_1(\Pi_0^\mu(\Delta^\text{mon}_1)) \)-definable picture languages is closed under column concatenation and column closure.

Its proof (see end of this section) is well-known for the important case \( k = 0 \). We prepare the proof for the case \( k \geq 1 \) with the concept of relativization, cf. [Str94], Lemma VI.1.3. Recall the definition of the \( \Delta^\text{mon}_1 \)-formula \( x \leq x' \) from Examples 2.4, 2.5. For a non-empty picture \( p \) and \( j, j' \) with \( 1 \leq j \leq j' \leq |p| \) we define \( p[j,j'] \) to be the picture that is assembled by the columns \( j, \ldots, j' \) of \( p \).

Let \( J, K \) be disjoint attribute sets. Let \( \varphi \) be a formula with free set variables in \( \{X_\mu \mid \mu \in J\} \) and free first-order variables in \( \{x_\nu \mid \nu \in K\} \). Let \( x, x' \) be two fresh first-order variables. Let \( \varphi' \) be a formula whose free variables are those of \( \varphi \) as well as \( x, x' \). We say that \( \varphi' \) relativizes \( \varphi \) to \( x, x' \) iff for all non-empty pictures \( p \in \text{Unique}_{J,K;K} \) and all \( j, j' \leq |p| \) we have

\[
p, (\frac{1,j}{x}) (\frac{1,j'}{x'}) \models \varphi' \iff j \leq j' \text{ and } p[j,j'] \models \varphi.
\]

Intuitively, \( \varphi' \) says about the subpicture demarcated by the top-row positions \( x, x' \) the same as \( \varphi \) says about the whole picture.

We will need the following obvious remark:

Remark 3.5 Let \( \varphi_{[x,x']} \) relativize \( \varphi \) to \( x, x' \). Let \( p_1, p_2 \) be two non-empty pictures of the same size and \( j, j' \leq |p_1| \) such that \( p_1[j,j'] = p_2[j,j'] \). Then

\[
p_1, (\frac{1,j}{x}) (\frac{1,j'}{x'}) \models \varphi_{[x,x']} \iff p_2, (\frac{1,j}{x}) (\frac{1,j'}{x'}) \models \varphi_{[x,x']}.
\]

Lemma 3.6 For every first-order formula \( \varphi \) that does not use the first-order variables \( x, x' \) there is a \( \Delta^\text{mon}_1 \)-formula \( \varphi' \) that relativizes \( \varphi \) to \( x, x' \).


\textbf{Proof} Set

\[ \text{columns} = \forall x_1 \forall x_2 (S_1 x_1 x_2 \rightarrow (X_{\text{rect}} x_1 \leftrightarrow X_{\text{rect}} x_2)). \]

Then \text{columns} asserts that \( X_{\text{rect}} \) is closed under vertical predecessors and successors and hence a union of columns. Recall the formulas \( \text{top}(x) \) and \( \text{left}(x) \) from Example 2.3. Set

\[ \text{between} = \text{columns} \wedge X_{\text{rect}} x \wedge X_{\text{rect}} x' \wedge \]

\[ \forall x_1 (S_2 x_1 x \rightarrow \neg X_{\text{rect}} x_1) \]

\[ \forall x_2 (S_2 x_2 x \rightarrow \neg X_{\text{rect}} x_2) \]

\[ \forall x_1 x_2 (S_2 x_1 x_2 \wedge \text{top}(x_1) \wedge x_1 \neq x' \wedge x_2 \neq x \rightarrow (X_{\text{rect}} x_2 \leftrightarrow X_{\text{rect}} x_1)). \]

Intuitively, \( \text{between} \) asserts for a set \( X_{\text{rect}} \) and two top-row positions \( x, x' \) that \( X_{\text{rect}} \) is the subblock cyclically between the columns marked by the top-row positions \( x \) and \( x' \). In other words, for \( j, j', m, n \geq 1 \) with \( j, j' \leq n \) there exists exactly one picture \( p \) of size \((m, n)\) over alphabet \( \{0, 1\}^{\text{rect}} \) such that \( p, \frac{(1,j)}{x}, \frac{(1,j')}{x'} \models \text{between} \). That picture is characterized as follows: If \( j \leq j' \), then \( \text{pr}_{\text{rect}}(p) \) carries a 1 exactly in all positions in the columns \( j, \ldots, j' \). If \( j > j' \), then \( \text{pr}_{\text{rect}}(p) \) carries a 1 exactly in all positions in the columns \( 1, \ldots, j', j, \ldots, |p| \).

We introduce a formula \( \text{nowrap} \) that asserts that the first case is true.

\[ \text{nowrap} = \text{left}(x) \lor \exists x_2 (\text{left}(x_2) \wedge X_{\text{rect}} x_2). \]

For every non-empty picture \( p \) over \( \{0, 1\}^{\text{rect}} \) and every \( j, j' \leq |p| \) with \( p, \frac{(1,j)}{x}, \frac{(1,j')}{x'} \models \text{between} \) we have

\[ p, \frac{(1,j)}{x} \models \text{nowrap} \iff j \leq j'. \]

Let \( \varphi \) be a first-order formula that does not use the variables \( x, x', \) and \( X_{\text{rect}} \). Assume w.l.o.g. that there are no universal quantifications in \( \varphi \). Let the formula \( \varphi' \) result from \( \varphi \) by relativization to \( X_{\text{rect}} \), i.e., by successively replacing every first-order quantification of the form \( \exists x \phi \) by \( \exists x (X_{\text{rect}} x \wedge \phi) \).

Define two formulas \( \sigma, \pi \) as:

\[ \sigma(x, x') = \exists X_{\text{rect}} (\text{between} \wedge \text{nowrap} \wedge \varphi'), \]

\[ \pi(x, x') = \forall X_{\text{rect}} (\text{between} \rightarrow (\text{nowrap} \wedge \varphi')). \]

Then \( \sigma \in \Sigma_1^{\text{mon}} \) and \( \pi \in \Pi_1^{\text{mon}} \). We have for every non-empty picture \( p \) and every \( j, j' \leq |p| \) that

\[ p, \frac{(1,j)}{x}, \frac{(1,j')}{x'} \models \pi \iff (j \leq j' \land p[j, j'] \models \varphi) \iff p, \frac{(1,j)}{x}, \frac{(1,j')}{x'} \models \sigma. \]

Hence \( \varphi_{[x, x']} = \sigma \) is a \( \Delta_1^{\text{mon}} \)-formula and has the desired property.

This completes the proof. \( \square \)

A formula class \( \mathcal{F} \) is \textit{relativizable} iff for every formula \( \varphi \in \mathcal{F} \) and two fresh first-order variables \( x, x' \), there is a formula \( \varphi' \in \mathcal{F} \) that relativizes \( \varphi \) to \( x, x' \).

\textbf{Lemma 3.7} \textit{For every} \( k \geq 0 \), the formula class \( \Pi_k^0(\Delta_1^{\text{mon}}) \) is relativizable.
3 EXPRESSION RESULT

Proof The proof is by induction on \( k \). For the induction basis, let \( k = 0 \) and \( \varphi \in \Delta^\text{mon}_1 \). Then \( \varphi \) is equivalent to a formula of the form \( \exists X_1 \ldots X_n(\varphi') \) as well as to a formula of the form \( \forall X_1 \ldots X_n(\varphi'') \) for two first-order formulas \( \varphi', \varphi'' \).

As we have shown in the preceding lemma, there exist a \( \Sigma^\text{mon}_1 \)-formula \( \varphi_{[x,x']} \) and a \( \Pi^\text{mon}_1 \)-formula \( \varphi''_{[x,x']} \) that relativize \( \varphi' \) (and \( \varphi'' \), respectively) to \( x, x' \).

Let
\[
\sigma = \exists X_1 \ldots \exists X_n(\varphi'_{[x,x']}),
\]
\[
\pi = \forall X_1 \ldots \forall X_n(\varphi''_{[x,x']}).
\]

Then \( \sigma \in \Sigma^\text{mon}_1 \) and \( \pi \in \Pi^\text{mon}_1 \). By Remark 3.5 they are equivalent and relativize \( \varphi \) to \( x, x' \). This completes the proof for the case \( k = 0 \).

Now assume \( k \geq 1 \) and the claim is true for \( k - 1 \) instead of \( k \). Let \( \varphi \in \Pi^0_k(\Delta^\text{mon}_1) \). Then \( \varphi \) is equivalent to a formula of the form
\[
\forall x_1 \ldots \forall x_n(\neg \psi),
\]
for some \( n \geq 1 \) and \( \psi \in \Pi^0_{k-1}(\Delta^\text{mon}_1) \). By assumption there is a \( \Pi^0_{k-1}(\Delta^\text{mon}_1) \)-formula \( \psi_{[x,x']} \) that relativizes \( \psi \) to \( x, x' \). Choose
\[
\varphi_{[x,x']} = \forall x_1 \ldots \forall x_n \left( \left( \bigwedge_{i=1}^n x \leq x_i \land x_i \leq x' \right) \rightarrow \neg \psi_{[x,x']} \right).
\]

Since \( x \leq x' \) is a \( \Delta^\text{mon}_1 \)-formula, \( \varphi_{[x,x']} \) is indeed a \( \Pi^0_k(\Delta^\text{mon}_1) \)-formula. Besides, \( \varphi_{[x,x']} \) relativizes \( \varphi \) to \( x, x' \). This completes the proof. \( \square \)

In Section 4.3 we will come back to the following observation. See also Remark 2.2.

Remark 3.8 Let \( \mathcal{F} \) be a class of formulas closed under conjunction and disjunction. The class of \( \Sigma^\text{mon}_1(\mathcal{F}) \)-definable picture languages is closed under intersection, union, and alphabet projection.

Lemma 3.9 Let \( \mathcal{F} \supseteq \Delta^\text{mon}_1 \) be a relativizable class of formulas. Let \( \Gamma = \{0,1\}^I \). Let \( L_1, L_2 \subseteq \Gamma^{+,+} \) be two \( \Sigma^\text{mon}_1(\mathcal{F}) \)-definable picture languages.

1. If \( \mathcal{F} \) is closed under conjunction and disjunction, then \( L_1L_2 \) is \( \Sigma^\text{mon}_1(\mathcal{F}) \)-definable.

2. If \( \mathcal{F} \) is closed under conjunction, disjunction, and universal FO-quantification, then \( L_1^+ \) is \( \Sigma^\text{mon}_1(\mathcal{F}) \)-definable.

Proof of Lemma 3.9, Claim 1 Let \( \varphi, \psi \in \Sigma^\text{mon}_1(\mathcal{F}) \) be formulas with \( \text{Mod}(\varphi) = L_1 \) and \( \text{Mod}(\psi) = L_2 \). Let \( x_0, x_1, x_2, x_3 \) be four fresh first-order variables. Choose formulas \( \varphi_{[x_0,x_1]} \) and \( \psi_{[x_2,x_3]} \) that relativize \( \varphi \) and \( \psi \), respectively. Recall the formulas \( \text{top}(x) \), \( \text{left}(x) \), and \( \text{right}(x) \) from Example 2.3.

Choose
\[
\varphi' = \exists x_0, x_1, x_2, x_3 \left( \text{top}(x_0) \land \text{top}(x_1) \land \text{top}(x_2) \land \text{top}(x_3) \land \text{left}(x_0) \land S_{23} x_1 x_2 \land \text{right}(x_3) \land \varphi_{[x_0,x_1]} \land \psi_{[x_2,x_3]} \right).
\]
Then $\varphi' \in \Sigma_1^0(\Sigma_1^\text{mon}(F)) = \Sigma_1^\text{mon}(F)$. It remains to show that $\text{Mod}(\varphi') = L_1 L_2$.

