Available at
www.ElsevierComputerScience.com
POWERED BY SCIENCE DIRECT®

Journal of Computer and System Sciences 68 (2004) 657–674

JOURNAL OF COMPUTER AND SYSTEM SCIENCES

http://www.elsevier.com/locate/jcss

Tight lower bounds on the ambiguity of strong, total, associative, one-way functions[☆]

Christopher M. Homan

Department of Computer Science, University of Rochester, Rochester, NY 14627, USA

Received 25 October 2002; revised 27 October 2003

Abstract

We study the ambiguity, or "many-to-one"-ness, of two-argument, one-way functions that are strong (that is, hard to invert even if one of their arguments is given), total, and associative. Such powerful one-way functions are the basis of a cryptographic paradigm described by Rabi and Sherman (Inform. Process. Lett. 64(2) (1997) 239) and were shown by Hemaspaandra and Rothe (J. Comput. System Sci. 58(3) (1999) 648) to exist exactly if standard one-way functions exist.

Rabi and Sherman (1997) show that no total, associative function defined over a universe having at least two elements is one-to-one. We show that if $\mathrm{P} \neq \mathrm{UP}$, then, for every $d \in \mathbb{N}^+$, there is an $\mathcal{O}(\log^{\frac{1}{d}} n)$-to-one, strong, total, associative, one-way function σ_d. We argue that this bound is tight in the sense that any total, associative function having similar properties to σ_d but not necessarily strong or one-way must have at least the same order of magnitude of ambiguity as σ_d has. We demonstrate that the techniques used in proving the above-stated results easily apply to other classes of total, associative functions.

We provide a complete characterization for the existence of strong, total, associative, one-way functions whose ambiguity approaches the lower bounds we provide. We say a language is in PolylogP if there exists a polynomial-time Turing machine M accepting the language such that for some $d \in \mathbb{R}^+$ it holds that M has on each string x at most $\mathcal{O}(\log^d n)$ accepting paths, where $n = |x|$. We show that $\mathrm{P} \neq \mathrm{PolylogP}$ if and only for some $d \in \mathbb{R}^+$ there exists an $\mathcal{O}(\log^d n)$-to-one, strong, total, associative, one-way function.

Keywords: Associativity; Computational complexity; Cryptocomplexity; Cryptography; Ambiguity; One-way functions

[☆] Supported in part by Department of Education (GAAN program) Grant EIA-0080124 and by Grants NSF/CRCD-EEC-98-13002, NSF-INT-9815095/DAAD-315-PPP-gü-ab, and NSF-CCR-9322513.

E-mail address: choman@cs.rochester.edu.

0022-0000/$ - see front matter © 2003 Elsevier Inc. All rights reserved.
doi:10.1016/j.jcss.2003.10.004

1. Introduction

An important, natural property of functions is their degree of ambiguity, or "many-to-one"-ness. We say a function $\sigma : \Sigma^* \to \Sigma^*$ is *h-to-one*, where $h : \mathbb{N} \to \mathbb{N}$, if for each y in the image of σ it holds that $||\{x \mid \sigma(x) = y\}|| \leqslant h(|y|)$ (the definition of h-to-one for k-ary functions, where $k \in \mathbb{N}^+$, is analogous).

We study the ambiguity of two-argument, one-way functions that are strong (that is, hard to invert even if one of their arguments is given), total, and associative. Such powerful one-way functions are the basis of cryptographic protocols described by Rabi and Sherman [RS97] (and due, according to Rabi and Sherman [RS97], to Rivest and Sherman) for two-party, secret-key agreement and for digital signatures. Strong, total, associative one-way functions were shown by Hemaspaandra and Rothe [HR99] to exist exactly if standard one-way functions exist.

Rabi and Sherman [RS97] show that no total, associative function (over a universe having at least two elements) can be unambiguous (i.e., one-to-one). Prior to the present paper, the result of Rabi and Sherman was also the best known lower bound on the ambiguity of strong, total, associative, one-way functions.

We prove that, for each total, associative function σ, if for some $d_\sigma \in \mathbb{N}^+$ the length of each output string is bounded in the lengths of the corresponding input strings by a polynomial of degree d_σ, then for any $\delta \in \mathbb{R}^+$ it holds that σ is not $\mathcal{O}(\log^{\frac{1}{\delta + \log d_\sigma}} n)$-to-one. Thus, we obtain a lower bound on ambiguity that simultaneously is greater than the lower bound provided by Rabi and Sherman and depends only on how fast the output lengths grow relative to the input lengths.

How close to optimal is this lower bound? Grollmann and Selman [GS88] and, independently, Ko [Ko85] and Berman [Ber77] show that $\mathrm{P} \neq \mathrm{UP}$ if and only if there exists a total, one-to-one, one-way function. UP [Val76] is the class of all languages accepted by a nondeterministic Turing machine that runs in polynomial time and has on any input at most one accepting path. We show that if $\mathrm{P} \neq \mathrm{UP}$, then for any $d \in \mathbb{N}^+$ there exists an h-to-one, strong, total, associative, one-way function, where $h : \mathbb{N} \to \mathbb{N}$ is $\mathcal{O}(\log^{\frac{1}{d}} n)$. Moreover, the lengths of the outputs of this function are bounded in the lengths of the inputs by a polynomial of degree 2^d. Thus, in conjunction with our lower bound result, there is no $d' > d$ such that this function is $\mathcal{O}(\log^{\frac{1}{d'}} n)$-to-one. Intuitively speaking, this means, first, that under a standard complexity-theoretic assumption we can construct a strong, total, associative, one-way function σ whose ambiguity depends only on how long the outputs grow with respect to the length of the inputs and, second, that no total, associative function having the same output-length bounds as σ can achieve less ambiguity (up to a constant factor). Thus the lower bounds we provide are quite tight.

The techniques we use to prove the above-mentioned claims can be applied to other classes of total, associative functions. We show that the same tightness argument presented above applies unconditionally (i.e., without requiring that $\mathrm{P} \neq \mathrm{UP}$) to the class of all total, associative, polynomial-time computable functions. We provide improved lower bounds on the ambiguity (over the bound provided by Rabi and Sherman [RS97]) for the class of all total, associative, recursive functions, and the class of all total, associative functions (where in both cases the functions are defined over the set of all finite strings). In both cases we argue that the bounds are quite tight.

