On the Complexity of Free Monoid Morphisms

Klaus-Jörn Lange and Pierre McKenzie*

Wilhelm-Schickard-Institut für Informatik, Universität Tübingen
{lange,mckenzie}@informatik.uni-tuebingen.de

Abstract. We locate the complexities of evaluating, of inverting, and of testing membership in the image of, morphisms $h : \Sigma^* \to \Delta^*$. By and large, we show these problems complete for classes within NL. Then we develop new properties of finite codes and of finite sets of words, which yield image membership subproblems that are closely tied to the unambiguous space classes found between L and NL.

1 Introduction

Free monoid morphisms $h : \Sigma^* \to \Delta^*$, for finite alphabets Σ and Δ, are an important concept in the theory of formal languages (e.g. [7, 12]), and they are relevant to complexity theory. Indeed, it is well known (e.g. [8]) that NP $= \mathit{Closure}(\leq_m^{\mathrm{AC}^0}, HOM_{n.e.}) \subset \mathit{Closure}(\leq_m^{\mathrm{AC}^0}, HOM) = R.E.$, where $\leq_m^{\mathrm{AC}^0}$ denotes many-one AC^0-reducibility, HOM (resp. $HOM_{n.e.}$) is the set of morphisms (resp. nonerasing morphisms), and *Closure* denotes the smallest class of languages containing a finite nontrivial language and closed under the relations specified. Morphisms and their inverses also play a role in studying regular languages and "small" complexity classes: regular language varieties are closed under inverse morphisms [7], and the replacement of morphisms by "polynomial length M-programs", in the definition of recognition by a finite monoid M, allows automata to capture many subclasses of NC^1 [4, 6, 14].

Here we consider the complexity of evaluating inverse morphisms and morphisms $h : \Sigma^* \to \Delta^*$. Specifically, we consider the simple problem **eval** of computing the image of a word v under h, the problem **range** of determining whether a word $w \in h(\Sigma^*)$, and the problem **inv** of computing an element of $h^{-1}(w)$ given $w \in h(\Sigma^*)$. We examine the *fixed* setting, in which the morphism is input-independent, and the *variable* setting, in which the morphism is defined as part of the input.

The general framework of our results is summarized in the following figure. In the fixed case, the **eval** problem characterizes the relation between the classes NC^0, AC^0 and TC^0, and the problems **range** and **inv** are

* On sabbatical leave from the Université de Montréal until August 1998.

closely related to the class NC^1. Membership of **inv** in NC^1 is then to be contrasted with Håstad's result that there exists a fixed NC^0-computable function whose associated inversion problem is P-complete [11]. We also observe that $\mathit{Closure}(\leq_T^{\mathrm{AC}^0}, HOM^{-1}) = \mathrm{TC}^0$, where HOM^{-1} denotes inverse morphisms, yielding yet another characterization of this important subclass of NC^1. In the variable case, the problem **eval** remains in TC^0 while the **range** and **inv** problems capture complexity classes between L and NL.

Problem	*Fixed* setting	*Variable* setting
evaluation	isometric: NC^0 nonisom.: TC^0-complete	isometric: AC^0 nonisom.: TC^0-complete
range	any h: NC^1 chosen h: NC^1-complete [1]	$h(\Sigma)$ prefix code: L-complete unrestricted h: NL-complete
inversion	NC^1	$(\text{Functional-L})^{NL}$

Here we do not distinguish between a circuit-based language class and its functional counterpart. A morphism $h : \Sigma^* \to \Delta^*$ is isometric iff h applied to each $a \in \Sigma$ yields a word of the same length.

An important part of our results, motivated by recent interest in classes intermediate between L and NL [2, 13, 3], is the investigation of the probem **range** in the variable case. Restricting the underlying morphism affects the complexity of the **range** problem, e.g. the **range** problem for prefix codes is in L and is complete for this class. Now, one might expect that imposing the code property on $h(\Sigma)$ should render the **range** problem complete for an unambiguous logspace class. However the resulting problem remains NL-complete. We therefore develop properties of codes and of sets of words, in particular the *stratification* property (see Section 4.2), which yield **range** subproblems of complexity identical to the complexity of the graph accessibility problems introduced to study unambiguous logspace classes (see Section 2). In particular, we show that the problem **range** in which $h(\Sigma)$ is a *stratified code* is many-one equivalent to the GAP problem L_{stu} capturing $\mathit{StUSPACE}(\log n)$, and that a variant of **range** in which $h(\Sigma)$ is a *stratified left partial* code is $\mathit{RUSPACE}(\log n)$-complete. This is particularly interesting since $\mathit{RUSPACE}(\log n)$ was only recently found to have a complete problem [13].

2 Preliminaries

2.1 Complexity theory

We assume familiarity with basic complexity theory. In particular, recall $\mathrm{NC}^0 \subset \mathrm{AC}^0 \subset \mathrm{TC}^0 \subseteq \mathrm{NC}^1 \subseteq \mathrm{L} \subseteq \mathit{StUSPACE}(\log n) \subseteq \mathit{RUSPACE}(\log n) \subseteq \mathit{UL} \subseteq \mathrm{NL} \subseteq \mathrm{P} \subseteq \mathrm{NP}$, where UL is the set of languages accepted by logspace Turing machines which are nondeterministic with at most one accepting computation, $\mathit{RUSPACE}(\log n)$ is defined like UL with the stronger condition that, on any input, at most one path should exist from the initial configuration to *any* accessible configuration y, and $\mathit{StUSPACE}(\log n)$ is defined like UL with yet the stronger condition that, between any pair of configurations (x, y), at most one path should exist from x to y. Furthermore, Functional-L, also denoted FL, is the functional counterpart of L, i.e. the set of functions computable by deterministic Turing machines and FL^{NL} is the set of functions computable by a deterministic Turing machine M having access to an NL-oracle [16].