Let $p \in \text{Mod}(\varphi')$. Then there exist top-row positions $\langle 1, j_0 \rangle, \langle 1, j_1 \rangle, \langle 1, j_2 \rangle, \langle 1, j_3 \rangle \in \text{dom}(p)$ such that $j_0 = 1$ and $j_1 + 1 = j_2$ and $j_3 = |p|$ and $p[j_0, j_1] \models \varphi$ and $p[j_2, j_3] \models \psi$. This implies $p \in \text{Mod}(\varphi) \text{Mod}(\psi) = L_1 L_2$. Thus we have shown $\text{Mod}(\varphi') \subseteq L_1 L_2$. The converse inclusion is similar. This completes the proof of Claim 1. □

**Proof of Lemma** 3.9 **Claim** 2 Let $\mathcal{X} = (X_\mu)_{\mu \in J}$ be a tuple of set variables and $\varphi \in F$ be a formula such that

$$\text{Mod}(\exists \mathcal{X} \varphi) = L_1.$$

Let $\text{end}$ be a fresh attribute. Choose $\Delta_1^\text{mon}$-formulas $\text{top-in}_{\text{end}}(0^*1)$ and $\text{top-in}_{\text{end}}(\{0,1\}^*1)$ according to Corollary 3.3. Set $\varphi' = \varphi \land \text{top-in}_{\text{end}}(0^*1)$. Let $x, y$ be fresh first-order variables. Let $\varphi'_{[x,y]}$ be an $F$-formula that relativizes $\varphi'$ to $x, y$. Let no-between be a $\Delta_1^\text{mon}$-formula that relativizes $\text{top-in}_{\text{end}}(0^*1)$ to $x, y$.

Recall formula $\text{top}(x)$ from Example 2.3. Set

$$\varphi'' = \forall x \forall y(\text{next}_{\text{end}} \rightarrow \varphi'_{[x,y]}).$$

Then $\text{next}_{\text{end}}$ is a $\Delta_1^\text{mon}$-formula and $\varphi'' \in \Sigma_1^\text{mon}(F)$. We claim that

$$\text{Mod}(\varphi'') = L_1^+.$$  

(1)

Let $J' = J \cup \{\text{end}\}$.
First let $p \in \text{Mod}_J(\varphi'')$. There exists a picture $p'' \in \text{Mod}_{J'}(\varphi'')$ such that $\text{ex}_{J \cup \{\text{end}\}}(p'') = p$ and $\text{top}(\text{pr}_{\text{end}}(p'')) \in \{0,1\}^*1$.

Pick $n \geq 1$ and top-row positions $\langle 1, j_1 \rangle, \ldots, \langle 1, j_n \rangle$ such that $j_1 < \ldots < j_n$ such that these positions are those top-row positions of $p''$ that carry 1 for attribute $\text{end}$. (Note that $j_n = |p|$.) Choose $j_0 = 0$.

Choose a decomposition $p'' = p_1' \ldots p_n'$ into non-empty pictures $p_1', \ldots, p_n'$ such that $|p_1' \ldots p_k'| = j_k$ for every $k \in \{1, \ldots, n\}$. For every $k$, choose picture $p_k$ over alphabet $\{0,1\}^I$ such that $\text{ex}_{J \cup \{\text{end}\}}(p_k') = p_k$. Then

$$p = p_1 \ldots p_n.$$

Let $k \in \{1, \ldots, n\}$. The position $\langle 1, j_{k-1} + 1 \rangle$ is a position in the picture $p''$ whose $S_2$-predecessor either does not exist (in case $k = 1$) or carries a 1 for attribute $\text{end}$. Thus

$$p'' , \frac{\langle 1, j_{k-1} + 1 \rangle \langle 1, j_k \rangle}{x \ y} \models \text{next}_{\text{end}}.$$  

Since $p'' \models \varphi''$, this implies

$$p'' , \frac{\langle 1, j_{k-1} + 1 \rangle \langle 1, j_k \rangle}{x \ y} \models \varphi'_{[x,y]},$$

which in turn implies $p_k' \in \text{Mod}_{J'}(\varphi') \subseteq \text{Mod}_{J'}(\varphi) = \text{Mod}_{J \cup J \cup \{\text{end}\}}(\varphi)$. Thus $\text{ex}_{\{\text{end}\}}(p_k') \in \text{Mod}_{J \cup J}(\varphi)$. By choice of $p_k$, we have $p_k \in \text{Mod}_J(\exists \mathcal{X} \varphi) = L_1$. 


Since $k$ has been chosen arbitrarily from $\{1, \ldots, n\}$, this implies $p = p_1 \ldots p_n \in L_1^+ \subseteq L_1^+$. This completes the proof of the direction “$\subseteq$” of Equation (1).

For the converse direction, let $p \in L_1^+$. Pick $n \geq 1$ and $p_1, \ldots, p_n \in L_1$ such that $p = p_1 \ldots p_n$. Choose $j_0 = 0$ and for $k \in \{1, \ldots, n\}$, choose $j_k = |p_1 \ldots p_k|$. For every $k$, we have $p_k \in \text{Mod}_f(\exists \bar{X}(\varphi))$, thus for every $k$, there exists $p'_k \in \text{Mod}_I(\varphi)$ such that $\text{ex}_{J(\text{end})}(p'_k) = p_k$. Furthermore, we may pick $p'_k$ in such a way that $\text{top}(\text{pr}_{\text{end}}(p'_k)) \in \text{ex}_{J(\text{end})}(p''_k) = p''_k$. Then $\text{ex}_{J(\text{end})}(p''_k) = p$ and $\text{top}(\text{pr}_{\text{end}}(p''_k)) \in (0^*1)^n \subseteq \{0, 1\}^*1$. In order to show $p \in \text{Mod}_I(\varphi''')$, it remains to show $p'' \in \text{Mod}_I(\varphi'')$. To see this, let $z, z'$ be positions in $p''$ such that $p'', z_{\bar{x}}z_{\bar{y}} \models \text{next}_\text{end}(x, y)$. By definition of $\text{next}_\text{end}$, these are top-row positions, so there are $j, j'$ such that $z = \langle 1, j \rangle$ and $z' = \langle 1, j' \rangle$, and (because $\text{top}(\text{pr}_{\text{end}}(p'_k)) \in 0^*1$ for every $k$), the columns $j$ and $j'$ are the start- and end-column of one and the same $p'_k$-subblock of $p''$ (for some $k \in \{1, \ldots, n\}$). Since $p'_k \models \varphi \wedge \text{top-in}_{\text{end}}(0^*1)$, we conclude that this $p'_k$-subblock is in $\text{Mod}(\varphi')$, i.e., $p'', z_{\bar{x}}z_{\bar{y}} \models \varphi'[x,y]$. Since $z, z'$ have been chosen arbitrarily, this implies that $p'' \models \varphi''$. We also have $p'' \models \text{top-in}_{\text{end}}(0^*1)$. This shows $p \models \varphi'''$ and completes the proof of Equation (1) and of Lemma 3.9.

We are now ready to prove the result of this section.

**Proof of Proposition 3.4** For $k \geq 1$, this is a consequence of Lemmas 3.7, 3.9 and the fact that $\Pi^0_1(\Delta^0_{\text{mon}})$ is closed under conjunction, disjunction, and universal first-order quantifications.

For $k = 0$, we have $\Sigma^0_1(\Pi^0_k(\Delta^0_{\text{mon}})) = \Sigma^0_1(\Pi^0_k(\Delta^0_{\text{mon}}))$, which is the class of recognizable picture languages. For this class, the statement is well known, see e.g. [GRST96].

### 3.4 Assembling the Picture Language

For the rest of this section, let $\mathcal{F} \supseteq \Delta^0_{\text{mon}}$ be a class of formulas such that the class of $\Sigma^0_1(\mathcal{F})$-definable picture languages is closed under column concatenation, column closure, union and intersection. We will need our results only for the cases provided by Proposition 3.4, i.e., for the case $\mathcal{F} = \Pi^0_k(\Delta^0_{\text{mon}})$ for some $k \geq 0$.

For a function $f : \mathbb{N}_{\geq 1} \rightarrow \mathbb{N}_{\geq 1}$ and an alphabet $\Gamma$, the picture language associated to $f$ is defined as

$$L_{f, \Gamma} = \{ p \in \Gamma^{+, +} \mid |p| = f(\overline{p}) \}.$$

Typically $\Gamma$ is clear from the context or irrelevant because of Remark 2.11 so we usually omit the second subscript.

If $f : \mathbb{N}_{\geq 1} \rightarrow \mathbb{N}_{\geq 1}$ is a function, we define another function $f + 1 : \mathbb{N}_{\geq 1} \rightarrow \mathbb{N}_{\geq 1}, n \mapsto f(n) + 1$.

**Remark 3.10** Let us denote the set of all non-empty pictures of length 1 over $\Gamma$ by $\Gamma^{+, 1}$. Then $L_{f + 1, \Gamma} = L_{f, \Gamma} \Gamma^{+, 1}$. Clearly $\Gamma^{+, 1}$ is $\mathcal{F}$-definable, thus if $L_f$ is $\Sigma^0_1(\mathcal{F})$-definable, then, by Lemma 3.8, so is $L_{f + 1}$.
If \( n \geq 1 \) and \( i, j \in \{1, \ldots, n\} \), set \( \text{code}_n(i, j) = (i-1)n + j \). Then \( \text{code}_n \) defines a bijection from \( \{1, \ldots, n\} \times \{1, \ldots, n\} \) onto \( \{1, \ldots, n^2\} \).

If \( n \geq 1 \) and \( p \) is a picture of length \( n^2 \) over \( \{0, 1\} \), we define \( \text{fold}_n(p) \) as the \( n \times n \)-matrix over \( \{0, 1\} \) with \( \text{fold}_n(p)(i, j) = p(1, \text{code}_n(i, j)) \) for every \( i, j \in \{1, \ldots, n\} \).

Every top-row position of a picture \( p \) of length \( n^2 \) corresponds to exactly one position in the \( n \times n \)-matrix \( \text{fold}_n(p) \). The intuition for the attributes used in the following lemma is: Picture positions marked by \( \text{blk} \) (or \( \text{diag} \), or \( \text{end} \)) correspond to the matrix positions in the right column (or on the diagonal, or in the bottom-right corner, respectively).

**Lemma 3.11** Let \( f : \mathbb{N}_{\geq 1} \to \mathbb{N}_{\geq 1} \) be a function such that its associated picture language \( L_f \) is \( \Sigma_1^{\text{mon}}(\mathcal{F}) \)-definable. Consider attribute set \( I = \{\text{diag}, \text{end}, \text{blk}\} \).

There exists a \( \Sigma_1^{\text{mon}}(\mathcal{F}) \)-definable picture language \( L_0 \) such that for all pictures \( p \) over alphabet \( \{0, 1\}^I \) we have: \( p \in L_0 \) iff \( |p| = f(\overline{p})^2 \) and for every \( k \leq |p| \) we have the following three conditions:

\[
\begin{align*}
p(1, k)(\text{blk}) = 1 & \quad \iff \quad f(\overline{p}) \mid k, \quad (2) \\
p(1, k)(\text{diag}) = 1 & \quad \iff \quad (f(\overline{p}) + 1) \mid (k - 1), \quad (3) \\
p(1, k)(\text{end}) = 1 & \quad \iff \quad k = f(\overline{p})^2. \quad (4)
\end{align*}
\]

**Proof** First, we observe that for every \( k \leq |p| \) the Equivalence (3) is equivalent to

\[
\begin{align*}
p(1, k)(\text{diag}) = 1 & \quad \iff \quad k \in \{\text{code}_{f(\overline{p})}(i, i) \mid i \in \{1, \ldots, f(\overline{p})\}\}. \quad (5)
\end{align*}
\]

This is because for every \( k \leq |p| \), we have the equivalence chain: \( (f(\overline{p}) + 1) \mid (k - 1) \) iff \( \exists a \geq 0 : a(f(\overline{p}) + 1) = k - 1 \) iff \( \exists a \geq 0 : af(\overline{p}) + a + 1 = k \) iff \( \exists a \geq 0 : \text{code}_{f(\overline{p})}(a + 1, a + 1) = k \)

iff \( \exists i \geq 1 : \text{code}_{f(\overline{p})}(i, i) = k \).