Finally, we provide a complete complexity-theoretic characterization for the existence of strong, total, associative, one-way functions whose ambiguity approaches the lower bounds we provide. We define PolylogP to be the class of all languages for which there exists a nondeterministic Turing machine that runs in polynomial time and has on each input $x \in \Sigma^*$ at most $h(n)$ accepting paths, where $n = |x|$ and for some $d \in \mathbb{R}^+$ it holds that $h : \mathbb{N} \to \mathbb{N}$ is $\mathcal{O}(\log^d n)$. PolylogP is a promise class that is quite naturally analogous to the previously-studied classes UP [Val79], FewP [AR88], and $\mathrm{U}_{f(n)}P$ [Bei89], each of which, like PolylogP, is based on a promise that for every language belonging to the class in question there exists a nondeterministic Turing machine that accepts the language with only a limited number of accepting paths. We show that P$\neq$PolylogP if and only if for some $d \in \mathbb{R}^+$ and some $\mathcal{O}(\log^d n)$-to-one function $h : \mathbb{N} \to \mathbb{N}$ there exists an h-to-one, strong, total, associative, one-way function.

The rest of this paper is organized as follows. In the second section we present preliminaries. In the third section we provide lower bounds on the ambiguity of a variety of classes of total, associative functions, each of which includes the strong, total, associative, one-way functions. In the fourth section we prove, unconditionally in some cases and under standard complexity-theoretic assumptions in others, that the lower bounds from the third section are tight. The fifth section concludes the paper and suggests possible future directions.

2. Preliminaries

Fix the alphabet Σ to be $\{0,1\}$. We denote the set of all real numbers by $\mathbb{R}$, the set of all natural numbers by $\mathbb{N}$, the set of all positive real numbers by $\mathbb{R}^+$, and the set of all positive natural numbers by $\mathbb{N}^+$. As is standard, we will sometimes use a regular expression to denote the set of all strings satisfying the regular expression, i.e., Σ^* denotes the set of all finite-length strings, and $\Sigma^* 1$ denotes the set of all finite-length strings ending with a 1. Throughout this paper, "log" denotes the base two logarithm.

A language $L \subseteq \Sigma^*$ is in UP [Val76] if there exists a nondeterministic Turing machine that accepts L, runs in polynomial time, and for all inputs has at most one accepting path. A language L is in PolylogP if there exists a number $d \in \mathbb{R}^+$, an $\mathcal{O}(\log^d n)$ function $h : \mathbb{N} \to \mathbb{N}$, and a nondeterministic Turing machine accepting L that runs in polynomial time and on each input $x \in \Sigma^*$ has at most $h(n)$ accepting paths, where $n = |x|$.

Let $f : A \to B$ denote the function f that maps elements of A to elements of B. We say f is *total* if it is defined on each element of A. The *image* of f, denoted $\mathrm{im}(f)$, is defined as the set $\{b \in B \mid (\exists a \in A)[f(a) \text{ is defined and equal to } b]\}$. The *preimage set* of $b \in B$, denoted $f^{-1}(b)$, is defined as the set $\{a \in A \mid f(a) \text{ is defined and equal to } b\}$. A (possibly partial) function $g : B \to A$ *inverts* f if for each $b \in \mathrm{im}(f)$ it holds that $g(b)$ is defined and $f(g(b))$ is defined and equal to b. A function is in FP if and only if it is total and computable in deterministic polynomial time. We say that $f : A \to \Sigma^*$ is *polynomial-time invertible* if there exists a function $g : \Sigma^* \to A$ that inverts f and is computable in polynomial time in the length of its input. For k-ary functions (where $k \in \mathbb{N}^+$) the terms in this paragraph are defined analogously. For 2-ary functions, we will sometimes use infix notation (e.g., "$x\sigma y$") instead of prefix notation (e.g., "$\sigma(x,y)$").

For each total function $f : A \to A$, each $k \in \mathbb{N}^+$, and each $a \in A$, we denote by $f^k(a)$ the depth-k recursive composition of f on a, e.g., $f^3(a) = f(f(f(a)))$.

A function $f : \mathbb{N} \to \mathbb{N}$ is *unbounded* if for all $n \in \mathbb{N}$ there exists an $m \in \mathbb{N}$ such that $f(m) > n$.

Grollmann and Selman [GS88] (see also independent work by Ko [Ko85] and Berman [Ber77]) provided the first independent study of complexity-theoretic, single-argument, one-to-one, one-way functions. The definition of a one-way function depends on a notion called *honesty*, defined as follows.

Definition 2.1 (Grollmann and Selman [GS88]) (see [Ko85,Ber77,Wat88,Sel92]). A function $f : \Sigma^* \to \Sigma^*$ is *honest* if there exists some polynomial p such that for each $z \in \mathrm{im}(f)$ there exists an $x \in f^{-1}(z)$ such that $|x| \leqslant p(|z|)$.

Intuitively speaking, honesty guarantees that the function is not hard to invert merely because it shrinks the input too much. For instance, the function $f(x) = 1^{\log |x|}$ is not honest and is trivially not polynomial-time invertible.

In this paper, we do not require one-way functions to be one-to-one. Such one-way functions have been studied in the past. Watanabe, for instance, defines one-way functions as we do below and calls one-to-one, one-way functions *strictly one-way* [Wat88].

Definition 2.2 (Watanabe [Wat88]). (see [GS88,Ko85,Ber77,Sel92]). A function $f : \Sigma^* \to \Sigma^*$ is one-way if f is honest, polynomial-time computable, and not polynomial-time invertible.

We can modify the above definitions in a natural way to account for two-argument one-way functions [RS97,HR99].

Definition 2.3 (Rabi and Sherman [RS97]; Hemaspaandra and Rothe [HR99]). We say a two-argument function $\sigma : \Sigma^* \times \Sigma^* \to \Sigma^*$ is *honest* if there exists some polynomial p such that for each $z \in \mathrm{im}(\sigma)$ there exists a pair of strings $(x, y) \in \sigma^{-1}(z)$ such that $\max\{|x|, |y|\} \leqslant p(|z|)$.

We now define two-argument, one-way functions.

Definition 2.4 (Rabi and Sherman [RS97]; Hemaspaandra and Rothe [HR99]). Let $\sigma : \Sigma^* \times \Sigma^* \to \Sigma^*$ be an arbitrary two-argument function. We say σ is a *one-way function* if σ is honest, polynomial-time computable, and not polynomial-time invertible.

Strong noninvertibility captures the possibility that some two-argument, one-way function may still be difficult to invert even when one of its input arguments is known. Strong noninvertibility, in turn, depends on a variation of honesty called *s-honesty*.

Definition 2.5 (Hemaspaandra et al. [HPR01]). A two-argument function σ is called *s-honest* if there exists a polynomial $p : \mathbb{N} \to \mathbb{N}$ such that both 1 and 2 below are true.

1. For each $x, y, z \in \Sigma^*$ such that $x\sigma y = z$ there exists a $y' \in \Sigma^*$ such that $|y'| \leqslant p(\max\{|x|, |z|\})$ and $x\sigma y' = z$.