DLOGTIME uniformity of a circuit family refers to the ability for a Turing machine equipped with an index tape allowing direct access to its input to compute, in time $O(\log n)$, the ith bit in an appropriate binary description of the nth circuit in the family. Specifically, the constructor receives as input the binary representation of i, and some string of length n. For precise details on circuit descriptions, see [5].

Just as GAP is NL-complete and outdegree-one GAP is L-complete [10], the obvious GAP problems L_{stu}, L_{ru}, and L_u, which are respectively $\mathit{StUSPACE}(\log n)$-hard, $\mathit{RUSPACE}(\log n)$-hard, and UL-hard, were introduced for topologically sorted graphs in [2, 13]. L_{ru} is $\mathit{RUSPACE}(\log n)$-complete [13], while L_{stu} is not known to belong to $\mathit{StUSPACE}(\log n)$ and L_u is already NL-complete.

We will make use of the reducibilities $\leq_m^{\mathrm{AC}^0}$ and $\leq_T^{\mathrm{AC}^0}$, which refer to many-one and Turing AC^0 reducibilities respectively.

2.2 Problem definitions

Fix a morphism $h : \Sigma^* \to \Delta^*$ for finite alphabets Σ and Δ, with Σ assumed ordered. In the fixed setting, the three problems of interest in this note are:

eval(h) Given $v \in \Sigma^*$, compute $h(v)$. The *decision problem* has $b \in \Sigma$ and $j \in N$ as further inputs, and asks whether b is the jth symbol in $h(v)$.

range(h) Given $w \in \Delta^*$, determine whether $w \in h(\Sigma^*)$.

inv(h) Given $w \in \Delta^*$, express w as $h(a_{i_1})h(a_{i_2}) \cdots h(a_{i_k})w'$ such that, first, $|w'|$ is minimal, and second, $v := a_{i_1}a_{i_2} \cdots a_{i_k}$ is lexicographically minimal with respect to the ordering of Σ. The *decision problem* is obtained by adding $j \in N$ as an input parameter, and asking for the jth bit in the representation of w.

In the variable setting, the three problems of interest are **eval**, **range**, and **inv**, defined as above, except that the alphabets Σ and Δ, and the morphism h, now form part of the input.

Fix a finite alphabet Γ. Let $v = a_1a_2 \cdots a_n, a_i \in \Gamma, n \geq 0$. The length of v is written $|v|$, and $\#_a(v)$ represents the number of occurrences of $a \in \Gamma$ in v. For $0 \leq i \leq j \leq n$, we define ${}_iv_j$ as $a_{i+1} \cdots a_j$. In particular, ${}_{i-1}v_i$ is a_i if $i \geq 1$. By *subword*, we mean contiguous subword, i.e. a_1a_3 is not a subword of $a_1a_2a_3$.

We encode our problems, in both the fixed and the variable settings, as binary strings. In the fixed setting, a word v over an alphabet Γ is encoded as a sequence of equal length "bytes", each representing a letter in Γ. By the predicate $Q_a(v, i)$, $a \in \Gamma$, $v \in \Gamma^*$, we mean that ${}_{i-1}v_i$ is a (with $Q_a(v, i)$ false when $i > |v|$). In the variable setting, we write $Q_a(v, i)$ as $Q(a, v, i)$ in view of the input-dependent alphabet Σ. Any encoding which allows computing $Q(a, v, i)$ in AC^0 suffices.

To encode a morphism $h : \Sigma^* \to \Delta^*$ (only required in the variable setting), it suffices that the predicate associated with h, denoted $H(b, a, j)$, where $b \in \Delta$, $a \in \Sigma$, and $j \geq 0$, meaning that ${}_{j-1}h(a)_j$ is b, be AC^0-computable. The predicate $H(b, a, j)$ extends to $H(b, v, j)$ for $v \in \Sigma^*$ in the obvious way, and computing this extension is the object of the **eval** problem. We define $H(b, v, j)$ to be false if $j > |h(v)|$.

For $h : \Sigma^* \to \Delta^*$, we define $\max(h)$ as $\max\{|h(a)| : a \in \Sigma\}$.

3 Fixed Case

Throughout this section we fix $h : \Sigma^* \to \Delta^*$. We write the associated predicate $H(b, v, j)$, $b \in \Delta$, $v \in \Sigma^*$, $j \in N$ as $H_b(v, j)$, in view of the fixed alphabet Σ.

3.1 Evaluation

The complexity of evaluating h is low, but it depends in an interesting way on whether h is *isometric*, i.e. whether the length of any $h(w)$ only depends on $|w|$.

Proposition 1. $\mathbf{eval}(h) \in$ *Functional-NC*^{0} *if* $\forall_{a,b\in\Sigma}|h(a)| = |h(b)|$.

Proof. Let h be isometric and let $c = |h(a)|$ $(= \max(h))$ for any $a \in \Sigma$. Then, for $v \in \Sigma^*$, $b \in \Delta$, and $j \in N$, we have $H_b(v,j) \Leftrightarrow (\exists a \in \Sigma)[Q_a(v, \lceil j/c \rceil) \wedge H_b(a, j \ mod \ c)]$. Since Σ is fixed, the existential quantification over a can be done in NC^0. Hence, for each j, $1 \leq j \leq c \cdot |v|$, there is an NC^0 subcircuit C_j computing the jth symbol in $h(v)$. The circuit for $\mathbf{eval}(h)$ is a parallel arrangement of these C_j, $1 \leq j \leq c \cdot |v|$. Uniformity is argued in the technical appendix.