Recall the definition of \( \text{top}^{-1}_\mu \) from Corollary 3.3. Let

\[
\begin{align*}
M_1 & = L_f \cap \text{top}_\text{blk}^{-1}(0^*1), \\
M_2 & = L_{f+1} \cap \text{top}_\text{diag}^{-1}(0^*1), \\
M_3 & = \text{top}_\text{diag}^{-1}(1)M_2^*, \\
M_4 & = M_1^+ \cap M_3 \cap \text{top}_\text{end}^{-1}(0^*1), \\
X & = \{a \in \{0, 1\}^I \mid a(\text{diag}) = 1 \land a(\text{blk}) = 1 \iff a(\text{end}) = 1\}, \\
M_5 & = \text{top}^{-1}(X^+), \\
L_0 & = M_4 \cap M_5.
\end{align*}
\]

Then \( L_0 \) is \( \Sigma_1^{\text{mon}}(\mathcal{F}) \)-definable by Corollary 3.3 Remarks 3.8, 3.10 and Lemma 3.9.

For the only-if-direction of the lemma, let \( p \in L_0 \). Since \( p \in M_1^+ \), it may be decomposed into subpictures \( p = p_1 \ldots p_n \) such that for each \( h \leq n \) we have \( |p_h| = f(\overline{p}) \) and \( \text{top}(\text{pr}_\text{blk}(p_h)) \in 0^*1 \). This implies (2) for every \( k \leq |p| \).

Since \( p \in M_3 \), it may be decomposed into subpictures \( p = qp'_1 \ldots p'_{n'} \) such that \( n' \geq 1 \) and \( |q| = 1 \) and \( \text{top}(\text{pr}_\text{diag}(q)) = 1 \) and for every \( h \leq n' \) we have \( |p'_h| = f(\overline{p}) + 1 \) and \( \text{top}(\text{pr}_\text{diag}(p_h)) \in 0^*1 \). Thus for every \( k \leq |p| \) we have Equivalence (3) and hence (4).
Since \( p \in \text{top}_{\text{end}}^{-1}(0^+1) \), the position \( \langle 1, |p| \rangle \) is the only top-row position that carries a 1 for attribute \text{end}, thus (by \( p \in M_5 \)), the value \( |p| \) is the only value for \( k \) that fulfills the right sides of both (2) and (3), thus

\[
|p| = \min \{ k > 1 \mid f(\overline{p}) \mid k \land (f(\overline{p}) + 1) \mid (k - 1) \}.
\]

Thus \( |p| = f(\overline{p})^2 \) and (4). This completes the proof of the only-if-direction.

For the converse direction, let \( p \) be a picture over \( \{0, 1\}^I \) such that \( |p| = f(\overline{p})^2 \) and Equivalences (2)-(4) hold for every \( k \leq |p| \). Equivalences (2) and (4) and \( |p| = f(\overline{p})^2 \) imply \( p \in M_5 \). Equivalence (4) and \( |p| = f(\overline{p})^2 \) imply \( \text{top}(\text{pr}_{\text{end}}(p)) \in \ast \cdot 1 \). From (2) we conclude \( p \in M_1^+ \). From (3) we conclude \( p \in M_3 \). This implies \( p \in M_1^+ \cap M_3 \cap \text{top}_{\text{end}}^{-1}(0^+1) = M_4 \). This completes the proof of the lemma.

The intuition that the top-row positions of a picture correspond to square matrix positions is helpful to understand the next lemma, too. Here, the attributes intuitively mean: The attribute \text{inp} marks those picture positions where the Boolean “input” matrix carries a one. The attribute \text{piv} picks one of those as the “pivot”. The attributes \text{row} (and \text{col}) mark the position on the diagonal that shares the row (or column, respectively) with the pivot position.

**Lemma 3.12** Let \( f : \mathbb{N}_{\geq 1} \rightarrow \mathbb{N}_{\geq 1} \) be a function such that its associated picture language \( L_f \) is \( \Sigma_{1}^{\text{mon}}(\mathcal{F}) \)-definable. There exists a \( \Sigma_{1}^{\text{mon}}(\mathcal{F}) \)-definable picture language \( L_7 \) such that for all pictures \( p \) over alphabet \( \{0, 1\}^{\text{inp}, \text{piv}, \text{row}, \text{col}, \text{end}} \) we have: \( p \in L_7 \) iff \( |p| = f(\overline{p})^2 \) and there are \( i, j \leq f(\overline{p}) \) such that for all \( k \leq |p| \) we have

\[
\begin{align*}
p(1, k)(\text{end}) &= 1 \iff k = f(\overline{p})^2, \quad (6) \\
p(1, k)(\text{piv}) &= 1 \implies p(1, k)(\text{inp}) = 1, \quad (7) \\
p(1, k)(\text{piv}) &= 1 \iff k = \text{code}_f(\overline{p})(i, j), \quad (8) \\
p(1, k)(\text{row}) &= 1 \iff k = \text{code}_f(\overline{p})(i, i), \quad (9) \\
p(1, k)(\text{col}) &= 1 \iff k = \text{code}_f(\overline{p})(j, j). \quad (10)
\end{align*}
\]

**Proof** Recall the definition of \( L_{f+1} \) from Remark 3.10. Choose \( L_0 \) over the alphabet \( \{0, 1\}^{\text{diag}, \text{end}, \text{blk}} \) according to Lemma 3.11. We define the following picture languages over alphabet \( \Gamma = \{0, 1\}^{\text{inp}, \text{piv}, \text{row}, \text{col, end, diag, blk}} \).

\[
\begin{align*}
L_1 &= \text{ex}_{\{\text{inp}, \text{piv}, \text{row}, \text{col}\}}^{-1}(L_0), \\
L_2 &= \text{top}_{\text{piv}}^{-1}(0^*) \cap \text{top}_{\text{piv}}^{-1}(1) \cap \text{top}_{\text{piv}}^{-1}(1) \cap \text{top}_{\text{piv}}^{-1}(0^*), \\
L_3 &= \text{top}_{\text{row}}^{-1}(0^*) \cap \text{top}_{\text{diag}}^{-1}(1) \cap \text{top}_{\text{row}}^{-1}(1) \cap \text{top}_{\text{row}}^{-1}(0^*), \\
L_4 &= \text{top}_{\text{col}}^{-1}(0^*) \cap \text{top}_{\text{diag}}^{-1}(1) \cap \text{top}_{\text{col}}^{-1}(1) \cap \text{top}_{\text{col}}^{-1}(0^*), \\
N_5 &= \text{top}_{\text{piv}}^{-1}(0^* \cup 1^*) \cap \left( \text{top}_{\text{row}}^{-1}(0^*) \cap \text{top}_{\text{piv}}^{-1}(0^* \cup 1^*) \right) \cup \left( \text{top}_{\text{piv}}^{-1}(0^*) \cap \text{top}_{\text{row}}^{-1}(0^* \cup 1^*) \right), \\
L_5 &= \Gamma^\ast \cdot N_5 \cdot \Gamma^\ast, \\
N_6 &= \left( L_f \Gamma^+ \Gamma^+ \right) \cap \left( \text{top}_{\text{col}}^{-1}(0^*) \cap \text{top}_{\text{col}}^{-1}(0^* \cup 1^*) \right) \cup \left( \text{top}_{\text{piv}}^{-1}(0^*) \cap \text{top}_{\text{piv}}^{-1}(0^* \cup 1^*) \right), \\
L_6 &= \Gamma^\ast \cdot N_6 \cdot \Gamma^\ast.
\end{align*}
\]
Finally, we define the following picture language over alphabet \(\{0,1\}^{\text{inp,piv,row,col,end}}\):

\[
L_7 = \text{ex}_{\{\text{diag,blk}\}}(L_1 \cap \ldots \cap L_6).
\]

By Corollary \(\text{3.3}\) Remark \(\text{3.8}\) and Lemma \(\text{3.9}\), \(L_7\) is \(\Sigma_1^{\text{mon}}(\mathcal{F})\)-definable.

For the only-if-direction, let \(p \in L_7\). For abbreviation, set \(n = f(\overline{p})\). Pick picture \(\hat{p}\) over \(\Gamma\) such that \(\hat{p} \in L_1 \cap \ldots \cap L_6\) and \(\text{ex}_{\{\text{diag,blk}\}}(\hat{p}) = p\). We have to show the claim about the size of \(p\) as well as the Implications (6)-(10) for every \(k \leq |p|\).

The choice of \(L_1\) (or rather, of \(L_0\)) implies \(|p| = n^2\) as well as (6).

Implication (7) follows from \(\hat{p} \in L_2\).

Since \(\hat{p} \in L_2\), there exists \(k_{\text{piv}}\) such that

\[
\forall k: p(1,k)(\text{piv}) = 1 \Leftrightarrow k_{\text{piv}} = k.
\]

Choose \(i,j \leq n\) such that \(k_{\text{piv}} = \text{code}_n(i,j)\). This ensures Equivalence (8).

Similarly, since \(\hat{p} \in L_3\), there exist \(k_{\text{row}}\) such that

\[
\forall k: p(1,k)(\text{row}) = 1 \Leftrightarrow k_{\text{row}} = k.
\]

Choose \(i_{\text{row}},j_{\text{row}} \leq n\) such that

\[
k_{\text{row}} = \text{code}_n(i_{\text{row}},j_{\text{row}}).
\]

Since \(\hat{p} \in L_5\), the substring of \(\text{top}(\hat{p})\) demarcated by \(k_{\text{piv}}\) and \(k_{\text{row}}\) is in the same of its \(n\) blocks of length \(n\), thus we have \(i = i_{\text{row}}\). Since \(\hat{p} \in L_3\) and (5), we have \(i_{\text{row}} = j_{\text{row}}\). Thus \(k_{\text{row}} = \text{code}_n(i,i)\), which proves Equivalence (9).

Similarly, since \(\hat{p} \in L_4\), there exist \(k_{\text{col}}\) such that

\[
\forall k: p(1,k)(\text{col}) = 1 \Leftrightarrow k_{\text{col}} = k.
\]

Choose \(i_{\text{col}},j_{\text{col}} \leq n\) such that

\[
k_{\text{col}} = \text{code}_n(i_{\text{col}},j_{\text{col}}).
\]

Since \(\hat{p} \in L_6\), the difference \(|k_{\text{col}} - k_{\text{piv}}|\) is a multiple of \(n\), thus \(j = j_{\text{col}}\). Since \(\hat{p} \in L_4\) and (5), we have \(i_{\text{col}} = j_{\text{col}}\). Thus \(k_{\text{col}} = \text{code}_n(j,j)\), which proves Equivalence (10). This completes the proof of the only-if-direction of this lemma.

For the converse direction, let \(p\) be a picture over alphabet \(\{0,1\}^{\text{inp,piv,row,col,end}}\) such that \(|p| = f(\overline{p})^2\), and let \(i,j \leq f(\overline{p})\) such that for all \(k \leq |p|\) we have Implications (6)-(10).

Again, we set \(n = f(\overline{p})\) for abbreviation. Choose picture \(\hat{p}\) over alphabet \(\Gamma\) such that \(\text{restr}_{\{\text{inp,piv,row,col,end}\}}(\hat{p}) = p\) and Equivalences (2) and (3) from Lemma \(\text{3.11}\) hold for

\[
\text{restr}_{\{\text{diag,end,blk}\}}(\hat{p})
\]

instead of \(p\).

We have to verify that \(\hat{p} \in L_1 \cap \ldots \cap L_6\).

\textbf{Ad L}_1: The picture \(\text{restr}_{\{\text{diag,end,blk}\}}(\hat{p})\) fulfills Lemma \(\text{3.11}\) (2)-(4), so \(\text{restr}_{\{\text{diag,end,blk}\}}(\hat{p}) \in L_0\), thus \(\hat{p} \in \text{restr}^{-1}_{\{\text{diag,end,blk}\}}(L_0) = \text{ex}^{-1}_{\{\text{inp,piv,row,col}\}}(L_0) = L_1\).
3 EXPRESSIBILITY RESULT

\textbf{Ad L2:} Choose a decomposition \( p = qrs \) with \(|q| = \text{code}_n(i, j) - 1\) and \(|r| = 1\). By (8) we have \( 1 = p(1, \text{code}_n(i, j))(\text{piv}) = r(1, 1)(\text{piv}) \). From (7) it follows \( 1 = r(1, 1)(\text{inp}) \). Thus \( r \in \top_{\text{piv}}^{-1}(1) \cap \top_{\text{inp}}^{-1}(1) \). Again by (8), for all \( k < \text{code}_n(i, j) \) we have \( 0 = p(1, k)(\text{piv}) = q(1, k)(\text{piv}) \), thus \( q \in \top_{\text{piv}}^{-1}(0^*) \). Similarly \( s \in \top_{\text{piv}}^{-1}(0^*) \).