2. For each $x, y, z \in \Sigma^*$ such that $x\sigma y = z$ there exists an $x' \in \Sigma^*$ such that $|x'| \leqslant p(\max\{|y|, |z|\})$ and $x'\sigma y = z$.

Definition 2.6 (Rabi and Sherman [RS97]; Hemaspaandra and Rothe [HR99]). A total, two-argument function σ is said to be *strongly noninvertible* (or *strong*) if σ is s-honest and neither 1 nor 2 holds.

1. There exists a $g_1 \in \mathrm{FP}$ such that for each $z \in \mathrm{im}(\sigma)$ and each $(x, y) \in \sigma^{-1}(z)$ it holds that $x\sigma g_1(x, z) = z$.
2. There exists a $g_2 \in \mathrm{FP}$ such that for each $z \in \mathrm{im}(\sigma)$ and each $(x, y) \in \sigma^{-1}(z)$ it holds that $g_2(y, z)\sigma y = z$.

Strong noninvertibility does not necessarily imply invertibility; it is known that if $\mathrm{P} \neq \mathrm{NP}$, then some strongly noninvertible functions are invertible [HPR01].

The definition below is the standard definition of associativity found in the mathematics literature. We include it here because previous work on associative one-way functions [RS97,HR99] dealt with a notion known (in the nomenclature of Hemaspaandra and Rothe [HR99]) as *weak associativity*. The difference between the two notions is not relevant for us since for total functions the two notions are known to coincide [HR99].

Definition 2.7 (Rabi and Sherman [RS97]; Hemaspaandra and Rothe [HR99]). Let $\sigma : \Sigma^* \times \Sigma^* \rightarrow \Sigma^*$ be any total, two-argument function. We say σ is *associative* if for all $x, y, z \in \Sigma^*$ it holds that $x\sigma(y\sigma z) = (x\sigma y)\sigma z$.

3. Lower bounds

In this section, we provide lower bounds on the ambiguity of several classes of total, associative functions. As stated in the introduction, our primary goal is to construct strong, total, associative, one-way functions that have low ambiguity. We first provide a lower bound on the ambiguity of such functions that actually applies to *all* total, associative, polynomial-time computable (but not necessarily strong or one-way) functions.

Theorem 3.1. *For all $k \in \mathbb{N}$, no total, associative function from $\Sigma^* \times \Sigma^*$ to Σ^* is k-to-one.*

We do not provide a proof for Theorem 3.1 as it follows almost directly from Lemma 3.2, which is presented below.

Lemma 3.2. *For each total, associative function $\sigma : \Sigma^* \times \Sigma^* \rightarrow \Sigma^*$ and each $k \in \mathbb{N}^+$, there exist strings $x_1, \ldots, x_{k+1} \in \Sigma^*$ for which both* 1 *and* 2 *below hold. (Let $x = x_1\sigma \ldots \sigma x_{k+1}$.)*

1. $\max\{|x_1|, \ldots, |x_{k+1}|\} \leqslant \log(k^2 + 1)$, *and*
2. *at least one of the following holds.*

(a) *There exist distinct $a_1, \ldots, a_k \in \Sigma^*$ and (possibly not distinct) $b_1, \ldots, b_k \in \Sigma^*$ such that for each $i \in \{1, \ldots, k\}$ it holds that $a_i\sigma b_i = x$ and $a_i \neq x$, or*

(b) *there exist distinct* $b_1, \dots, b_k \in \Sigma^*$ *and (possibly not distinct)* $a_1, \dots, a_k \in \Sigma^*$ *such that for each* $i \in \{1, \dots, k\}$ *it holds that* $a_i \sigma b_i = x$ *and* $b_i \neq x$.

Proof. We prove the lemma by induction on k. Let $\sigma : \Sigma^* \times \Sigma^* \to \Sigma^*$ be a total, associative function.

For the basis, let $k = 1$, $x_1 = \varepsilon$, and $x_2 = 0$. Since $\max\{|\varepsilon|, |0|\} \leqslant \log(1^2 + 1)$, item 1 holds. Since $\varepsilon \neq 0$, it holds that one of 2(a) or 2(b) is satisfied, even if $\varepsilon\sigma 0 \in \{\varepsilon, 0\}$.

For the induction hypothesis, choose $k \in \mathbb{N}^+$ and suppose that $x_1, \dots, x_{k+1} \in \Sigma^*$ satisfy conditions 1 and 2(a) (the proof is analogous if conditions 1 and 2(b) are instead satisfied). Let $x = x_1 \sigma \dots \sigma x_{k+1}$. By condition 2(a) we can choose distinct $a_1, \dots, a_k$, and (possibly not distinct) $b_1, \dots, b_k$ in Σ^* such that for each $i \in \{1, \dots, k\}$ it holds that $a_i \sigma b_i = x$ and $a_i \neq x$. Choose $y_1, \dots, y_{k^2+k+1}$ to be the $k^2 + k + 1$ lexicographically smallest strings in Σ^* such that $\{x, a_1, \dots, a_k\} \cap \{y_1, \dots, y_{k^2+k+1}\} = \emptyset$. (Note that $||\{x, a_1, \dots, a_k\} \cup \{y_1, \dots, y_{k^2+k+1}\}|| = k^2 + 2k + 2 = (k+1)^2 + 1$.) Since there are no fewer than $(k+1)^2 + 1$ strings of length at most $\log((k+1)^2 + 1)$, it follows that $\max\{|y_1|, \dots, |y_{k^2+k+1}|\} \leqslant \log((k+1)^2 + 1)$. Consider the following two cases, which cover all possibilities.

For the first case, suppose that there exists a $y \in \{y_1, \dots, y_{k^2+k+1}\}$ such that $x\sigma y \notin \{x, a_1, \dots, a_k\}$. Since σ is associative and since for each $i \in \{1, \dots, k\}$ it holds that $a_i \neq a_i \sigma b_i = x$, it follows that

$$\begin{aligned} a_1\sigma(b_1\sigma y) &= a_2\sigma(b_2\sigma y) \\ &\vdots \\ &= a_k\sigma(b_k\sigma y) \\ &= x\sigma y. \end{aligned}$$

Since $a_1, \dots, a_k$, and x are by hypothesis distinct and distinct from $x\sigma y$, there exist distinct $a'_1, \dots, a'_{k+1}$ (namely $a_1, \dots, a_k$, and x) and (possibly not distinct) $b'_1, \dots, b'_{k+1}$ (namely $b_1\sigma y, \dots, b_k\sigma y$, and y) in Σ^* such that for each $i \in \{1, \dots, k+1\}$ it holds that $a'_i \sigma b'_i = x'_1 \sigma \dots \sigma x'_{k+2}$ and $a'_i \neq x'_1 \sigma \dots \sigma x'_{k+2}$ (where, for $j : 1 \leqslant j \leqslant k+1$, $x'_j = x_j$, and $x'_{k+2} = y$). Thus, condition 2(a) holds for $k+1$. Since $x'_1, \dots, x'_{k+2}$ are each of length less than $\log((k+1)^2 + 1)$, condition 1 also holds.