It follows that, when h is isometric, the decision problem $\mathbf{eval}(h) \in \mathrm{AC}^0$. Interestingly, the converse also holds: if h is not isometric, then $\mathbf{eval}(h) \notin$ Functional-AC^0 and the decision problem $\mathbf{eval}(h) \notin \mathrm{AC}^0$, as follows from:

Theorem 2. *If h is nonisometric, then the decision problem* $\mathbf{eval}(h)$ *is TC^0-hard under $\leq_T^{AC^0}$.*

Proof. Since h is not isometric, there exist $a, b \in \Sigma$, $s, t \in N$, such that $|h(a)| = s$ and $|h(b)| = s + t$ with $t > 0$. We claim that MAJORITY, i.e. the language of all words v over the alphabet $\{a, b\}$ having $|v|/2 \leq \#_b(v)$, $\leq_T^{\mathrm{AC}^0}$-reduces to computing the length of $h(v)$. This implies that the extended predicate $H_b(v,j)$, $v \in \Sigma^*$, is TC^0-hard, because $|h(v)|$ is trivially expressed as the largest j, $1 \leq j \leq |v| \cdot \max(h)$, such that $\bigvee_{b\in\Sigma} H_b(v,j)$. And computing the extended predicate $H_b(v,j)$ is precisely the decision problem $\mathbf{eval}(h)$.

To prove the claim that MAJORITY reduces to computing $|h(v)|$, note that $|v|/2 \leq \#_b(v)$ iff $s \cdot |v| + t \cdot |v|/2 \leq s \cdot |v| + t \cdot \#_b(v)$. Now the left hand side of the latter equality can be computed in AC^0 because s and t are constants. As to the right hand side, it is precisely $|h(v)| = s \cdot \#_a(v) + (s + t) \cdot \#_b(v) = s \cdot |v| + t \cdot \#_b(v)$. Hence one can test $|v|/2 \leq \#_b(v)$ in AC^0, once an oracle gate provides the value of $|h(v)|$. Hence MAJORITY $\leq_T^{\mathrm{AC}^0}$-reduces to computing $|h(v)|$.

Corollary 3. *The decision problem* $\mathbf{eval}(h)$ *is in AC^0 iff h is isometric.*

On the other hand, we prove in the appendix that a fixed morphism can always be evaluated in TC^0, so that the reduction from MAJORITY to $\mathbf{eval}(h)$ exhibited in Theorem 2 can in fact be reversed:

Theorem 4. *For each morphism h, the decision problem* $\mathbf{eval}(h) \in TC^0$.

Corollary 5. *If h is a nonisometric morphism, then the decision problem* **eval**(h) *is TC^0-complete under $\leq_T^{AC^0}$.*

The next corollary is also justified in the appendix:

Corollary 6. $TC^0 = \mathit{Closure}(\leq_T^{AC^0}, HOM^{-1})$.

3.2 Range membership

We now turn to the problem of testing whether a word $w \in \Delta^*$ belongs to $h(\Sigma^*)$. Since Σ^* is regular and the regular languages are closed under morphisms, $h(\Sigma^*)$ is regular. Hence **range**$(h) \in$ NC^1. On the other hand, Schützenberger in 1965 exhibited the following family of finite biprefix codes (i.e. codes having the property that no code word is a proper prefix or a proper suffix of another code word) over the binary alphabet $\{a, b\}$:

$$C_n := \{a^n, a^{n-1}ba, a^{n-2}b, ba^{n-1}\} \cup \{a^iba^{n-i-1} \mid 1 \leq i \leq n-3\}.$$

Schützenberger [17] proved that, for each n, the symmetric group S_n divides (i.e. is an epimorphic image of a submonoid of) the syntactic monoid of the Kleene closure C_n^* of C_n. Thus:

Theorem 7. *For every morphism h,* **range**$(h) \in NC^1$. *Furthermore, there exists a morphism h such that* **range**(h) *is NC^1-complete under $\leq_m^{AC^0}$.*

Proof. By Schützenberger [17], S_5 divides the syntactic monoid of the Kleene closure C_5^* of $C_5 = \{aaaaa, aaaaba, aaab, aabaa, abaaa, baaaa\}$. Now Straubing [18, Theorem IX.1.5] proves that any nonsolvable regular language, as is the case here with C_5^* because S_5 is a nonsolvable group, is NC^1-complete. (In reality, the reducibility used by Straubing is neither many-one nor uniform, but the membership tests in Straubing's languages $u^{-1}Kv^{-1}$ and the evaluation of ψ at the end of his argument can be transformed into a single membership test in a finite Boolean combination of the $u^{-1}Kv^{-1}$ languages). Setting $\Sigma = C_5$, $\Delta = \{a, b\}$, and defining $h(w)$ for each $w \in \Sigma$ as the word $w \in \Delta^*$, yields a morphism $h : \Sigma^* \to \Delta^*$ such that $h(\Sigma^*) = C_5^*$. Hence, for this h, **range**(h) is NC^1-complete.

3.3 Inversion

Recall the definition of problem **inv**(h). By using **inv**(h) to determine whether $|w'| > 0$, the decision problem **range**(h) reduces to the decision

problem $\mathbf{inv}(h)$, under $\leq_m^{\mathrm{AC}^0}$ if an obvious encoding is chosen. Hence there is an h such that the decision problem $\mathbf{inv}(h)$ is NC^1-hard (by Theorem 7). Our goal in this section is to show that $\mathbf{inv}(h)$ is in Functional-NC^1, which holds, clearly, iff the decision problem $\mathbf{inv}(h)$ is in NC^1.