We have shown \( p = qrs \in \top_{\text{piv}}^{-1}(0^*) \cap \top_{\text{inp}}^{-1}(1) \cap \top_{\text{inp}}^{-1}(1) \cap \top_{\text{piv}}^{-1}(0^*) = L_2 \).

\textbf{Ad L3:} Similar to L2, but apply (5) instead of (7) and (9) instead of (8).

\textbf{Ad L4:} Similar to L2, but apply (5) instead of (7), and (10) instead of (8).

\textbf{Ad L5:} Choose a decomposition \( p = qrs \) with \(|q| = \min\{\text{code}_n(i, i), \text{code}_n(i, j)\} - 1\) and \(|r| = |\text{code}_n(i, i) - \text{code}_n(i, j)| + 1\). To complete the proof that \( p \in L_5 \), it suffices to show that \( r \in N_5 \).

In case \( i \leq j \), the picture \( r \) is the infix of \( p \) at the columns \( \text{code}_n(i, i), \ldots, \text{code}_n(i, j) \) (inclusively). None of these numbers (except for maybe the last one) is a multiple of \( n \), thus (by (2)) none of the corresponding top-row positions carries a 1 for attribute blk, thus \( r \in \top_{\text{blk}}^{-1}(0^1 \cup 0^*) \). Furthermore, \( r(1, \text{code}_n(i, i))(\text{row}) = 1 \) by (9) and \( r(1, \text{code}_n(i, j))(\text{piv}) = 1 \) by (8), which implies \( r \in \top_{\text{row}}^{-1}(1^*) \cap \top_{\text{piv}}^{-1}(0^*) \). We have shown \( r \in N_5 \).

In case \( i > j \), one similarly shows \( r \in \top_{\text{blk}}^{-1}(0^1 \cup 0^*) \) and \( r \in \top_{\text{piv}}^{-1}(1^*) \cap \top_{\text{row}}^{-1}(0^*) \), which also implies \( r \in N_5 \).

\textbf{Ad L6:} Choose a decomposition \( p = qrs \) with \(|q| = \min\{\text{code}_n(j, j), \text{code}_n(i, j)\} - 1\) and \(|r| = |\text{code}_n(j, j) - \text{code}_n(i, j)| + 1\). To complete the proof that \( p \in L_6 \), it suffices to show that \( r \in N_6 \). We have that \(|\text{code}_n(j, j) - \text{code}_n(i, j)|\) is a multiple of \( n \), thus \(|r| - 1\) is a multiple of \( n = f(\vec{p}) \), hence \( r \in L_f^+ \Gamma^+ \).

In case \( i \leq j \), one shows \( r \in \top_{\text{piv}}^{-1}(1^*) \cap \top_{\text{col}}^{-1}(0^*) \), which implies \( r \in N_6 \).

In case \( i > j \), one shows \( r \in \top_{\text{piv}}^{-1}(1^*) \cap \top_{\text{row}}^{-1}(0^*) \), which also implies \( r \in N_6 \).

We have shown \( p \in L_1 \cap \ldots \cap L_6 \), which completes the proof of the lemma. \hfill \( \square \)

In the next lemma, we consider a concatenations of a sequence of pictures, each of which encodes a Boolean “input” square matrix in its top row. The marker attributes introduced in the preceding lemmas help to calculate one position of their matrix multiplication of these input matrices.

**Lemma 3.13** Consider the alphabet \( \Gamma = \{0, 1\}^{\{\text{inp, end}\}} \). Let \( f : \mathbb{N}_{\geq 1} \rightarrow \mathbb{N}_{\geq 1} \) be a function such that its associated picture language \( L_f \) is \( \Sigma_{\mon}^1(\mathcal{F}) \)-definable. Let \( L \) be the picture language over \( \Gamma \) containing all pictures of the form \( p_1 \ldots p_n \) where \( n \geq 1 \) and \( p_1, \ldots, p_n \) have length \( f(\vec{p})^2 \) and \( \top_{\text{pr}_{\text{end}}(p_h)}(\vec{p}) \in 0^*1 \) (for all \( h \in \{1, \ldots, n\} \)) and \( \prod_{h=1}^n \text{fold}_f(\vec{p}_{\text{inp}}(p_h)) \neq 0 \), where the product refers to standard matrix multiplication over the Boolean semiring. Then \( L \) is \( \Sigma_{\mon}^1(\mathcal{F}) \)-definable.

**Proof** Set \( \Sigma = \{0, 1\}^{\{\text{inp, piv, row, col, end}\}} \). Let \( L_7 \) be the picture language over \( \Sigma \) defined in Lemma 3.12. Let \( \Sigma_{\mon}^{-1} \) denote the set of pictures of length 1 over \( \Sigma \). Consider the following
picture languages over $\Sigma$:

\[ Q = \top_{\text{end}}(0^*1), \]
\[ M = L_7 \Sigma^{+,1} = \{ p \in \Sigma^{+,+} \mid (|p| - 1) \text{ is a multiple of } f(\overline{p}) \}, \]
\[ N = \top_{\text{col}}(\{0,1\}^*) \cap \top_{\text{row}}(\{0,1\}^*1) \cap \top_{\text{end}}(0^*10^+(1 \cup \varepsilon)) \cap M, \]
\[ L_8 = (\Sigma^{*,*}L^{*,*} \cap (QQ)), \]
\[ L_9 = (L_8^*Q \cap L_8^+), \]
\[ L'_9 = (QL_9) \cup Q, \]
\[ L_{10} = (L_7^* \cap L_9 \cap L'_9) \cup L_7. \]

Let $L_{11} = \text{ex}_{\text{piv, row, col}}(L_{10})$. Then $L_{11}$ is $\Sigma_{\text{lmon}}(F)$-definable by Corollary 3.5, Remark 3.8, Lemma 3.9, and Lemma 3.12. We claim that $L_{11} = L$.

First, let $p \in L_{11}$. We will show that $p \in L$. There exists $\hat{p} \in L_{10}$ such that $p = \text{ex}_{\text{piv, row, col}}(\hat{p})$. Since $\hat{p} \in L_7^+$, there exist $n \geq 1$ and $\hat{p}_1, \ldots, \hat{p}_n \in L_7$ such that $\hat{p} = \hat{p}_1 \ldots \hat{p}_n$. Choose pictures $p_1, \ldots, p_n$ over $\Gamma$ such that for every $h \leq n$ we have $p_h = \text{ex}_{\text{piv, row, col}}(\hat{p}_h)$. Then $p = p_1 \ldots p_n$. Since (by (6)) we have $L_7 \subseteq Q$, we obtain $\top(\text{pr}_{\text{end}}(\hat{p}_h)) \in 0^*1$ and thus $\top(\text{pr}_{\text{end}}(p_h)) \in 0^*1$, as required.

As a shorthand, we set $m = \overline{p}$. By Lemma 3.12 we have $|\hat{p}_h| = f(m)^2$ for every $h \leq n$. Choose $i_1, \ldots, i_n, j_1, \ldots, j_n \leq f(m)^2$ according to Lemma 3.12 i.e., such that for every $h \leq n$ and every $k \leq f(m)^2$, we have

\[ \hat{p}_h(1,k)(\text{piv}) = 1 \Rightarrow \hat{p}(1,k)(\text{inp}) = 1, \quad (11) \]
\[ \hat{p}_h(1,k)(\text{piv}) = 1 \Leftrightarrow k = \text{code}_{f(m)}(i_h,j_h), \quad (12) \]
\[ \hat{p}_h(1,k)(\text{row}) = 1 \Leftrightarrow k = \text{code}_{f(m)}(i_h,i_h), \quad (13) \]
\[ \hat{p}_h(1,k)(\text{col}) = 1 \Leftrightarrow k = \text{code}_{f(m)}(j_h,j_h). \quad (14) \]

Furthermore, choose $i_{n+1} = j_n$. We claim that

\[ i_{h+1} = j_h \text{ for every } h \leq n. \quad (15) \]

To see this, let $h \leq n$. If $h = n$, we have $i_{n+1} = j_h$ by choice of $i_{n+1}$. So we may assume $h < n$ and $n \geq 1$. We note that $\hat{p}_h \hat{p}_{h+1} \in \Sigma^{*,*}N\Sigma^{*,*}$. (If $h$ is odd, this follows from $\hat{p} \in L_9$; if $h$ is even, this follows from $\hat{p} \in L_9$.) This means that $\hat{p}_h \hat{p}_{h+1}$ has an infix $r \in N$. Let $l, l' \leq 2f(m)^2$ be the start and end positions of that infix $r$ in $\hat{p}_h \hat{p}_{h+1}$. Since $\hat{p}_h, \hat{p}_{h+1} \in L_7$, we have $|\hat{p}_h| = |\hat{p}_{h+1}| = f(m)^2$. Since $\hat{p}_h, \hat{p}_{h+1} \in Q$, the only two top row positions of $\hat{p}_h \hat{p}_{h+1}$ carrying a 1 for attribute end are the rightmost positions of $\hat{p}_h$ and of $\hat{p}_{h+1}$. Since $r \in \top_{\text{end}}^{-1}(0^*10^+(1 \cup \varepsilon))$, the infix $r$ overlaps the center of $\hat{p}_h \hat{p}_{h+1}$, i.e., $l \leq f(m)^2$ and $l' > f(m)^2$. Since $r \in N$, we have

\[ 1 = r(1,1)(\text{col}) = (\hat{p}_h \hat{p}_{h+1})(1,l)(\text{col}) = \hat{p}_h(1,l)(\text{col}) \quad (16) \]
\[ 1 = r(1,|r|)(\text{row}) = (\hat{p}_h \hat{p}_{h+1})(1,l')(\text{row}) = \hat{p}_{h+1}(1,l' - f(m)^2)(\text{row}) \quad (17) \]

By (14) and (16), we have

\[ l = \text{code}_{f(m)}(j_h,j_h) = (j_h - 1)f(m)^2 + j_h. \quad (18) \]
By (13) and (17), we have
\[ l' - f(m)^2 = \text{code}_{f(m)}(i_{h+1}, i_{h+1}) = (i_{h+1} - 1)f(m)^2 + i_{h+1}. \] (19)

Since \( r \in M \) we have
\[ f(m) \mid l' - l = i_{h+1}f(m)^2 + i_{h+1} - (j_{h} - 1)f(m)^2 - j_{h}. \] (20)

We may conclude from (20) that \( f(m) \mid i_{h+1} - j_{h} \) and hence \( i_{h+1} = j_{h} \). This completes the proof of (15).

For every \( h \in \{1, \ldots, n\} \), choose \( A_h = \text{fold}_n(\text{pr}_{\text{imp}}(\hat{p}_h)) \).

Let \( h \leq n \). By (12), we have \( \hat{p}_h(1, \text{code}_{f(m)}(i_{h}, j_{h}))(\text{piv}) = 1 \). Thus \( A_h(i_{h}, i_{h+1}) = A_h(i_{h}, j_{h}) = \hat{p}_h(1, \text{code}_{f(m)}(i_{h}, j_{h}))(\text{inp}) = 1 \). (For the last equality, see (11).) By Lemma 3.14 this implies \( \prod_{h=1}^{n} A_h \neq 0 \) and hence \( p = \text{ex}_{\{\text{piv}, \text{row}, \text{col}\}}(\hat{p}) \in L \). This completes the proof of \( L_{11} \subseteq L \).