For the second case, suppose that for each $y \in \{y_1, \dots, y_{k^2+k+1}\}$ it holds that $x\sigma y \in \{x, a_1, \dots, a_k\}$. By the pigeonhole principle there exists an $a \in \{x, a_1, \dots, a_k\}$ and a set $\{y'_1, \dots, y'_{k+1}\} \subseteq \{y_1, \dots, y_{k^2+k+1}\}$ such that for each $y \in \{y'_1, \dots, y'_{k+1}\}$ it holds that $x\sigma y = a$. Since each such y was chosen to be distinct from a, there exist distinct $b'_1, \dots, b'_{k+1}$ (namely $y'_1, \dots, y'_{k+1}$) and (possibly not distinct) $a'_1, \dots, a'_{k+1}$ (indeed in this case they are all the same string, namely x) such that for each $i \in \{1, \dots, k+1\}$ it holds that $a'_i \sigma b'_i = a = x'_1 \sigma \dots \sigma x'_{k+2}$ (where, for $j : 1 \leqslant j \leqslant k+1$, $x'_j = x_j$, and x'_{k+2} is any particular y'_i) and $b'_i \neq a$. Thus condition 2(b) holds for $k+1$. Since $x'_1, \dots, x'_{k+2}$ are each shorter than $\log((k+1)^2 + 1)$, condition 1 also holds. □

As mentioned at the beginning of this section, Theorem 3.1 easily follows from Lemma 3.2.

Theorem 3.3 provides a better lower bound for the case of polynomial-time computable, total, associative functions.

Theorem 3.3. *For each total, associative function $\sigma \in \mathrm{FP}$ there exists a $d \in \mathbb{N}^+$ such that for each $\mathcal{O}(\log^{\frac{1}{d}} n)$ function $h : \mathbb{N} \to \mathbb{N}$ it holds that σ is not h-to-one.*

Note that both Theorems 3.1 and 3.3 provide better lower bounds for their respective classes of functions than does the one-to-one lower bound provided by Rabi and Sherman [RS97].

We will show in Section 4 that the lower bound provided by Theorem 3.3 is tight in the sense that for each $d \in \mathbb{N}^+$ there is a total, associative, $\mathcal{O}(\log^{\frac{1}{d}} n)$-to-one, polynomial-time computable function σ such that for all $x, y \in \Sigma^*$ it holds that $|x\sigma y|$ is $\mathcal{O}((\max\{|x|, |y|\})^{2^d})$ and for all $\delta \in \mathbb{R}^+$ it holds that σ is not $\mathcal{O}(\log^{\frac{1}{\delta+d}} n)$-to-one. Moreover, if $\mathrm{P} \neq \mathrm{UP}$, then it is also tight (in the same sense as above) for the class of all strong, total, associative, one-way functions. Thus, intuitively speaking, under a standard complexity-theoretic assumption restricting the set of all total, associative functions in FP to the set of strong, total, associative, one-way functions comes at little cost in the form of increased ambiguity.

Theorem 3.3 follows almost directly from Lemma 3.4, stated below.

Lemma 3.4. *For each total, associative function $\sigma : \Sigma^* \times \Sigma^* \to \Sigma^*$, if for some $e \in \mathbb{N}^+$ it holds that $|x\sigma y|$ is $\mathcal{O}((\max\{|x|, |y|\})^e)$, where $x, y \in \Sigma^*$, then for each $\delta \in \mathbb{R}^+$ and each $\mathcal{O}(\log^{\frac{1}{\delta+\log e}} n)$ function $h : \mathbb{N} \to \mathbb{N}$ it holds that σ is not h-to-one.*

Lemma 3.4 provides a lower bound on the ambiguity of total, associative functions whose output lengths are polynomially bounded by their input lengths (clearly, all polynomial-time computable, total, associative functions have this property). Moreover, Lemma 3.4 relates the degree of the polynomial bounding the output length to the degree of the radical used in expressing the lower bound on ambiguity.

The following is a brief sketch of how we prove Lemma 3.4. Lemma 3.2 shows that for every $k \in \mathbb{N}^+$ we can find $k+1$ strings $x_1, \dots, x_{k+1}$ such that $\max\{|x_1|, \dots, |x_{k+1}|\} \leqslant \log(k^2+1)$ and the cardinality of the preimage of $x_1\sigma\dots\sigma x_{k+1}$ is at least k. We apply Proposition 3.5 (stated below) to show that if the output string lengths are bounded in the length of the input strings by a polynomial of degree e, then for all positive integers c and real numbers δ there exists a constant C such that $|x_1\sigma\dots\sigma x_{k+1}| \leqslant (\max\{C, |x_1|, \dots, |x_{k+1}|\})^{(\frac{k}{c})^{\delta+\log e}}$. Putting Lemma 3.2 and Proposition 3.5 together lets us express $|x_1\sigma\dots\sigma x_{k+1}|$ as a function of k, which when solved for k can prove Lemma 3.4.

Proposition 3.5. *For each total, associative function $\sigma : \Sigma^* \times \Sigma^* \to \Sigma^*$, if for some total, nondecreasing polynomial $p : \mathbb{N} \to \mathbb{N}$, there exists a $C \in \mathbb{N}$ such that for each $x, y \in \Sigma^*$ it holds that $p(\max\{|x|, |y|, C\}) \geqslant \max\{|x\sigma y|, C\}$, then for each $x_1, \dots, x_k \in \Sigma^*$ it follows that $|x_1\sigma\dots\sigma x_k| \leqslant p^{\lceil \log k \rceil}(\max\{C, |x_1|, \dots, |x_k|\})$.*

Proof of Proposition 3.5. Suppose that $\sigma : \Sigma^* \times \Sigma^* \to \Sigma^*$ is a total, associative function such that for some nondecreasing polynomial $p : \mathbb{N} \to \mathbb{N}$ there exists a $C \in \mathbb{N}$ such that for each $x, y \in \Sigma^*$ it holds that $p(\max\{|x|, |y|, C\}) \geqslant \max\{|x\sigma y|, C\}$. Since σ is total and associative, for each