Suppose that a word $w \in h(\Sigma^*)$. Then if $h(\Sigma)$ were a code, i.e. if it had the property that any word in $h(\Sigma^*)$ is uniquely expressible as a sequence of elements from $h(\Sigma)$, then computing $h^{-1}(w)$ would simply require computing all the positions i, $1 \leq i \leq |w|$, at which w splits into $w = \alpha\beta$ with $\alpha, \beta \in h(\Sigma^*)$. This set of positions would uniquely break w up into words from $h(\Sigma)$. Since these positions can be computed in NC^1 because $h(\Sigma^*)$ is a regular language, this strategy would solve such instances of $\mathbf{inv}(h)$ in NC^1. Interestingly, we can combine this strategy with a greedy approach and solve the general case in which $h(\Sigma)$ is not a code. The next theorem is proved in the technical appendix:

Theorem 8. *For every morphism h, $\mathbf{inv}(h)$ is in Functional-NC^1.*

4 Variable Case

4.1 Evaluation

The fixed case construction for $\mathbf{eval}(h)$ carries over to the variable case **eval**. We must compute the predicate $H(b, v, j)$, i.e. determine whether the jth symbol in $h(v)$ is b. In the following let $\pi(v)$ be the *Parikh* vector of a word v and M_h the growth matrix of the morphism h, i.e. $(M_h)_{ik}$ is the number of b_k symbols in $h(a_i)$. Then, $H(b, v, j)$ holds iff there exists $i \in N$ and $a \in \Sigma$ such that

$$\pi({}_0v_{i-1})M_h\mathbf{1} < j \leq \pi({}_0v_i)M_h\mathbf{1} \quad \text{and} \quad Q(a, v, i) \quad \text{and} \quad h(a)_{j-(\pi({}_0v_{i-1})M_h\mathbf{1})} = b.$$

Now the computation of M_h out of h and the computations of $\pi({}_0v_{i-1})M_h\mathbf{1}$ and $\pi({}_0v_i)M_h\mathbf{1}$ out of v can be done in TC^0. Indeed, the integers involved in these computations are *small*, i.e. their absolute values are polynomial in the input size, and arithmetic with such integers can even be carried out in AC^0 [5, Lemma 10.5]. But the computation of the *Parikh* vectors needs counting and is TC^0-hard. Hence computing $H(b, v, j)$ is TC^0-hard and $\mathbf{eval} \in$ Functional-TC^0, which we record as:

Theorem 9. *The decision problem* **eval** *is TC^0–complete w.r.t. $\leq_T^{AC^0}$.*

We note that **eval** restricted to isometric morphisms is in AC^0.

4.2 Range membership

Our problem **range** is precisely the *Concatenation Knapsack Problem* considered by Jenner [9], who showed that:

Theorem 10. *(Jenner)* **range** *is NL–complete.*

Recall that a nonempty set $C \subset \Delta^*$ is a *code* if C freely generates C^*, and that C is a *prefix code* if C has the prefix property, i.e. if no word in C has a proper prefix in C. Define **prefixcoderange** to be the **range** problem restricted to input morphisms $h : \Sigma^* \to \Delta^*$ such that $h(\Sigma)$ is a prefix code. The easy proof of the following is included in the appendix:

Theorem 11. prefixcoderange *is L–complete.*

In view of Theorems 10 and 11, it is natural to ask for properties of $h(\Sigma)$ allowing the **range** problem to capture concepts between L and NL like symmetry or unambiguity. For instance, one might reasonably expect *codes* to capture unambiguity, and thus the obvious problem **coderange** to be complete for one of the unambiguous space classes between L and NL. But the mere problem of testing for the code property is NL-hard as shown by Rytter [15]. In the following subsection, we introduce a more elaborate approach which is able to capture unambiguity.

4.2.1 Stratified sets of words and morphisms

Definition 12. a) Let $C \subseteq \Delta^*$ be arbitrary. Define a relation $\rho_C \subseteq \Delta \times \Delta$ as $a \ \rho_C \ b$ iff some word in C contains ab as a subword.

b) C is said to be *stratified* if ρ_C forms a unique maximal acyclic chain $a_1 \ \rho_C \ a_2 \ \rho_C \ \cdots \ \rho_C \ a_n$; in that case, the word $\sigma(C) := a_1 a_2 \cdots a_n \in \Delta^*$ is called the *stratification* of C. (*Example:* The set $\{a, b, ab, bc\} \subset \{a, b, c\}^*$ is stratified, while $\{a, b\}$, $\{ab, ba\}$ and $\{ab, ac\}$ are not.)

Let $C \subset \Delta^*$ be stratified, where we assume from now on that such a stratified set makes use of all the letters in Δ. Clearly, any word $x \in C$ is a subword of $\sigma(C)$. Then, any word $w \in \Delta^*$ is uniquely expressible as $w = \alpha_1 \alpha_2 \ldots \alpha_k$, where each α_i is a maximal common subword of w and $\sigma(C)$.

Proposition 13. *Let $C \subset \Delta^*$ be a stratified set.*

a) *For any $w \in \Delta^*$, $w \in C^*$ iff its canonical decomposition $w = \alpha_1 \alpha_2 \ldots \alpha_k$ into maximal subwords common with $\sigma(C)$ satisfies $\alpha_i \in C^*$ for each i.*

b) *C is a code iff each subword of its stratification $\sigma(C)$ is expressible in at most one way as a concatenation of words from C.*

Testing whether a finite set $C \subset \Delta^*$ is stratified is L-complete. On the other hand, although stratification may seem like an overwhelming restriction, **stratifiedrange**, i.e. the **range** problem for stratified $h(\Sigma)$, is NL-hard:

Theorem 14. stratifiedrange *is NL-complete.*

Proof. To see that **stratifiedrange** is in NL, we first test deterministically in log space whether C is stratified. Then we use the fact that **range** $\in$ NL. The construction used to show NL-hardness is strongly inspired by a proof in [8] and is included in the appendix.