For the converse direction, let \( p \in L \). Again, set \( m = \overrightarrow{p} \). Choose \( n \geq 1 \) and pictures \( p_1, \ldots, p_n \) of length \( f(m)^2 \) over \( \Gamma \) such that \( p = p_1 \ldots p_n \) and \( \text{top}(\text{pr}_{\text{end}}(p_h)) \in \mathcal{O}^1 \) (for all \( h \in \{1, \ldots, n\} \)) and \( \prod_{h=1}^{n} \text{fold}_{f(m)}(\text{pr}_{\text{imp}}(p_h)) \neq 0 \).

We claim that there exists a picture \( \hat{p} \in \Sigma^{+, * +} \) with \( \text{ex}_{\{\text{piv}, \text{row}, \text{col}\}}(\hat{p}) = p \) and \( \hat{p} \in L_{10} \). By Lemma 3.14 there exist \( i_1, \ldots, i_n \leq f(m) \) such that \( \text{fold}_{m}(\text{pr}_{\text{imp}}(p_h))(i_{h}, i_{h+1}) = 1 \) for every \( h < n \). For every \( h \leq n \), choose \( \hat{p}_h \) as follows:

\[
\begin{align*}
\text{restr}_{\{\text{inp}, \text{end}\}}(\hat{p}_h) &= p_h, \\
\hat{p}_h(1, k')(\text{piv}) = 1 &\iff k = \text{code}_{f(m)}(i_{h}, i_{h+1}), \\
\hat{p}_h(1, k')(\text{row}) = 1 &\iff k = \text{code}_{f(m)}(i_{h}, i_{h}), \\
\hat{p}_h(1, k')(\text{col}) = 1 &\iff k = \text{code}_{f(m)}(i_{h+1}, i_{h+1}).
\end{align*}
\]

(The letters of \( \hat{p}_h \) at positions \( \langle i, k \rangle \) with \( i \neq 1 \) are irrelevant and may be set arbitrarily.)

It is straightforward to check that \( \hat{p}_h \in L_7 \) for every \( h \leq n \). We set \( \hat{p} = \hat{p}_1 \ldots \hat{p}_n \). We have \( \hat{p} \in L_{10} \).

If \( n = 1 \), we have \( \hat{p} \in L_7 \subseteq L_{10} \). Thus for completing the proof that \( \hat{p} \in L_{10} \), we may assume \( n \geq 2 \) and show that \( \hat{p} \in L_9 \cap L_{10}' \).

By definition of \( Q \) and \( L_{10} \), for showing \( \hat{p} \in L_{10} \) it suffices to show
\[ \hat{p}_h \hat{p}_{h+1} \in \Sigma^{*, * +} \Sigma^{*, * +} \] (21)
for every odd \( h < n \), whereas for \( \hat{p} \in L_{10}' \) it suffices to show (21) for every even \( h < n \). So for completing the proof that \( \hat{p} \in L_{10} \) it suffices to show (21) for every \( h < n \).

Let \( h < n \). Let \( l = \text{code}_{f(m)}(i_{h+1}, i_{h+1}) \) and \( l' = f(m)^2 + l \). Then the infix of \( \hat{p}_h \hat{p}_{h+1} \) from column \( l \) to \( l' \) (inclusively) is indeed in \( N \). This completes the proof that \( \hat{p} \in L_{10} \) and thus the proof of the lemma.

\[ \square \]

**Definition 3.14 (Monoid of binary relations)** Let \( n \geq 1 \). The monoid \( B_n \) is the set of binary relations over \( \{1, \ldots, n\} \) together with the usual relation product.
This monoid of binary relations has been studied extensively. We will use it in the lower bound proof (see Section 4). Besides, we use it to state the next lemma a little more generally than needed.

**Lemma 3.15** Consider the alphabet $\Gamma = \{0, 1\}^{\text{inp,end}}$. Let $f : \mathbb{N}_{\geq 1} \to \mathbb{N}_{\geq 1}$ be a function such that its associated picture language $L_f$ is $\Sigma_{1}^{\text{mon}}(\mathcal{F})$-definable. There is a $\Sigma_{1}^{\text{mon}}(\mathcal{F})$-definable picture language $L$ over $\Gamma$ such that for every $m \geq 1$ the syntactic monoid of $L[m]$ contains a submonoid isomorphic to $B_{f(m)}$.

**Proof** Let $L$ be defined according to Lemma 3.13. Then $L$ is indeed $\Sigma_{1}^{\text{mon}}(\mathcal{F})$-definable. Let $m \geq 1$. Set $n = f(m)$. We claim that the syntactic monoid $M(L[m])$ of the height-$m$ fragment of $L$ contains a submonoid isomorphic to $B_{n}$. If $n = 1$, this is trivial, so we may assume $n \geq 2$.

For a relation $\pi \in B_{n}$, its characteristic matrix is the $n \times n$-matrix $A_{\pi}$ defined by

$$A_{\pi}(i, j) = \begin{cases} 1 & \text{if } (i, j) \in \pi, \\ 0 & \text{else.} \end{cases}$$

For a relation $\pi \in B_{n}$, we define $p_{\pi}$ as the picture of size $(m, n^2)$ over $\Gamma$ such that the top row of $p_{\pi}$ is defined as follows: $\text{top}(\text{pr}_{\text{end}}(p_{\pi})) = 0^*1$ and $\text{fold}_{n}(\text{pr}_{\text{inp}}(p_{\pi})) = A_{\pi}$. The letters of $p_{\pi}$ at positions $(i, j)$ with $i \neq 1$ are irrelevant and may be chosen arbitrarily.

For a non-empty picture $p$ of height $m$, let $[p]$ denote its congruence class wrt. the syntactic congruence of $L[m]$. We claim that the mapping $\varphi : \pi \mapsto [p_{\pi}]$ is an injective homomorphism from $B_{n}$ into the syntactic semigroup of $L[m]$.

First we show that $\varphi$ is a homomorphism. For this aim, we have to show that for every $\pi, \tau \in B_{n}$, the pictures $p_{\pi\tau}$ and $p_{\pi}p_{\tau}$ are syntactically congruent wrt. $L[m]$. So let $\pi, \tau \in B_{n}$. Let $q, r \in \Gamma^{m,*}$. We will show that

$$qp_{\pi\tau}r \in L \iff qp_{\pi}p_{\tau}r \in L$$

Assume $qp_{\pi\tau}r \in L$. Each picture of $L$ is a column concatenation of one or more blocks of size $(m, n^2)$, each of which is in $\text{top}_{\text{end}}^{-1}(0^*1)$, i.e., demarcated by a 1 for attribute $\text{end}$ in its upper right corner. Since $qp_{\pi\tau}r \in L$ and $p_{\pi\tau}$ is one of these blocks, the pictures $q$ and $r$ are assembled by zero or more of these blocks. In other words, there are $s, s' \geq 0$ and pictures $q_{1}, \ldots, q_{s}, r_{1}, \ldots, r_{s'}$ of size $(m, n^2)$ such that

$$q = q_{1} \ldots q_{s} \quad \text{and} \quad r = r_{1} \ldots r_{s'}.$$ 

Let $\cdot$ denote standard matrix multiplication over the Boolean semiring. Choose

$$B = \text{fold}_{n}(\text{pr}_{\text{inp}}(q_{1})) \ldots \text{fold}_{n}(\text{pr}_{\text{inp}}(q_{s})),
C = \text{fold}_{n}(\text{pr}_{\text{inp}}(r_{1})) \ldots \text{fold}_{n}(\text{pr}_{\text{inp}}(r_{s'})).$$

Since $qp_{\pi\tau}r \in L$ and by

$$\text{fold}_{n}(\text{pr}_{\text{inp}}(p_{\pi\tau})) = A_{\pi\tau} = A_{\pi} \cdot A_{\tau} = \text{fold}_{n}(\text{pr}_{\text{inp}}(p_{\pi})) \cdot \text{fold}_{n}(\text{pr}_{\text{inp}}(p_{\tau})),$$
we have
\[ 0 \neq B \cdot \text{fold}_n(\text{pr}_{\text{inp}}(p_{\pi \tau})) \cdot C = B \cdot \text{fold}_n(\text{pr}_{\text{inp}}(p_{\tau})) \cdot \text{fold}_n(\text{pr}_{\text{inp}}(p_{\pi})) \cdot C, \]
which implies \( q_{p_{\pi}} r \in L \). This completes the proof of the direction “\( \Rightarrow \)” of (22). The other direction is similar. This completes the proof that \( \varphi \) is a homomorphism, so it remains to show that \( \varphi \) is injective.

For every \( a, b \in \{1, \ldots, n\} \) we define the square matrix \( C_{a,b} \in \{0,1\}^{n \times n} \) by
\[ C_{a,b}(i,j) = 1 \iff (i,j) = (a,b). \]
Recall that \( n \geq 2 \). Then for every \( \pi \in B_n \) we have
\[ \{(1,b)\}_\pi \{(a,2)\} = \begin{cases} \{(1,2)\} & \text{if } (b,a) \in \pi, \\ \emptyset & \text{otherwise}, \end{cases} \]

hence for the characteristic matrix \( A_\pi \) we have
\[ C_{1,b} \cdot A_\pi \cdot C_{a,2} = \begin{cases} C_{1,2} & \text{if } (b,a) \in \pi, \\ 0 & \text{otherwise}, \end{cases} \quad (23) \]
where \( 0 \) denotes the zero matrix of size \( n \times n \).

Now let \( \pi, \pi' \in B_n \) such that \([p_{\pi}] = [p_{\pi'}]\). Then
\[ \forall q, r \in \Gamma^{m,+} : q_{p_{\pi}} r \in L[m] \iff q_{p_{\pi'}} r \in L[m]. \]
This implies (for \( q, r \) with \( C_{1,b} = \text{fold}_n(\text{pr}_{\text{inp}}(q)) \) and \( C_{a,2} = \text{fold}_n(\text{pr}_{\text{inp}}(r)) \)):
\[ \forall a, b \in \{1, \ldots, n\} : C_{1,b} \cdot A_\pi \cdot C_{a,2} \neq 0 \iff C_{1,b} \cdot A_{\pi'} \cdot C_{a,2} \neq 0, \]
which by (23) implies
\[ \forall a, b \in \{1, \ldots, n\} : (b,a) \notin \pi \iff (b,a) \notin \pi'. \]
This implies \( \pi = \pi' \). We have shown that \( \varphi \) is injective, which completes the proof.

We need the following result:

**Theorem 3.16** ([Sch97, Mat99]) Let \( k \geq 1 \). There is a \( k \)-fold exponential function \( f \) such that \( L_f \) (over a singleton alphabet) is \( \Sigma^\text{mon}_1(\Pi^{k-1}_0(\Delta^\text{mon}_1)) \)-definable.

The formula construction for the above proof is in [Sch97], except for the observation that the inner quantifier block may be chosen as universal as well as as existential. For a construction including this observation, see [Mat99], Theorem 2.29.

**Lemma 3.17** Let \( k \geq 1 \). There is a \( k \)-fold exponential function \( f \) and a \( \Sigma^\text{mon}_1(\Pi^{k-1}_0(\Delta^\text{mon}_1)) \)-definable picture language \( L \) over alphabet \( \{0,1\}^{\text{inp,end}} \) such that for every \( m \geq 1 \), the syntactic monoid of \( L[m] \) contains a submonoid isomorphic to \( B_{f(m)} \).
**Proof** By the preceding theorem, there is a $k$-fold exponential function $f$ such that $L_f$ is definable in the specified formula class. The class of picture languages definable in $\Pi^0_k \Delta^0_1$ is closed under column concatenation and column closure by Proposition 3.4. The claim follows from Lemma 3.15. □

For the following theorem from [Rho74a] see also the remarks in [RS09], page 307.

**Theorem 3.18** ([Rho74a]) $c(B_n) = n - 1$ for every $n \geq 1$.

Lemma 3.17 and Theorem 3.18 imply

**Theorem 3.19** For every $k \geq 1$, the class of $\Sigma^1_{\text{mon}}(\Pi^0_k \Delta^0_1)$-definable picture languages over $\{0, 1\}^\{\text{inp,end}\}$ is at least $k$-fold exponential wrt. group complexity.