$x_1, \ldots, x_k \in \Sigma^*$ it follows that $x_1\sigma\ldots\sigma x_k$ is equal to $(x_1\sigma\ldots\sigma x_{\lfloor\frac{k}{2}\rfloor})\sigma(x_{\lfloor\frac{k}{2}\rfloor+1}\sigma\ldots\sigma x_k)$. We may group both $x_1\sigma\ldots\sigma x_{\lfloor\frac{k}{2}\rfloor}$ and $x_{\lfloor\frac{k}{2}\rfloor+1}\sigma\ldots\sigma x_k$ in a similar fashion, etc., to a maximum recursion depth of $\lceil \log k \rceil$, so that

$$|x_1\sigma\ldots\sigma x_k| \leqslant \begin{cases} p(\max\{C, |x_1\sigma\ldots\sigma x_{\lfloor k/2\rfloor}|, |x_{\lfloor k/2+1\rfloor}\sigma\ldots\sigma x_k|\}) & \text{if } k>2, \\ p(\max\{C, |x_1|, |x_2|\}) & \text{otherwise.} \end{cases}$$

Since for each $x, y \in \Sigma^*$ it holds that $p(\max\{|x|, |y|, C\}) \geqslant \max\{|x\sigma y|, C\}$, it follows that $|x_1\sigma\ldots\sigma x_k| \leqslant p^{\lceil \log k \rceil}(\max\{C, |x_1|, \ldots, |x_k|\})$. □

We can now prove Lemma 3.4.

Proof of Lemma 3.4. Suppose that $\sigma : \Sigma^* \times \Sigma^* \to \Sigma^*$ is a total, associative function such that for some $e \in \mathbb{N}^+$ it holds that, for all $x, y \in \Sigma^*$, $|x\sigma y|$ is $\mathcal{O}((\max\{|x|, |y|\})^e)$. Suppose that for some $\delta \in \mathbb{R}^+$ and some $\mathcal{O}(\log^{\frac{1}{\delta+\log e}} n)$ function $h : \mathbb{N} \to \mathbb{N}$ it holds that σ is h-to-one. By assumption, there exist $c, C_1 \in \mathbb{N}$ such that for each $n \in \mathbb{N}$ if $n \geqslant C_1$, then $h(n) \leqslant c \log^{\frac{1}{\delta+\log e}} n$. Since $|x\sigma y|$ is $\mathcal{O}((\max\{|x|, |y|\})^e)$, where $x, y \in \Sigma^*$, there exists a $C_2 \in \mathbb{N}$ such that for each $x, y \in \Sigma^*$ it holds that $(\max\{C_2, |x|, |y|\})^{2^{\frac{\delta}{4}}e} \geqslant \max\{|x\sigma y|, C_2\}$. Choose $k \in \mathbb{N}$ such that k has each of the following properties.

- $\log(k^2+1) \geqslant C_2$.
- For each $z \in \mathrm{im}(\sigma)$ if $||\sigma^{-1}(z)|| \geqslant k$, then $|z| \geqslant C_1$ (such a k exists, since otherwise σ would have an image element with an infinite preimage and so σ could not be h-to-one).
- $\lceil \log(k+1) \rceil = \log(k+1)$.
- $(k+1)^{\frac{\delta}{4}+\log e}\log\log(k^2+1) < (\frac{k}{c})^{\frac{\delta}{2}+\log e}$.

By Lemma 3.2 there exist $x_1, \ldots, x_{k+1} \in \Sigma^*$ such that $\max\{|x_1|, \ldots, |x_{k+1}|\} \leqslant \log(k^2+1)$ and $||\sigma^{-1}(x_1\sigma\ldots\sigma x_{k+1})|| \geqslant k$. By Proposition 3.5,

$$|x_1\sigma\ldots\sigma x_{k+1}| \leqslant (\max\{C_2, |x_1|, \ldots, |x_{k+1}|\})^{(2^{\frac{\delta}{4}}e)^{\lceil \log(k+1) \rceil}}.$$

Since $\max\{|x_1|, \ldots, |x_{k+1}|\} \leqslant \log(k^2+1)$, since k was chosen so that $\log(k^2+1) \geqslant C_2$, and since $\lceil \log(k+1) \rceil = \log(k+1)$,

$$\begin{aligned} |x_1\sigma\ldots\sigma x_{k+1}| &\leqslant (\log(k^2+1))^{(2^{\frac{\delta}{4}}e)^{\log(k+1)}} \\ &= (\log(k^2+1))^{(k+1)^{\frac{\delta}{4}+\log e}} \\ &= 2^{(k+1)^{\frac{\delta}{4}+\log e}\log\log(k^2+1)}. \end{aligned}$$

Since k was chosen so that $(k+1)^{\frac{\delta}{4}+\log e}\log\log(k^2+1) < (\frac{k}{c})^{\frac{\delta}{2}+\log e}$,

$$|x_1\sigma\ldots\sigma x_{k+1}| < 2^{(\frac{k}{c})^{\frac{\delta}{2}+\log e}}.$$

Thus solving for k yields

$$k > c\log^{\frac{1}{\frac{\delta}{2}+\log e}}(|x_1\sigma\ldots\sigma x_{k+1}|). \tag{1}$$

Since $||\sigma^{-1}(x_1\sigma\ldots\sigma x_{k+1})|| \geqslant k$, by our choice of k it follows that $|x_1\sigma\ldots\sigma x_{k+1}| \geqslant C_1$. Thus by assumption, $||\sigma^{-1}(x_1\sigma\ldots\sigma x_{k+1})|| \leqslant c\log^{\frac{1}{\delta+\log e}}(|x_1\sigma\ldots\sigma x_{k+1}|)$. But this contradicts Eq. (1). We conclude that σ is not $\mathcal{O}(\log^{\frac{1}{\delta+\log e}} n)$-to-one. □

4. Tightness of lower bounds

Our goal in this section is to first provide a theoretical framework for constructing total, associative, one-way functions of low ambiguity (in light of the lower bounds from the previous section) and then use this framework to prove that the lower bounds provided in Section 3 are (assuming in some cases certain complexity-theoretic assumptions) tight. We prove that the lower bound provided in Section 3 on the ambiguity of total, associative functions is tight.

Theorem 4.1. 1. *For every nondecreasing, unbounded function* $p : \mathbb{N} \to \mathbb{N}$ *there exists a* p*-to-one, total, associative function.*

2. *For every recursive, nondecreasing, unbounded function* $p : \mathbb{N} \to \mathbb{N}$ *there exists a* p*-to-one, total, associative, recursive function.*

We prove unconditionally that the lower bound provided in Section 3 on the ambiguity of total, associative functions in FP is tight. We prove that if P$\neq$UP, then there exists a strong, total, associative, one-way function whose ambiguity matches the lower bound from the previous section. Finally, we provide a complete complexity-theoretic characterization for the existence of strong, total, associative, one-way functions whose ambiguity approaches the lower bound from the previous section.