Hence, like **coderange**, but for a different reason, **stratifiedrange** is NL-complete and thus does not appear to capture an unambiguous logspace class. It is **stratifiedcoderange**, namely the problem **range** restricted to the case of a stratified code $h(\Sigma)$, which bears a tight relationship to $StUSPACE(\log n)$. The following theorem is proved in the appendix:

Theorem 15. stratifiedcoderange *and L_{stu} are many-one logspace-equivalent.*

Hence **stratifiedcoderange** is $StUSPACE(\log n)$-hard, and although we are unable to claim a complete problem for $StUSPACE(\log n)$, we have come very close, since even the $StUSPACE(\log n)$-hard language L_{stu}, specifically tailored to capture $StUSPACE(\log n)$, is only known to be in $RUSPACE(\log n)$ [13]. On the other hand, we can claim a complete problem for the unambiguous class $RUSPACE(\log n)$, as follows.

Proposition 13 states that the code property of a stratified set C translates into the unique expressibility of every expressible subword of the stratification of C as an element of C^*. Let us relax this condition and define a stratified set C to be a *left partial code* if no prefix of $\sigma(C)$ can be expressed in two ways as an element of C^*. Furthermore, we let **lpcstratification** be the special case of the **leftpartialcoderange** problem in which we are only asked to determine whether $\sigma(h(\Sigma)) \in h(\Sigma^*)$, i.e. **lpcstratification** is the language of all morphisms $h : \Sigma^* \to \Delta^*$ such

that $h(\Sigma)$ is a left partial code and the stratification of $h(\Sigma)$ is in $h(\Sigma^*)$. Then[1]:

Theorem 16. lpcstratification *is* $RUSPACE(\log n)$*-complete.*

Proof sketch. The construction used in Theorems 14 and 15 in effect proves that **lpcstratification** and L_{ru} are many-one logspace equivalent. Here L_{ru} is the language of graphs having a path from source to target, but required to possess the unique path property only from the source to any accessible node. This is precisely the property which corresponds to the action of canonically expressing the stratification of a left partial code. We then appeal to the main result of [13], namely that L_{ru} is $RUSPACE(\log n)$-complete.

4.3 Inversion

The class (Functional-L)^{NL} can be defined equivalently as the set of functions computed by single valued NL–transducers. We have:

Theorem 17. *Problem* **inv** *is in (Functional-L)*^{NL}*.*

Proof. To solve **inv**, we use the algorithm and the automaton constructed in Theorem 8. Here, instead of first producing $\widehat{w}$, we start the deterministic logspace simulation of the automaton. Whenever the simulation would require reading a letter from $\widehat{w}$, we appeal to an NL-oracle to test whether the current input position breaks w up into a prefix and a suffix in $h(\Sigma^*)$ (an NL-oracle can test this by Theorem 10). This concludes the proof.

We remark that the deterministic version of **inv**, namely the restriction of **inv** in which h is a prefix code, belongs to Functional-L.

Since computing the **inv** function allows answering the **range** question, we have $\mathrm{NL} \subseteq \mathrm{L}^{\mathbf{inv}}$, and by the previous theorem $\mathrm{NL} = \mathrm{L}^{\mathbf{inv}}$. This implies that $\mathrm{FL}^{\mathrm{NL}} = \mathrm{FL}^{\mathbf{inv}}$, i.e. that the **inv** function is Turing-complete for $\mathrm{FL}^{\mathrm{NL}}$.

References

1. E. Allender, V. Arvind, and M. Mahajan, *Arithmetic Complexity, Kleene Closure, and Formal Power Series,* DIMACS TechRep. 97-61, September 1997.

[1] A corresponding restriction to the **stratifiedcoderange** problem could be defined, but this restriction is many-one equivalent to **stratifiedcoderange**. This does not appear to be the case with **lpcstratification** and **leftpartialcoderange**.