This is the upper bound part of Theorem 2.10 and the result of this section.

## 4 Non-Expressibility Result

### 4.1 Some More Notation

In this section, we write a (monoid or semigroup) homomorphism to the right of its argument. Consequently, if $\eta : M \to N$ is a homomorphism, the image of $M$ under $\eta$ is denoted $M\eta$, and the pre-image of a subset $X$ of $N$ is denoted $X\eta^{-1}$. If $\pi : N \to T$ is another homomorphism, then $\eta\pi$ denotes the composition of $\eta$ and $\pi$.

We recall some notions in addition to those in Section 2.6. Let $L$ be a word language over $\Gamma$. If $M$ is a monoid and $\eta : \Gamma^* \to M$ is a homomorphism such that there exists a subset $X \subseteq M$ with $L = X\eta^{-1}$, then we say that $M$ and $\eta$ recognize $L$. We are only interested in the case that $M$ is finite.

The syntactic homomorphism $\eta_L : \Gamma^* \to M(L)$ maps every word to its syntactic congruence class. $M(L)$ and $\eta_L$ recognize $L$. Besides, if $\eta$ is a homomorphism that recognizes $L$, then $\eta_L$ factors through $\eta$, meaning that there exists a homomorphism $\theta : \Gamma^*\eta \to M(L)$ such that $\eta\theta = \eta_L$.

### 4.2 Transition Monoid of an NFA

Let $L$ be recognized by a non-deterministic finite automaton (NFA) $\mathfrak{A}$ with $c$ states. Using the transition structure of $L$, one can construct the transition monoid $M_{\mathfrak{A}}$ of $\mathfrak{A}$, which is a monoid with $2^{c^2}$ elements that recognizes $L$. We sketch this construction from [Pin96]. Let $Q$ be the state set of $\mathfrak{A}$ and let $\Gamma$ be its alphabet. Let $M_{\mathfrak{A}} = \{0, 1\}^{Q \times Q}$. $M_{\mathfrak{A}}$ forms a monoid, with the multiplication given as follows: for all $q, q'' \in Q$ we set

$$(A \cdot B)(q, q'') = \sum_{q' \in Q} A(q, q') \cdot B(q', q''),$$
where sum and product on the right refer to the Boolean semiring. To every letter $a \in \Gamma$, we assign the element $\delta_a \in M_A$ such that for every $q, q' \in Q$ we have $\delta_a(q, q') = 1$ iff there is a transition from $q$ to $q'$ labeled $a$.

The mapping $\delta : a \mapsto \delta_a$ induces a monoid homomorphism $\Gamma^* \to M_A$. Then $L$ is the pre-image of $\{(i, f) \in Q \times Q \mid i \text{ is initial and } f \text{ is final}\}$ under $\delta$, thus $M_A$ and $\delta$ recognize $L$.

### 4.3 A Semantic Equivalent to First-Order Quantification

In this section, let $I$ be an attribute set, $K \subseteq I$, and $\Gamma = \{0, 1\}^I$. Recall from Remark 2.2 how the alphabet projection $\text{ex}_{\{\mu\}}$ corresponds to the set quantification over variable $X_\mu$. Similarly, the syntactic concepts of disjunction and negation correspond to union and complementation wrt. $\text{Unique}_{I, K}$, respectively, in the sense that

$$
\begin{align*}
\text{Mod}_{I, K}(\varphi \lor \psi) &= \text{Mod}_{I, K}(\varphi) \cup \text{Mod}_{I, K}(\psi), \\
\text{Mod}_{I, K}(\neg \varphi) &= \text{Unique}_{I, K} \setminus \text{Mod}_{I, K}(\varphi).
\end{align*}
$$

The next definition and remark present an operation on picture languages that similarly corresponds to the effect of first-order quantification.

**Definition 4.1** Let $\mu \in I$. Let $L$ be a picture language over alphabet $\{0, 1\}^I$. Then $\text{exfo}_\mu(L)$ denotes the set of non-empty pictures $p$ over alphabet $\{0, 1\}^I \setminus \{\mu\}$ for which there exists a picture $p' \in \text{Unique}_{I, \{\mu\}} \cap L$ such that $p = \text{ex}_{\{\mu\}}(p')$.

**Remark 4.2** Let $\mu \in K$, let $\varphi$ be a formula, and let $x_\mu$ be a first-order variable.

$$
\text{Mod}_{I, K \setminus \{\mu\}}(\exists x_\mu \varphi) = \text{exfo}_\mu(\text{Mod}_{I, K}(\varphi)).
$$

### 4.4 The Block Product

The *block product* has been introduced in [RT89]. That block product captures the effect of first-order quantification on the syntactic monoid in the sense of Lemma 4.3 below. Following the presentation of [Str94], pp. 61-65, we prepare the definition of the block product by introducing bilateral semidirect products.

Let $S, T$ be finite monoids, and let us write $S$ additively. Assume a given left action as in Definition 2.8. The action is monoidal if it additionally satisfies:

- $1s = s$ for every $s \in S$,
- $0t = 0$ for every $t \in T$.

*Monoidal right actions* are defined dually. A left and a right action of $T$ on $S$ are compatible if $(ts)t' = t(st')$ for every $t, t' \in T$ and every $s \in S$.

Given a pair of compatible actions of $S$ on $T$, we define the *bilateral semidirect product* $S \bowtie T$. This is the set $S \times T$ with multiplication given by

$$(s, t)(s', t') = (st' + ts', tt').$$
If $M$ and $N$ are monoids and the underlying left and right actions are monoidal, then the bilateral semidirect product $M ** N$ is indeed a monoid, see \cite{Str94}, Proposition V.4.1. We remark that by \cite{Str94}, Example V.4.b, the semidirect product from Section 2.7 is a special case of the bilateral semidirect product with the right action defined by $st = s$.

Closely following \cite{Str94}, we can now define the block product. Let $M, N$ be monoids, but this time we will write the products in both of these monoids multiplicatively. The set $M^{N \times N}$ of all maps from $N \times N$ into $M$ forms a monoid under the component-wise product, which we write additively. That is, for $F_1, F_2 : N \times N \to M$ we define $F = F_1 + F_2$, where $F(n_1, n_2) = F_1(n_1, n_2) \cdot F_2(n_1, n_2)$ for all $n_1, n_2 \in N$. Thus $M^{N \times N}$ is isomorphic to the direct product of $|N|^2$ copies of $M$. The identity of this monoid is the map that sends every element of $N \times N$ to 1. We define left and right actions of $N$ on $M^{N \times N}$ by

\[
(nF)(n_1, n_2) = F(n_1n, n_2), \quad (Fn)(n_1, n_2) = F(n_1, nn_2).
\]

It is straightforward to verify that these equations define a pair of compatible left and right actions. The resulting bilateral semidirect product if called the block product of $M$ and $N$ and is denoted $M \square N$.

Recall that, for a word language $L$, we denote its syntactic monoid by $M(L)$.

The following lemma is an adaption of \cite{Str94}, Lemma VI.1.2.

**Lemma 4.3** Let $I$ be an attribute set, $\Gamma = \{0, 1\}^I$, $\mu \in I$, $L \subseteq \Gamma^{+, +}$, $m \geq 1$. Then $U_1 \square M(L[m])$ recognizes $\text{exfo}_\mu(L)[m]$. More precisely, set $J = I \setminus \{\mu\}$ and $\Sigma = \{0, 1\}^J$.

Consider the syntactic homomorphisms

\[
\eta_{L[m]} : \Gamma^{m,*} \to M(L[m]), \quad \eta_{\text{exfo}_\mu(L)[m]} : \Sigma^{m,*} \to M(\text{exfo}_\mu(L)[m]),
\]

of $L[m]$ and $\text{exfo}_\mu(L)[m]$, respectively.

Let $\pi : U_1 \square M(L[m]) \to M(L[m])$, $(F, n) \mapsto n$ be the projection homomorphism, and let $\sigma : \Sigma \to \Gamma$ be the alphabet mapping that maps every $a \in \Sigma$ to the letter $\overline{a}$ with $\overline{\overline{a}} = J = a$ and $\overline{a}(\mu) = 0$. We extend $\sigma$ to a homomorphism $\Sigma^{m,*} \to \Gamma^{m,*}$ as usual.

There exist homomorphisms $\zeta : \Sigma^{m,*} \sigma \to U_1 \square M(L[m])$ and $\tau : U_1 \square M(L[m]) \to M(\text{exfo}_\mu(L)[m])$ such that $\zeta \sigma = \eta_{L[m]} \vert (\Sigma^m \sigma)^*$ and $\sigma \zeta \tau = \eta_{\text{exfo}_\mu(L)[m]}$.

**Proof** We define the mapping $\otimes : \Sigma \times \{0, 1\} \to \Gamma$ the following way:

\[
(a \otimes b)(\nu) = \begin{cases} 
  a(\nu) & \text{if } \nu \neq \mu, \\
  b & \text{if } \nu = \mu.
\end{cases}
\]

(Then $\overline{a} = a \otimes 0$ for every $a \in \Sigma$.) If $p \in \Sigma^{+, +}$ and $q \in \{0, 1\}^{+, +}$ are pictures of the same size, we write $p \otimes q$ for the equally sized picture over $\Gamma$ with $(p \otimes q)(i, j) = p(i, j) \otimes q(i, j)$ for every $(i, j) \in \text{dom}(p)$.
Choose $T \subseteq M(L[m])$ such that $L[m] = T \eta_{L[m]}^{-1}$. Define

$$\zeta : \Sigma^m \sigma \rightarrow U_1 \Box M(L[m]), \quad \left( \begin{array}{c} a_1 \\ \vdots \\ a_m \end{array} \right) \mapsto \left( \begin{array}{c} F, \\ F, \end{array} \right) \eta_{L[m]} \right),$$

where $F$ is defined as follows: for all $n_1, n_2 \in M(L[m])$, the component $F(n_1, n_2) \in \{0, 1\}$ is 0 iff there exist $b_1, \ldots, b_m \in \{0, 1\}$ such that $b_1 \ldots b_m \in 0^*10^*$ and

$$n_1 \cdot \left( \begin{array}{c} a_1 \otimes b_1 \\ \vdots \\ a_m \otimes b_m \end{array} \right) \eta_{L[m]} \cdot n_2 \in T.$$

We extend $\zeta$ to a monoid homomorphism $(\Sigma^m \sigma)^* \rightarrow U_1 \Box M(L[m])$ as usual. Then indeed $\zeta \pi = \eta_{L[m]} \downarrow (\Sigma^m \sigma)^*$, as claimed in the lemma.

Let $\theta = \sigma \zeta$. Then $\theta$ is a homomorphism $\Sigma^m \star \rightarrow U_1 \Box M(L[m])$. Choose

$$K := \{ G \in \{0, 1\}^{M(L[m]) \times M(L[m])} \mid G(1, 1) = 0 \} \times M(L[m]) \subseteq U_1 \Box M(L[m]).$$

We show that $\text{exfo}_\mu(L)[m] = K \theta^{-1}$.