Theorem 4.2. 1. *For each* $d \in \mathbb{N}^+$ *there exists a polynomial-time computable, total, associative,* q*-to-one function* $\sigma : \Sigma^* \times \Sigma^* \to \Sigma^*$, *where* $q : \mathbb{N} \to \mathbb{N}$ *is* $\mathcal{O}(\log^{\frac{1}{d}} n)$, *and* $|x\sigma y|$ *is* $\mathcal{O}((\max\{|x|,|y|\})^{2^d})$, *where* $x, y \in \Sigma^*$.

2. *If* P$\neq$UP, *then for each* $d \in \mathbb{N}^+$ *there exists a strong, total, associative,* q*-to-one, one-way function* $\sigma : \Sigma^* \times \Sigma^* \to \Sigma^*$, *where* $q : \mathbb{N} \to \mathbb{N}$ *is* $\mathcal{O}(\log^{\frac{1}{d}} n)$, *and* $|x\sigma y|$ *is* $\mathcal{O}((\max\{|x|,|y|\})^{2^d})$, *where* $x, y \in \Sigma^*$.

3. P$\neq$PolylogP *if and only if there exists a strong, total, associative,* q*-to-one, one-way function, where for some* $d \in \mathbb{R}^+$, $q : \mathbb{N} \to \mathbb{N}$ is $\mathcal{O}(\log^d n)$.

Note that the bound on the output length provided by parts 1 and 2 shows that the lower bound that Lemma 3.4 provides is tight up to a constant factor.

The theoretical framework we use to prove the above theorems is based on a family of total, associative functions of the form $\sigma_{[f,g]} : \Sigma^* \times \Sigma^* \rightarrow \Sigma^*$. Let $\langle \cdot, \ldots, \cdot \rangle : \Sigma^* \times \cdots \times \Sigma^* \rightarrow \Sigma^*$ be a multiarity grouping function that is total, bijective, polynomial-time invertible, and for all $k \in \mathbb{N}^+$ and all $x_1, \ldots, x_k \in \Sigma^*$ is polynomial-time computable in $k + \sum_{i=1}^{k} |x_i|$ and nondecreasing in $k + \sum_{i=1}^{k} |x_i|$, and

$$2k + 2\sum_{i=1}^{k} |x_i| \geqslant |\langle x_1, \ldots, x_k \rangle| \geqslant \sum_{i=1}^{k} |x_i| \quad \text{and} \tag{2}$$

$$|\langle x_1, \ldots, x_k \rangle| + 1 \geqslant k. \tag{3}$$

Note that we require the running time of the function to be polynomially bounded in $k + \sum_{i=1}^{k} |x_i|$ rather than simply $\sum_{i=1}^{k} |x_i|$ in order, for example, to account for the overhead of grouping an arbitrarily long sequence of empty strings. An example of such a function is one that on input $(x_1, \ldots, x_k)$, where $x_1, \ldots, x_k \in \Sigma^*$ and $k \in \mathbb{N}^+$, regards $x_1, \ldots, x_k$ as the nth string in the lexicographical order over all finite strings of the alphabet "0" and "1" and "," (for whichever value of n is appropriate) and maps it to the nth element in the lexicographical order of Σ^*.

For each total function $f : \Sigma^* \rightarrow \Sigma^*$ and each total, nondecreasing, unbounded function $g : \mathbb{N} \rightarrow \mathbb{N}$ we define $\sigma_{[f,g]} : \Sigma^* \times \Sigma^* \rightarrow \Sigma^*$ on input $(x, y) \in \Sigma^* \times \Sigma^*$ as

$$x\sigma_{[f,g]}y = \langle x_1 0^{m_1}, \ldots, x_i 0^{m_i}, y_1 0^{n_1}, \ldots, y_j 0^{n_j} \rangle,$$

where

- $\langle x_1, \ldots, x_i \rangle = \gamma_{[f,g]}(x)$ ($\gamma_{[f,g]} : \Sigma^* \rightarrow \Sigma^*$ is defined below),
- $\langle y_1, \ldots, y_j \rangle = \gamma_{[f,g]}(y)$,
- $(\forall k \in \{1, \ldots, i\})[m_k = \max\{0, g(i+j) - |x_k|\}]$, and
- $(\forall k \in \{1, \ldots, j\})[n_k = \max\{0, g(i+j) - |y_k|\}]$.

The function $\gamma_{[f,g]} : \Sigma^* \rightarrow \Sigma^*$ mentioned in the first two lines of the list above is a subroutine of $\sigma_{[f,g]}$ that determines when to apply f to x or y. The function $\gamma_{[f,g]}$ interprets its single string input as an encoding of a sequence of strings via the mapping $\langle \cdot, \ldots, \cdot \rangle$ that was described above. We define $\gamma_{[f,g]} : \Sigma^* \rightarrow \Sigma^*$ on input $\langle x_1, \ldots, x_k \rangle \in \Sigma^*$ as

$$\gamma_{[f,g]}(\langle x_1, \ldots, x_k \rangle) = \begin{cases} \langle x_1, \ldots, x_k \rangle & \text{if } k > 1 \text{ and} \\ & (\forall j \in \{1, \ldots, k\})[(|x_j| = g(k) \text{ and} \\ & x_j \notin 0^*) \text{ or } (|x_j| > g(k) \text{ and} \\ & x_j \in \Sigma^* 1)], \\ \langle f(x_1) 1 \rangle & \text{if } k = 1, \\ \langle f(\langle x_1, \ldots, x_k \rangle) 1 \rangle & \text{otherwise.} \end{cases}$$

Essentially, the first condition above guarantees that f is not applied to elements in the image of $\sigma_{[f,g]}$. We shall see that this property of $\gamma_{[f,g]}$ helps us prove that $\sigma_{[f,g]}$ is associative.

The intuition behind the design of $\sigma_{[f,g]}$ is as follows. Each function $\sigma_{[f,g]}$ is based on the well-known, total, associative function *concatenation*, but with three key modifications. First, $\sigma_{[f,g]}$ pads its output in such a way that associativity is preserved and the cardinality of the preimage of the padded string is about the same as the cardinality of the preimage that the unpadded string would have under normal concatenation. Since, however, the padding increases (relative to normal concatenation) the length of the output, the ambiguity increases more slowly than it would if the outputs had not been padded. The function g controls the amount of padding. Second, $\sigma_{[f,g]}$ runs some of its inputs through the function f before it pads and outputs them. We will show that whenever f is assumed to be a one-way function, we can choose a g such that $\sigma_{[f,g]}$ is a strong, total, associative, one-way function. Finally, $\sigma_{[f,g]}$ differs from simple concatenation in that rather than conjoining its two inputs side-by-side, it views each string input as an encoding of a sequence of strings and joins the two inputs together by joining together the sequence of strings each input encodes.