2. E. Allender and K.-J. Lange, *StUSPACE(*$\log n$*)* $\subseteq$ *DSPACE(*$\log^2 n/\log\log n$*)*, *Proc. of the 7th ISAAC*, Springer LNCS vol. 1178, pp. 193–202, 1996.
3. E. Allender and K. Reinhardt, Making nondeterminism unambiguous, *Proc. of the 38th IEEE FOCS* , pp. 244–253, 1997.
4. D. A. M. Barrington. Bounded-width polynomial-size branching programs recognize exactly those languages in NC^1. *J. Comput. System Sci.*, 38:150–164, 1987.
5. D. A. M. Barrington, N. Immerman, and H. Straubing. On uniformity within $\mathcal{NC}^1$. *Journal of Computer and System Sciences*, 41:274–306, 1990.
6. D. Barrington and D. Thérien, Finite Monoids and the Fine Structure of NC^1, *J. of the ACM*, 35(4):941-952, 1988.
7. S. Eilenberg, *Automata, Languages and Machines,* Academic Press, Vol. B, (1976).
8. P. Flajolet and J. Steyaert, *Complexity of classes of languages and operators*, Rap. de Recherche 92 de l'IRIA Laboria, novembre 1974.
9. B. Jenner, Knapsack problems for NL, *Information Processing Letters* 54 (1995), pp. 169-174.
10. N. Jones. Space-bounded reducibility among combinatorial problems. *Journal of Computer and System Sciences*, 11:68–85, 1975.
11. J. Håstad, *Computational Limitations for Small-Depth Circuits,* PhD Thesis, M.I.T., ACM Doctoral Dissertation Awards, MIT Press (1987).
12. T. Harju and J. Karhumäki, Morphisms, in *Handbook of Formal Languages*, ed. G. Rozenberg and A. Salomaa, Springer, 1997.
13. K.-J. Lange, An unambiguous class possessing a complete set, *Proc. 14th Annual Symp. on Theoret. Aspects of Computer Science,* Springer LNCS vol. 1200, pp. 339–350, 1997.
14. P. McKenzie, P. Péladeau and D. Thérien, NC^1: The Automata-Theoretic Viewpoint, *Computational Complexity* 1:330-359, 1991.
15. W. Rytter, The space complexity of the unique decipherability problem, *Information Processing Letters* 23 (1986), pp. 1–3.
16. W. Ruzzo, J. Simon and M. Tompa, Space-bounded hierarchies and probabilistic computations *J. Computer and Systems Science* 28, 216–230, 1984.
17. M. Schützenberger, On finite monoids having only trivial subgroups, *Information and Control* 8, 190–194, 1965.
18. H. Straubing, *Finite automata, formal logic, and circuit complexity*, Birkhäuser, Boston, 1994.

Technical Appendix

Uniformity argument in the proof of Proposition 1:
To see that the NC^0 circuit obtained is DLOGTIME-uniform, let s be the (constant) size of the description of any C_j subcircuit. When the DLOGTIME constructor needs to determine the kth bit in the description of the complete circuit, it first checks that $k \leq s{\cdot}c{\cdot}|v|$, and then determines the relevant subcircuit by computing $j = \lceil k/s \rceil$. Note that (the binary representation of) $|v|$ is DLOGTIME-computable from an input of length $|v|$ [5], and that the school method suffices to compute $s \cdot c \cdot |v|$, j, and $k \ mod \ s$, since k is a $\log n$-bit number. The constructor must then seek the bit $k \ mod \ s$ within the description of C_j. This bit is easily computed unless it pertains to an input gate of C_j, in which case the constructor computes $\lceil j/c \rceil$ and makes use of the fact that C_j only ever reads (bits within the binary encoding of) the $\lceil j/c \rceil$th symbol in $|v|$. Note that $j \ mod \ c$ is DLOGTIME-computable as well.

Proof of Theorem 4:
Let the cardinality of Σ be m. In order to compute $H_b(v, j)$, i.e. to check whether the jth symbol of $h(v)$ is a b, we first have to find the integer i fulfilling $k := |h({}_0v_{i-1})| < j \leq |h({}_0v_i)|$. Then we must locate the ith symbol in v, say $a \in \Sigma$, and check that $h(a)_{j-k} = b$. Let l_μ be the length of $h(a_\mu)$ where $a_1, a_2, \ldots, a_m$ are the elements of Σ. Then, $H_b(v, j)$ holds iff, for some i, $1 \leq i \leq n$,

$$\Sigma_{\mu=1}^{m}(l_\mu \cdot \#_{a_\mu}({}_0v_{i-1})) < j \qquad \text{and} \qquad h({}_{i-1}v_i)_{j-k} = b,$$

where $k = |h({}_0v_{i-1})|$, and $h({}_{i-1}v_i)_{j-k}$ is the $(j-k)$th letter of $h({}_{i-1}v_i)$. Now, for a given i, evaluating the above sum is easily reduced in AC^0 to a single operation of counting the number of ones in a zero-one string (say by producing, for each symbol a_μ in ${}_0v_{i-1}$, a zero-one string of length $\max(h)$ having exactly l_μ ones). This counting operation, akin to iterated integer addition, can be done in TC^0. So can the comparison with j and, obviously, the test for $h({}_{i-1}v_i)_{j-k} = b$. By working on all i in parallel and connecting the results with AC^0 circuitry, a DLOGTIME-uniform TC^0-circuit for $H_b(v, j)$ takes shape.

Proof of Corollary 6:
$\subseteq$: Clearly $\mathrm{AC}^0 \subseteq \mathit{Closure}(\leq_T^{\mathrm{AC}^0})$, so that $L := \{0^i 1^j | i \geq j\}$ is in $\mathit{Closure}(\leq_T^{\mathrm{AC}^0})$. Now define $h : \{a, b, c\}^* \to \{0, 1\}^*$ by $h(a) := 0, h(b) := 00$, and $h(c) := 1$. By definition, $h^{-1}(L)$ is in $\mathit{Closure}(\leq_T^{\mathrm{AC}^0}, HOM^{-1})$. But also,

$v \in$ MAJORITY iff $\#_b(v) \geq |v|/2$
iff $|v| + \#_b(v) \geq 3 \cdot |v|/2$
iff $h(vc^{\lceil 3\cdot|v|/2\rceil}) = 0^i 1^j$, $i = |v| + \#_b(v) \geq \lceil 3 \cdot |v|/2\rceil = j$
iff $h(vc^{\lceil 3\cdot|v|/2\rceil}) \in L$
iff $vc^{\lceil 3\cdot|v|/2\rceil} \in h^{-1}(L)$.

Since $c^{\lceil 3\cdot|v|/2\rceil}$ is AC^0-computable from v, we have MAJORITY $\leq_m^{\mathrm{AC}^0}$ $h^{-1}(L)$. Hence MAJORITY is in $\mathit{Closure}(\leq_T^{\mathrm{AC}^0}, HOM^{-1})$, and so is all of TC^0.