Let $p \in \Gamma^+ \pm$ be a picture of size $(m, n)$, say $p = \left( \begin{array}{c} a_{1,1} \cdots a_{1,n} \\ \vdots \\ a_{m,1} \cdots a_{m,n} \end{array} \right)$. Then there are appropriate $F_1, \ldots, F_n \in \{0, 1\}^{M(L[m]) \times M(L[m])}$ such that

$$\left( \begin{array}{c} a_{1,l} \\ \vdots \\ a_{m,l} \end{array} \right) \theta = \left( \begin{array}{c} a_{1,l} \\ \vdots \\ a_{m,l} \end{array} \right) \zeta = \left( \begin{array}{c} F_1, \\ F_1, \end{array} \right) \eta_{L[m]} \right),$$

for every $l \leq n$. We have

$$p \theta = \left( F_1, \left( \begin{array}{c} a_{1,1} \\ \vdots \\ a_{m,1} \end{array} \right) \eta_{L[m]} \right) \cdots \left( F_n, \left( \begin{array}{c} a_{1,n} \\ \vdots \\ a_{m,n} \end{array} \right) \eta_{L[m]} \right).$$
By induction over \( n \) one shows that there exists \( G \in \{0, 1\}^{M(L[m]) \times M(L[m])} \) such that

\[
p\theta = \left( G, \left( \begin{array}{c}
\bar{a}_{1,1} \\
\vdots \\
\bar{a}_{m,1} \\
\vdots \\
\bar{a}_{1,n} \\
\vdots \\
\bar{a}_{m,n}
\end{array} \right) \right) \eta_{L[m]}.
\]

with

\[
G(1, 1) = \prod_{l=1}^{n} F_l \left( \left( \begin{array}{c}
\bar{a}_{1,1} \\
\vdots \\
\bar{a}_{m,1} \\
\vdots \\
\bar{a}_{1,l-1} \\
\vdots \\
\bar{a}_{m,l-1}
\end{array} \right) \eta_{L[m]}, \left( \begin{array}{c}
\bar{a}_{1,l} \\
\vdots \\
\bar{a}_{m,l}
\end{array} \right) \eta_{L[m]} \right).
\]

Thus we have the following equivalence chain:

\[
p\theta \in K \iff G(1, 1) = 0 \iff \text{there is } l \leq n \text{ such that } 0 = F_l \left( \left( \begin{array}{c}
\bar{a}_{1,1} \\
\vdots \\
\bar{a}_{m,1} \\
\vdots \\
\bar{a}_{1,l-1} \\
\vdots \\
\bar{a}_{m,l-1}
\end{array} \right) \eta_{L[m]}, \left( \begin{array}{c}
\bar{a}_{1,l} \\
\vdots \\
\bar{a}_{m,l}
\end{array} \right) \eta_{L[m]} \right)
\]

iff there is \( l \leq n \) and \( b_1, \ldots, b_m \in \{0, 1\} \) such that \( b_1 \ldots b_m \in 0^*10^* \) and

\[
\left( \begin{array}{c}
\bar{a}_{1,1} \\
\vdots \\
\bar{a}_{m,1} \\
\vdots \\
\bar{a}_{1,l-1} \\
\vdots \\
\bar{a}_{m,l-1}
\end{array} \right) \eta_{L[m]} \cdot \left( a_{1,l} \otimes b_1 \\
\vdots \\
\vdots \\
a_{m,1} \otimes b_m \right) \eta_{L[m]} \cdot \left( \begin{array}{c}
\bar{a}_{1,l+1} \\
\vdots \\
\bar{a}_{m,l+1} \\
\vdots \\
\bar{a}_{1,n} \\
\vdots \\
\bar{a}_{m,n}
\end{array} \right) \eta_{L[m]} \in T
\]

iff there exists a picture \( q \) of size \((m, n)\) over \( \{0, 1\} \) such there is exactly one position \((k, l) \in \text{dom}(q)\) with \( q(k, l) = 1 \) and

\[
\left( \begin{array}{c}
\bar{a}_{1,1} \\
\vdots \\
\bar{a}_{m,1} \\
\vdots \\
\bar{a}_{1,n} \\
\vdots \\
\bar{a}_{m,n}
\end{array} \otimes q \right) \eta_{L[m]} \in T
\]

iff there exists \( q \in \text{Unique}_{\{\mu\}, \{\mu\}} \) of size \((m, n)\) such that

\[
p \otimes q \in T \eta_{L[m]}^{-1} = L
\]

iff \( p \in \text{exfo}_\mu(L)[m] \).

Since \( p \) was chosen arbitrary, this implies \( K \theta^{-1} = \text{exfo}_\mu(L)[m] \). Thus \( U_1 \square M(L[m]) \) and \( \theta \) recognize \( \text{exfo}_\mu(L)[m] \).

Since the syntactic homomorphism factors through any other homomorphism that recognizes the same language, there exists a homomorphism \( \tau \) such that \( \eta_{\text{exfo}_\mu(L)[m]} = \theta \tau = \sigma \zeta \tau \).

This completes the proof. \( \square \)

The above lemma and its proof closely follow [Str94, Lemma VI.1.2]. Straubing’s lemma is obtained from ours by choosing \( m = 1 \). Besides, [Str94] does not introduce the operator \( \text{exfo}_\mu \) from Definition 4.1, so it must be applied to a formula \( \varphi \) rather than to its language \( L = \text{Mod}(\varphi) \). In [Str94], that formula is from the first-order theory with order, but that condition is of no concern, as the syntax of that formula is irrelevant for the proof.


4.5 Using the Group Complexity

In this section, we finish the proof of Theorem 2.10. A semigroup that does not contain a non-trivial group is called aperiodic. A semigroup homomorphism \( \varphi : S \to T \) is called aperiodic if for every aperiodic subsemigroup \( W \) of \( T \), its pre-image \( W \varphi^{-1} \) is aperiodic. Recall the definition of group complexity from Section 2.7. The following theorem is from [Rho74b], see e.g. [RS09], Theorem 4.9.1.

**Theorem 4.4 (Fundamental Lemma of Complexity)** Let \( S, T \) be semigroups. Let \( \varphi : S \to T \) be a surjective aperiodic homomorphism. Then \( c(S) = c(T) \).

The observation of the next lemma has probably been made before, but I did not find an explicit statement of it in the literature, so we prove it here. A similar statement (concerning the Malcev product) can be found in [RS09], Corollary 4.9.4.

**Lemma 4.5** Let \( S, T \) be semigroups such that \( S \) is aperiodic. Then \( c(S**T) = c(T) \).

**Proof** We write \( S \) additively and write \( ns = s + \cdots + s \) to denote, for \( n \geq 0 \) and \( s \in S \), the \( n \)-fold sum of \( s \). By Theorem 4.4 it suffices to show that the projection homomorphism \( \pi : S**T \to T \), \( (s,t) \mapsto t \) is aperiodic.

Let \( W \) be an aperiodic subsemigroup of \( T \). Let \( G \) be a cyclic group contained in \( W \pi^{-1} \). It suffices to show that \( G \) is trivial.

Choose \( g \in G \) such that \( G \) is generated by \( g \), i.e., \( G = \{g, g^2, \ldots, g^{|G|}\} \). Choose \( s \in S \) and \( t \in T \) such that \( g = (s,t) \). We have \( \{t, t^2, \ldots, t^{|G|}\} = G \pi \) is a group contained in \( W \), thus it is trivial, which implies \( t = t^2 \). Simple induction shows that for every \( n \geq 0 \) it holds

\[
(s,t)^{n+2} = \left(st + n(tst) + ts, t\right).
\]

Since \( S \) is aperiodic, there exists \( n \geq 1 \) such that \( n(tst) = (n+1)(tst) \). Now \( (s,t)^{n+2} = (st + n(tst) + ts, t) = (st + (n+1)(tst) + ts, t) = (s,t)^{n+3} \). Since \( (s,t) \) generates the group \( G \), this implies that \( (s,t) \) is the identity of \( G \), so \( G \) is trivial, which completes the proof. \( \square \)

**Remark 4.6** Let \( L \) be a word language. Let \( M \) be a monoid that recognizes \( L \). Then \( c(M(L)) \leq c(M) \).

**Proof** Set \( n = c(M) \). Since \( M \) recognizes \( L \), the syntactic monoid of \( L \) is a homomorphic image of \( M \) and hence \( M(L) \preceq M \). Since \( M \in C_n \) and \( C_n \) is a pseudovariety, this implies \( M(L) \in C_n \), thus \( c(M(L)) \leq n = c(M) \). \( \square \)

**Lemma 4.7** Let \( I \) be an attribute set, let \( \mu \in I \) be an attribute, let \( L \) be a set of pictures over alphabet \( \{0, 1\}^I \), let \( m \geq 1 \). Then \( c(M(\text{exfo}_\mu(L)[m])) \leq c(M(L[m])) \).
4 NON-EXPRESSIBILITY RESULT

**Proof** By Lemma 4.3, the monoid $U_1 \square M(L[m])$ recognizes $\text{exfo}_\mu(L)[m]$. By Remark 4.6,

$$c(M(\text{exfo}_\mu(L)[m])) \leq c(U_1 \square M(L[m])) = c(U_1^{M(L[m]) \times M(L[m])} \ast M(L[m])).$$

Since $U_1$ is aperiodic, so is $U_1^{M(L[m]) \times M(L[m])}$. Thus the claim follows by Lemma 4.5. □

Now we show that the group complexity is not increased by existential first-order quantification, disjunction, and negation. More precisely:

**Proposition 4.8** Let $m \geq 1$. For every formula $\varphi$, we set $M(\varphi) = M(\text{Mod}_{I,K}(\varphi)[m])$ for abbreviation, where the attribute sets $I$, $K$ are understood as containing the indices of all free variables (or all free first-order variables, respectively) of $\varphi$.

Let $\varphi, \psi$ be formulas. Then

1. $c(M(\exists x\varphi)) \leq c(M(\varphi))$, \hfill (24)
2. $c(M(\varphi \lor \psi)) \leq \max\{c(M(\varphi)), c(M(\psi))\}$, \hfill (25)
3. $c(M(\neg \varphi)) = c(M(\varphi))$. \hfill (26)

**Proof** Ad (24): This is an immediate consequence of Lemma 4.7 and Remark 4.2.

Ad (25): Let $n = \max\{c(M(\varphi)), c(M(\psi))\}$. Then $M(\varphi), M(\psi) \in C_n$. The direct product $M(\varphi) \times M(\psi)$ recognizes the word language $\text{Mod}(\varphi \lor \psi)[m]$, thus $M(\varphi \lor \psi)$ is a homomorphic image of that direct product. Since $C_n$ is a pseudovariety, $M(\varphi \lor \psi) \in C_n$, i.e., $c(M(\varphi \lor \psi)) \leq n$. This completes the proof of (25).

Ad (26): Let $n = c(M(\varphi))$. Since $\text{Mod}_{I,K}(\neg \varphi) = \text{Unique}_{I,K}\setminus\text{Mod}_{I,K}(\varphi)$, the word language $\text{Mod}_{I,K}(\neg \varphi)[m]$ is recognized by the direct product $M(\text{Unique}_{I,K}[m]) \times M(\varphi)$, thus $M(\neg \varphi)$ is a homomorphic image of that direct product. Since $M(\text{Unique}_{I,K}[m]), M(\varphi) \in C_n$ and $C_n$ is a pseudovariety, we conclude $M(\neg \varphi) \in C_n$, i.e., $c(M(\neg \varphi)) \leq n$. Equality follows by symmetry. □

Define $s : \mathbb{N} \to \mathbb{N}, s(m) = 2^m$. As usual, $s^0(m) = m$ and $s^{k+1}(m) = s(s^k(m))$ for every $k$. The function $s^k$ is $k$-fold exponential. Fix some $k \geq 1$ for the rest of this section. Furthermore, assume that $\Gamma = \{0, 1\}^I$ is an alphabet with $I = J \cup K$ for disjoint attribute sets $J, K$.

**Theorem 4.9 ([MT97])** Let $\varphi$ be a $\Sigma_k^\text{mon}$-formula with free set variables in $(X_\mu)_{\mu \in J}$ and free first-order variables in $(x_\nu)_{\nu \in K}$. Then there exists $c \geq 1$ such that for every $m \geq 1$ there exists an NFA with at most $s^k(cm)$ states that recognizes $\text{Mod}_{I,K}(\varphi)[m]$.

The original theorem only states the above result for the case $K = \emptyset$. The present form follows easily by using $\text{Mod}_{I,K}(\varphi) = \text{Mod}_{I \cup K, \emptyset}(\varphi) \cap \text{Unique}_{I,K}$.

Let $n \geq 1$. The transition monoid (see Section 4.2) of an NFA with $n$ states is a submonoid of the monoid $B_n$ of binary relations of an $n$-set (see Definition 3.11).

**Proposition 4.10** Let $\varphi$ be a $\Sigma_k^\text{mon}$-formula. There exists $c \geq 1$ such that for every $m \geq 1$ the syntactic monoid of $\text{Mod}(\varphi)[m]$ divides $B_{s^k(cm)}$. 