In order to get a feel for how $\sigma_{[f,g]}$ works, consider the following example. For any string $x \in \Sigma^*$, let x^R denote the reversal of x, that is, $\varepsilon^R = \varepsilon$ and, for any $a \in \Sigma$ and any $w \in \Sigma^*$, $(aw)^R = w^R a$. Define $f(x) = x^R$. Note that f is one-to-one and polynomial-time computable and invertible. Define $g(n) = 2n$.

Now, for any y, w, and z in Σ^*, $\langle y \rangle \sigma_{[f,g]} \langle w \rangle = \langle y^R 10^m, w^R 10^n \rangle$ and $\langle w \rangle \sigma_{[f,g]} \langle z \rangle = \langle w^R 10^n, z^R 10^p \rangle$, where m (respectively, n, p) is the least number that makes $|y^R 10^m|$ (respectively, $|w^R 10^n|$, $|z^R 10^p|$) greater than or equal to $g(2) = 4$. One can easily check that $\langle y^R 10^m, w^R 10^n \rangle \sigma_{[f,g]} \langle z \rangle = \langle y \rangle \sigma_{[f,g]} \langle w^R 10^n, z^R 10^p \rangle = \langle y^R 10^{m'}, w^R 10^{n'}, z^R 10^{p'} \rangle$, where m' (respectively, n', p') is the least number that makes $|y^R 10^{m'}|$ (respectively, $|w^R 10^{n'}|$, $|z^R 10^{p'}|$) greater than or equal to $g(3) = 6$. We will later prove that $\sigma_{[f,g]}$, for any total f and any total, nondecreasing g, is associative. It is also easy to check that there are only two elements in the preimage of $\langle y^R 10^{m'}, w^R 10^{n'}, z^R 10^{p'} \rangle$, namely $(\langle y^R 10^m, w^R 10^n \rangle, \langle z \rangle)$ and $(\langle y \rangle, \langle w^R 10^n, z^R 10^p \rangle)$, and that this preimage ambiguity is in some sense due to the associativity of $\sigma_{[f,g]}$. Note that the padding provided by the string of zeros at the end of each element in the output effectively allows us to use g to control the amount of ambiguity in $\sigma_{[f,g]}$ that is "due" to associativity.

The following proposition collects some of the basic properties of $\sigma_{[f,g]}$ and $\gamma_{[f,g]}$ that we will use in later proofs.

Proposition 4.3. *For each total $f : \Sigma^* \to \Sigma^*$ and each total, nondecreasing $g : \mathbb{N} \to \mathbb{N}$ the following hold.*

1. *$\gamma_{[f,g]}$ and $\sigma_{[f,g]}$ are both total.*
2. *For each $z \in \mathrm{im}(\sigma_{[f,g]})$ there exist $x_1, \ldots, x_k \in \Sigma^* - 0^*$, where $k > 1$, such that $z = \langle x_1, \ldots, x_k \rangle$.*
3. *For all $x, y \in \Sigma^*$ it holds that $\gamma_{[f,g]}(x \sigma_{[f,g]} y) = x \sigma_{[f,g]} y$.*
4. *For each $z \in \mathrm{im}(\gamma_{[f,g]})$ there exist $x_1, \ldots, x_k \in \Sigma^*$ and $n_1, \ldots, n_k \in \mathbb{N}$, where $k \geqslant 1$, such that $z = \langle x_1 10^{n_1}, \ldots, x_k 10^{n_k} \rangle$ and if for some $z' \in \mathrm{im}(\gamma_{[f,g]})$ there exist $n'_1, \ldots, n'_k \in \mathbb{N}$ such that $z' = \langle x_1 10^{n'_1}, \ldots, x_k 10^{n'_k} \rangle$, then $z' = z$.*

5. *For each* $x \in \Sigma^*$ *such that* $\langle x \rangle \in \mathrm{im}(\gamma_{[f,g]})$ *there exists a* $y \in \Sigma^*$ *such that* $x = y1$ *and* $||\gamma^{-1}_{[f,g]}(\langle x \rangle)|| \leqslant 2 \cdot ||f^{-1}(y)||$.
6. *For each* $\langle x_1, \ldots, x_k \rangle \in \mathrm{im}(\gamma_{[f,g]})$, *where* $k > 1$, *it holds that* $\gamma^{-1}_{[f,g]}(\langle x_1, \ldots, x_k \rangle) = \{\langle x_1, \ldots, x_k \rangle\}$.
7. *If* f *is honest, then* $\gamma_{[f,g]}$ *is honest and* $\sigma_{[f,g]}$ *is honest and s-honest.*

Proof.