$\supseteq$: By induction on the number of steps in the representation of a language as a member of $\mathit{Closure}(\leq_T^{\mathrm{AC}^0}, HOM^{-1})$. In the inductive step, it is required to exhibit a TC^0 circuit simulating an AC^0 circuit with oracle gates for membership tests of the form $v \in h^{-1}(Y)$, for some morphism h and some $Y \in \mathrm{TC}^0$. This is possible by simulating each gate in TC^0 using Theorem 4.

Proof of Theorem 8:
Consider an instance $w \in \Delta^*$ of $\mathbf{inv}(h)$, that is, given w, we wish to compute a decomposition $w = h(a_{i_1})h(a_{i_2})\cdots h(a_{i_k})w'$ such that, first, $|w'|$ is minimal, and second, $v := a_{i_1}a_{i_2}\cdots a_{i_k}$ is lexicographically minimal with respect to the ordering of Σ. Since the longest w-prefix in $h(\Sigma^*)$ is easily determined in NC^1 knowing that $\mathbf{range}(h) \in \mathrm{NC}^1$, we assume in the sequel that $w \in h(\Sigma^*)$, i.e. that w' is the empty word. We also assume with no loss of generality that Σ is ordered in such a way that $|h(a_i)| < |h(a_j)|$ implies $a_i < a_j$. We write X for $h(\Sigma)$ and let $X = \{w_1, w_2, \cdots, w_k\} \subseteq \Delta^*$ such that $|w_1| \leq |w_2| \leq \cdots \leq |w_k| = \max(h)$.

As a first step, the input $w = b_1 b_2 \cdots b_n \in \Delta^*$ is transformed into a word $\widehat{w} = (b_1, \gamma_1)(b_2, \gamma_2)\cdots(b_n, \gamma_n) \in (\Delta')^*$ where $\Delta' := \Delta \times \{0, 1\}$, having the property that $\gamma_i = 1$ iff $b_1 \cdots b_i \in X^*$ and $b_{i+1} \cdots b_n \in X^*$. As seen above, this is possible in NC^1.

Now the strategy will be to scan $\widehat{w}$ from left to right, keeping track of the possible words $w_j \in X$ which, at any one time, remain candidates to express the prefix of w read so far. (To indicate that a word remains possible, in the automaton formalisation below, a "+" symbol is stored in the corresponding state vector.) When a position i in $\widehat{w}$ is reached which splits w into a prefix in X^* and a suffix in X^*, the lexicographically least expression for the prefix is recorded, the set of current possible words is reset to "all possible words", and the procedure continues with the suffix.

To make this formal, we define a finite automaton A operating on input $\widehat{w}$. A is in fact a finite transducer, but instead of cluttering the

definition of A further by formally defining its output function, we will make plain which transitions output a word from X forming part of the desired decompositon of w.

Let $A := (Z, \Delta', \delta, z_0, z_0)$, where $Z := \{F\} \cup \{+,-\}^k \times \{1, 2, \cdots, \max(h)\}$, $z_0 := \langle +, \cdots, +; 1\rangle$, and the transition function $\delta : Z \times \Delta' \longrightarrow Z$ is defined as follows. First, $\delta(F, .) := F$, and then, for $\theta_i \in \{+,-\}, 1 \leq j \leq \max(h), b \in \Delta$ and $\gamma \in \{0,1\}$

$\delta\left(\langle \theta_1, \theta_2, \cdots, \theta_k; j\rangle, (b, \gamma)\right) :=$

IF $\gamma = 1 \wedge (\exists_{1 \leq i \leq k} \theta_i = + \wedge |w_i| = j \wedge (w_i)_j = b)$

THEN z_0 (and output w_i as the next word in the decomposition of w)

ELSE IF $j < \max(h)$

THEN $\langle \theta'_1, \theta'_2, \cdots, \theta'_k; j+1\rangle$

ELSE F

where θ'_i is defined as "+" iff $[\theta_i = +$ and $(w_i)_j = b]$.

With the proviso that the "$\exists_{1 \leq i \leq k}$" above selects the least such i when one exists, the resulting transducer A correctly outputs the lexicographically least sequence of words from X expressing w. In fact, the set of positions $\{i : 1 \leq i \leq |w|, A$ is in state z_0 after reading $_0(\widehat{w})_i\}$ marks the desired decomposition of w. Since this set equals $\{i : A$ accepts $_0(\widehat{w})_i\}$, an NC^1 circuit can perform parallel membership tests in the regular language accepted by A in order to solve $\mathbf{inv}(h)$, proving that $\mathbf{inv}(h)$ is in Functional-NC^1.

Proof of Theorem 11:
It is easy to verify, even in AC^0, that an input morphism h has the prefix property, hence is a prefix code. In that case, determining whether $w \in h(\Sigma^*)$ can be done deterministically in log space. Hence **prefixcoderange** $\in$ L. Let $G = (V, f)$ be an outdegree-one digraph, i.e. $V = \{1, 2, \cdots, n \geq 2\}$ and $f : V \to V$ is such that $i < f(i)$ for all $i < n$. Such graphs have an L-hard accessibility problem. A path exists from node 1 to node n in G iff $23 \cdots n \in h(\Sigma^*)$, where $\Sigma = V \setminus \{n\}$, $\Delta = V$, and for $1 \leq i < n$, $h(i) = (i+1)(i+2) \cdots f(i)$. Since $h(\Sigma)$ has the prefix property, this shows that **prefixcoderange** is L-hard.