Proof Choose \( c \) according to Theorem 4.9. Let \( m \geq 1 \). Set \( n = s^k(cm) \). Let \( \mathfrak{A} \) be an NFA with at most \( n \) states that recognizes \( \text{Mod}(\varphi)[m] \). Let \( M \) be the transition monoid of \( \mathfrak{A} \). Since \( M \) recognizes \( \text{Mod}(\varphi)[m] \), the syntactic monoid of \( \text{Mod}(\varphi)[m] \) is a homomorphic image of \( M \), thus \( M(\text{Mod}(\varphi)[m]) \prec M \). Besides, \( M \prec B_n \). Since \( \prec \) is transitive, we have \( M(\text{Mod}(\varphi)[m]) \prec B_n \), i.e., the claim. \( \square \)

**Proposition 4.11** \( \text{FO}(\Sigma^\text{mon}_k) \) is at most \( k \)-fold exponential wrt. group complexity.

Proof Let \( \mathcal{F} \) be the class of formulas \( \varphi \) such that the function \( m \mapsto c(\text{Mod}(\varphi)[m]) \) is at most \( k \)-fold exponential. By Proposition 4.8 \( \mathcal{F} \) is closed under existential first-order quantification, disjunction, and negation, i.e., \( \text{FO}(\mathcal{F}) = \mathcal{F} \).

By Proposition 4.10 and Theorem 3.18 the class \( \Sigma^\text{mon}_k \) is at most \( k \)-fold exponential wrt. group complexity, i.e., \( \Sigma^\text{mon}_k \subseteq \mathcal{F} \). Thus \( \text{FO}(\Sigma^\text{mon}_k) \subseteq \text{FO}(\mathcal{F}) = \mathcal{F} \), which finishes the proof. \( \square \)

We are now ready to prove the main result of this paper.

**Proof of Theorem 2.10.** By Remark 2.7 we have \( \Sigma^\text{mon}_1(\Pi^0_{k-1}(\Delta^\text{mon}_1)) \subseteq \Sigma^\text{mon}_1(\Pi^0_{k-1}) \subseteq \Sigma^\text{mon}_k \subseteq \text{FO}(\Sigma^\text{mon}_k) \). Therefore it suffices to show that \( \Sigma^\text{mon}_1(\Pi^0_{k-1}(\Delta^\text{mon}_1)) \) is at least \( k \)-fold exponential whereas \( \text{FO}(\Sigma^\text{mon}_k) \) is at most \( k \)-fold exponential wrt. group complexity. The first fact is Theorem 3.19, the second is the preceding proposition. \( \square \)

## 5 Conclusion

We continued the work of [Mat99, Mat02] to investigate the expressive power of first-order quantifications in the context of picture languages. We have adapted a lemma by Straubing that analyses the effect of first-order quantifications in terms of monoid complexity. We combined this with the height fragment technique invented in [Gia94, GRST96] and used in the above papers. This allowed to deduce a new separation result (Theorem 2.10). It may be stated informally as: Adding one more set quantifier alternation gives you expressive power that cannot be captured by adding any number of first-order quantifier alternations.

At the same time we have found a new sequence of picture languages that witness the strictness of the quantifier alternation hierarchy of monadic second-order logic. Unlike the picture languages in [MT97], these new witness picture languages are not characterized by the sizes of their pictures, but rather by the group complexity required to recognize them.

### 5.1 Remarks on the Height Fragment Technique

The height fragment technique (Remark 2.9) plays a crucial role for the separation results for picture language classes defined by quantifier alternation classes of monadic second-order logic. Therefore, it may be instructive to summarize the measures that have been considered so far (more or less explicitly) in the literature and in this paper.
• The state set size measure assigns to every regular word language $L$ the minimal number of states of an NFA that accepts $L$.

• The singleton length measure assigns to every singleton word language $\{a^n\}$ over a singleton alphabet $\{a\}$ the length $n$ of its only element.

• The minimal length measure assigns to every non-empty word language over a singleton alphabet the length of its shortest element.

• The group complexity measure assigns to every non-empty word language $L$ the group complexity of its syntactic monoid.

The proof that the class of $\Sigma_{mon}^1$-definable picture languages over $\{0, 1\}$ is not closed under complement was done in [GRST96] and uses the state set size measure. That picture language class is at most singly exponential wrt. state set size, but the class of $\Pi_{mon}^{k}$-definable picture languages is not, as it contains a language with state set size $2^{\Omega(m^2)}$, namely the picture language of all pictures of the form $pp$, where $p$ is a non-empty square picture.

The first result involving the singleton length measure is from [Gia94] and says that the class of recognizable (or, by [GRST96] equivalently, of $\Sigma_{mon}^1$-definable) picture languages over a singleton alphabet is both at most and at least 1-fold exponential.

Generalizing Giammarresi’s result, in [MT97] (and [Sch97], respectively) it is shown that the class of $\Sigma_{mon}^k$-definable picture languages over a singleton alphabet is at most (and at least, respectively) $k$-fold exponential wrt. singleton length.

In [Mat99], Corollary 3.66 and Theorem 4.25, it is shown that $FO(\Sigma_{mon}^k)$ is both at most and at least $(k+1)$-fold exponential wrt. singleton length.

In [Mat99], Theorem 3.61 and Corollary 4.15, it is shown that $\Pi_{mon}^k$ is at least $(k+1)$-fold exponential whereas $\Sigma_{mon}^k$ is at most $k$-fold exponential wrt. minimal length. This allowed to separate these two classes for the case of a singleton alphabet.

Our result Corollary 2.11 is based on the group complexity measure. That corollary can be proved neither by state set size nor by singleton length, since for every $k \geq 1$, even the class of $FO(\Sigma_{mon}^k)$-definable picture languages is at least $k$-fold exponential wrt. state set size ([MT97]), and both $FO(\Sigma_{mon}^k)$ and $\Sigma_{mon}^k$ are both at most and at least $(k+1)$-fold exponential wrt. singleton length ([Mat99]).

5.2 Open Questions

Corollary 2.11 states that there is a $\Sigma_{mon}^k$-definable picture language that is not $FO(\Sigma_{mon}^{k-1})$-definable. Lemma 3.13 shows that the alphabet is $\{0, 1\}^{\{inp, end\}}$, i.e., the alphabet size is four. We note without proof that one can reduce the size of the alphabet to two by applying standard encoding techniques. It remains open whether we can even reduce the size to one. For that case, we only know:

**Theorem 5.1** ([Mat99], Theorems 2.29, 2.30) Let $k \geq 1$. For a singleton alphabet, there is a $\Sigma_{mon}^k$-definable picture language that is not $FO(\Sigma_{mon}^{k-1})$-definable.
The following problem from [Mat99, JM01] remains open, too.

**Problem 5.2** Is there an MSO-formula that is not equivalent to any $\Sigma_1^{\text{mon}}(\text{FO}(\Sigma_1^{\text{mon}}))$-formula?

Separation results such as Corollary 2.11 may be transferred to other classes of structures, for example, to directed graphs, using standard encoding techniques. This has been carried out formally in [Mat99], Chapter 5. Problem 5.2 is also open in that more general setting of directed graphs. Answering that question might be the first step towards attacking the closed hierarchy as defined in [AFS00].

I find the following questions interesting from a methodological point of view:

**Problem 5.3** Is there any separation result concerning quantifier alternation classes of MSO-formulas (as defined in Section 2.5) that either holds for directed graphs but not for pictures, or holds for pictures but cannot be proved with the height fragment technique?

### 6 Acknowledgments

Thanks go to several participants of the 2010 workshop on “Circuits, logic, and games” in Dagstuhl: Wolfgang Thomas for discussions on the draft of this paper; Nicole Schweikardt for her detailed analysis and helpful feedback; Jean-Eric Pin for the copy of [Pin86] and for pointing me helpful hints when I was stuck in the proof of Proposition 4.11—later I discovered that the group complexity was more suitable than the investigation of the symmetric subgroups, so the respective papers are not cited; Klaus-Jörn Lange for a proof related to the block product, even though that proof did not make it into the present paper because I discovered later that I had asked the wrong question; Pierre McKenzie for pointing me to the Landau function, which I did not need in the end either, because the lengths of the cyclic subgroups then seemed to be the wrong trace; and Thomas Colcombet and Etienne Grandjean for discussions on related subjects.

Last, but not least, I am grateful to Thomas Wilke. When he pointed me to Chapter VI in [Str94], it was not the first time that he gave me the crucial hint that I needed to turn a vague idea into a theorem.

### References

- [AFS00] M. Ajtai, R. Fagin, and L. Stockmeyer. The closure of monadic NP. *Journal of Computer and System Sciences*, 60(3):660–716, 2000. Journal version of STOC’98 paper.
- [Eil76] S. Eilenberg. *Automata, Languages, and Machines*. Number Bd. 2 in Pure and applied mathematics. Academic Press, 1976.
- [Gia94] D. Giannarroresi. Two-dimensional languages and recognizable functions. In G. Rozenberg and A. Salomaa, editors, *Developments in Language Theory, Proceedings of the conference, Turku (Finland) ’93*, pages 290–301. World scientific, Singapore, 1994.
REFERENCES

[GRST96] D. Giammarresi, A. Restivo, S. Seibert, and W. Thomas. Monadic second-order logic and recognizability by tiling systems. *Information and Computation*, 125(1):32–45, 1996. Journal version of STACS’94 paper.

[JM01] D. Janin and J. Marcinkowski. A toolkit for first order extensions of monadic games. In *Proceedings of 18th Annual Symposium on Theoretical Aspects of Computer Science (STACS’01)*, volume 2010 of *Lecture Notes in Computer Science*, pages 353–364. Springer-Verlag, 2001.

[KR65] K. Krohn and J. Rhodes. Algebraic theory of machines. I. Prime decomposition theorem for finite semigroups and machines. *Trans. Amer. Math. Soc.*, 116:450–464, 1965.

[Mat99] O. Matz. *Dot-depth and monadic quantifier alternation over pictures*. PhD thesis, RWTH Aachen, 1999.

[Mat02] O. Matz. Dot-depth, monadic quantifier alternation, and first-order closure over grids and pictures. *Theor. Comput. Sci.*, 270(1-2):1–70, 2002.

[MST02] O. Matz, N. Schweikardt, and W. Thomas. The monadic quantifier alternation hierarchy over grids and graphs. *Information and Computation*, 179(2):356–383, 2002.

[MT97] O. Matz and W. Thomas. The monadic quantifier alternation hierarchy over graphs is infinite. In *Twelfth Annual IEEE Symposium on Logic in Computer Science*, pages 236–244, Warsaw, Poland, 1997. IEEE.

[Pin86] J.-E. Pin. *Varieties Of Formal Languages*. Plenum Publishing Co., 1986.

[Pin96] J.-E. Pin. Logic, semigroups and automata on words. *Annals of Mathematics and Artificial Intelligence*, 16:343–384, 1996.

[Rho74a] J. Rhodes. Finite binary relations have no more complexity than finite functions. *Semigroup Forum*, 7:92–103, 1974.

[Rho74b] J. Rhodes. Proof of the fundamental lemma of complexity (strong version) for arbitrary finite semigroups. *J. Comb. Theory, Ser. A*, 16(2):209–214, 1974.

[RS09] J. Rhodes and B. Steinberg. *The q-theory of finite semigroups*. Springer monographs in mathematics. Springer, 2009.

[RT89] J. Rhodes and B. Tilson. The kernel of monoid morphisms. *Information and Computation*, 62:227–268, 1989.

[Sch97] N. Schweikardt. The monadic quantifier alternation hierarchy over grids and pictures. In Mogens Nielson and Wolfgang Thomas, editors, *Computer Science Logic*, volume 1414 of *Lecture Notes in Computer Science*, pages 441–460. Springer, 1997.

[Str94] H. Straubing. *Finite automata, formal logic, and circuit complexity*. Birkhäuser Verlag, Basel, Switzerland, 1994.