Proof of Theorem 14:
We reduce from the accessibility problem of node n from node 1 in a topologically ordered graph $G = (V = \{1, \cdots, n\}, \emptyset \neq E \subseteq \{(i,j) | 1 \leq i < j \leq n\})$. We will in fact prove that a very special case of **stratifiedrange**, namely the problem of testing whether the stratification $\sigma(C)$ of a strat-

ified set C is in C^* (think of C as the image of some alphabet Σ of size $|C|$ under an obvious morphism h, and of $\sigma(C)$ as the only word tested for membership in $h(\Sigma^*) = C^*$), is already NL-hard.

Set $\Delta := \{(i,j)|(i,j) \in E\} \cup \{\overline{(i,j)}|(i,j) \in E\} \cup \{\overline{(0,k)}, (k,n+1)|1 \leq k \leq n\}$. Then, for each $1 \leq i \leq n$, let $w(i)$ be the concatenation of $(i,j)\overline{(i,j)}$ over all $(i,j) \in E$ in ascending order of the js. Observe that $w(i)$ is empty if there are no outgoing edges from node i. Now let $w(0) := \overline{(0,1)(0,2)} \ldots \overline{(0,n)}$, let $w(n+1) := (1,n+1)(2,n+1)\ldots(n,n+1)$, and set $w := w(0)w(1)w(2)\cdots w(n)w(n+1)$. Now define C as the set containing the following words: 1) the word $w(0)w(1)\ldots w(n)$, 2) the word $w(1)w(2)\ldots w(n+1)$, 3) any subword of w of the form $\overline{(i,j)}\ldots(j,k)$, with the exception of such subwords for which $i = 0$ and $k = n+1$. Since all words in C are subwords of w and no symbol occurs more than once, ρ_C induces no cycle on Δ. Moreover, since $E \neq \emptyset$, the words $w(0)w(1)\ldots w(n)$ and $w(1)w(2)\ldots w(n+1)$ have a common subword, so that ρ_C forms a unique maximal chain on Δ. Hence C is stratified with $\sigma(C) := w$. Finally, there is a path from node 1 to node n in G iff $\sigma(C)$ can be written as a concatenation of words from C (a much stronger statement holds, as will be seen in the proof of Theorem 15). This concludes the reduction.

Proof of Theorem 15:
We begin with the reduction from **stratifiedcoderange** to L_{stu}. On input $(h : \Sigma^* \to \Delta^*, w)$ we will construct deterministically in logspace a GAP instance (G,s,t) such that $h(\Sigma)$ is a stratified code and $w \in h(\Sigma^*)$ if and only if G is strongly unambiguous, i.e. there are no two different paths joining any two nodes i and j, and there is a path from s to t. First, check that $h(\Sigma)$ is stratified. If this is not the case set (G,s,t) to be some fixed unsolvable GAP instance with no path from s to t. Second, compute $\sigma(h(\Sigma)) = a_1 a_2 \ldots a_n$. Third, construct a graph $G := (\{0,1,\ldots,n\}, E)$, where E consists of all edges (i,j), $i < j$, such that $a_{i+1}\ldots a_j \in h(\Sigma)$. These operations can be performed in deterministic logspace. Now, for each $i < j$, there is a bijection between distinct expressions of $a_{i+1}\ldots a_j$ as an element of $h(\Sigma)^*$ and distinct paths from node i to node j in G. Hence using Proposition 13, $h(\Sigma)$ is a code if and only if G is strongly unambiguous. We now decompose w into $w = \alpha_1 \cdots \alpha_m$ such that each α_k is a maximal subword of $\sigma(h(\Sigma))$. Thus for each k we have $\alpha_k = a_{i_k+1}\cdots a_{j_k}$ for some $0 \leq i_k < j_k \leq n$. Then $\alpha_k \in h(\Sigma^*)$ if and only if there is a path in G from node i_k to node j_k. Hence h is a code and $w \in h(\Sigma^*)$ exactly when each $(G, i_k, j_k) \in L_{stu}$, $1 \leq k \leq m$. The statement now follows from

the easy fact that L_{stu} is closed under conjunctive reducibilities, i.e.: that $(L_{stu}\$)^* \leq_m L_{stu}$.

To reduce L_{stu} to **stratifiedcoderange**, we use the construction of Theorem 14, where a topologically sorted graph G is transformed into a stratified set of words C in such a way that there is a path from node 1 to node n iff $\sigma(C) \in C^*$. We now show that G is strongly unambiguous if and only if C is a code. If, on the one hand, two distinct paths in G lead from some node i to some node j, then clearly, there exist two distinct expressions of the subword of $\sigma(C)$ which begins with the symbol $\overline{(0,i)}$ and ends with $(j, n+1)$, as an element of C^*.

On the other hand, assume that C is not a code. By Proposition 13 we know that there exists a subword v of $\sigma(C)$ which possesses two different decompositions $v = c_1 \cdots c_m = c_1^{'} \cdots c_{m'}^{'}$ for some $c_i, c_i^{'} \in C$. C consists of two special words (enforcing stratification) together with the subset $\{y \in \Delta^* | \exists_{x,z} : w = xyz, \exists_{i,j,k} : y \in \overline{(i,j)}\Delta^*(j,k)\}$. Obviously, only words from the latter subset can be used to build an ambiguous decomposition of v since the two special words do not start with a barred symbol or do not end with an unbarred one. Thus v is of the form $\overline{(i,j)}v^{'}(j^{'},k)$ for some $i, j, j^{'}, k \leq n$ and $v^{'} \in \Delta^*$. Then $(c_1, \cdots, c_m) \neq (c_1^{'}, \cdots, c_{m'}^{'})$ implies the existence of two different paths in G leading from node j to node $j^{'}$, concluding the proof.