1. Clearly, both $\gamma_{[f,g]}$ and $\sigma_{[f,g]}$ are by their definitions total.
2. Choose $z \in \mathrm{im}(\sigma_{[f,g]})$. By the definition of $\gamma_{[f,g]}$, there exist $x_1, \ldots, x_k \in \Sigma^*$ with $k > 1$ such that $z = \langle x_1, \ldots, x_k \rangle$, and for each $j \in \{1, \ldots, k\}$ it holds that $x_j \notin 0^*$.
3. Choose $z \in \mathrm{im}(\sigma_{[f,g]})$. By the definitions of $\sigma_{[f,g]}$ and $\gamma_{[f,g]}$, z satisfies the first of the three conditions listed in the definition of $\gamma_{[f,g]}$, i.e., for some $x_1, \ldots, x_k \in \Sigma^*$ with $k > 1$ it holds that $z = \langle x_1, \ldots, x_k \rangle$ and for each $j \in \{1, \ldots, k\}$ either $|x_j| = g(k)$ and $x_j \notin 0^*$ or $|x_j| > g(k)$ and $x_j \in \Sigma^* 1$. Thus, $\gamma_{[f,g]}(z) = z$.
4. Choose $z \in \mathrm{im}(\gamma_{[f,g]})$. Clearly, by the definition of $\gamma_{[f,g]}$, there exist a $k \in \mathbb{N}^+$, $x_1, \ldots, x_k \in \Sigma^*$, and $n_1, \ldots, n_k$ such that $z = \langle x_1 10^{n_1}, \ldots, x_k 10^{n_k} \rangle$. Suppose for some $z' \in \mathrm{im}(\gamma_{[f,g]})$ that there exist $n'_1, \ldots, n'_k \in \mathbb{N}$ such that $z' = \langle x_1 10^{n'_1}, \ldots, x_k 10^{n'_k} \rangle$. Consider two cases. First, suppose that $k = 1$. Then z and z' are each the output of some string that satisfied one of the last two conditions in the definition of $\gamma_{[f,g]}$. Thus by the definition of $\gamma_{[f,g]}$, $n_1 = n'_1 = 0$. Second, suppose that $k > 1$. In this case choose $l \in \{1, \ldots, k\}$. By the definition of $\gamma_{[f,g]}$, both $|x_l 10^{n_l}|$ and $|x_l 10^{n'_l}|$ are greater than or equal to $g(k)$. If either $|x_l 10^{n_l}|$ or $|x_l 10^{n'_l}|$ is greater than $g(x)$, then by the definition of $\gamma_{[f,g]}$, $n_l = n'_l = 0$. Otherwise, both $|x_l 10^{n_l}|$ and $|x_l 10^{n'_l}|$ are equal to $g(k)$, and so clearly $n_l = n'_l$. Since l was chosen arbitrarily from $\{1, \ldots, k\}$, for all $l \in \{1, \ldots, k\}$ it holds that $n_l = n'_l$. We conclude that $z = z'$.
5. If for some $x \in \Sigma^*$ it holds that $\langle x \rangle \in \mathrm{im}(\gamma_{[f,g]})$, then by the definition of $\gamma_{[f,g]}$, x has a trailing 1. Thus for some $y \in \Sigma^*$ it follows that $x = y1$. Choose $w \in \Sigma^*$ such that $\gamma_{[f,g]}(w) = \langle x \rangle = \langle y1 \rangle$. Then, by the definition of $\gamma_{[f,g]}$, either $f(w) = y$ or $f(w') = y$, where $\langle w' \rangle = w$.
6. If $\langle x_1, \ldots, x_k \rangle \in \mathrm{im}(\gamma_{[f,g]})$, where $k > 1$, then $\langle x_1, \ldots, x_k \rangle$ is the output of some string that satisfies the first of the three conditions listed in the definition of $\gamma_{[f,g]}$. Choose $w \in \Sigma^*$ such that $\gamma_{[f,g]}(w) = \langle x_1, \ldots, x_k \rangle$. By the definition of $\gamma_{[f,g]}$, it follows that $w = \langle x_1, \ldots, x_k \rangle$.
7. Suppose f is honest, via polynomial $p : \mathbb{N} \to \mathbb{N}$. We may assume without loss of generality that p is nondecreasing and that for all $n \in \mathbb{N}$, $p(n) \geqslant n$. By the definition of $\gamma_{[f,g]}$, for each $z \in \mathrm{im}(\gamma_{[f,g]})$ either $\gamma_{[f,g]}(z) = z$ or $\{\langle y \rangle \mid \langle f(y) 1 \rangle = z\} \subseteq \gamma^{-1}_{[f,g]}(z)$. Let $q : \mathbb{N} \to \mathbb{N}$ be a nondecreasing polynomial witnessing that for all $(x_1, \ldots, x_k)$ such that $x_1, \ldots, x_k \in \Sigma^*$ with $k \geqslant 0$ it holds that $\langle \cdot, \ldots, \cdot \rangle$ is polynomial-time computable in $k + \sum_i^k |x_i|$. Either $\gamma_{[f,g]}(z) = z$ or, since f is honest via p and p is nondecreasing, there exists some $\langle y' \rangle \in \{\langle y \rangle \mid \langle f(y) 1 \rangle = z\}$ such that $p(|z|) \geqslant |y'|$. In either case $q(p(|z|)) \geqslant |z'|$, where $z' \in \{z, \langle y' \rangle\}$. Thus $\gamma_{[f,g]}$ is honest. Since $\langle \cdot, \ldots, \cdot \rangle$ is nondecreasing in $k + \sum_{i=1}^k |x_i|$, by the definition of $\sigma_{[f,g]}$, for each $x, y \in \Sigma^*$ it holds

that $|x\sigma_{[f,g]}y| \geqslant \max\{|\gamma_{[f,g]}(x)|, |\gamma_{[f,g]}(y)|\}$. Thus if $\gamma_{[f,g]}$ is honest, then clearly there exist polynomials that witness that $\sigma_{[f,g]}$ is honest and s-honest. □

Next, we prove that each function $\sigma_{[f,g]}$ is indeed associative.

Proposition 4.4. *For each total $f : \Sigma^* \to \Sigma^*$ and each total, nondecreasing $g : \mathbb{N} \to \mathbb{N}$ it holds that $\sigma_{[f,g]}$ is associative.*

Proof. Choose total $f : \Sigma^* \to \Sigma^*$, total, nondecreasing $g : \mathbb{N} \to \mathbb{N}$, and $x, y, z \in \Sigma^*$. Choose $i, j, k \in \mathbb{N}^+$ and $x_1, \dots, x_{i+j+k} \in \Sigma^*$ such that $\langle x_1, \dots, x_i \rangle = \gamma_{[f,g]}(x)$, $\langle x_{i+1}, \dots, x_{i+j} \rangle = \gamma_{[f,g]}(y)$, and $\langle x_{i+j+1}, \dots, x_{i+j+k} \rangle = \gamma_{[f,g]}(z)$ (such $x_1, \dots, x_{i+j+k}$ exist by number 4 of Proposition 4.3).

By the definition of $\sigma_{[f,g]}$, by number 3 of Proposition 4.3, and since g is nondecreasing,

$$\begin{aligned}(x\sigma_{[f,g]}y)\sigma_{[f,g]}z &= \langle x_1 0^{m_1}, \dots, x_{i+j}0^{m_{i+j}} \rangle \sigma_{[f,g]} z \\ &= \langle x_1 0^{n_1}, \dots, x_{i+j+k}0^{n_{i+j+k}} \rangle,\end{aligned}$$

where for each $l \in \{1, \dots, i+j\}$ it holds that $m_l = \max\{0, g(i+j) - |x_l|\}$ and for each $l \in \{1, \dots, i+j+k\}$ it holds that $n_l = \max\{0, g(i+j+k) - |x_l|\}$ (note that $n_l = \max\{0, g(i+j+k) - |x_l|\}$ holds because $g(i+j+k) \geqslant g(i+j)$, which holds because g is nondecreasing). Likewise,

$$\begin{aligned}x\sigma_{[f,g]}(y\sigma_{[f,g]}z) &= x\sigma_{[f,g]} \langle x_{i+1}0^{m_{i+1}}, \dots, x_{i+j+k}0^{m'_{i+j+k}} \rangle \\ &= \langle x_1 0^{n'_1}, \dots, x_{i+j+k}0^{n'_{i+j+k}} \rangle,\end{aligned}$$

where for each $l \in \{i+1, \dots, i+j+k\}$ it holds that $m'_l = \max\{0, g(j+k) - |x_l|\}$ and for each $l \in \{1, \dots, i+j+k\}$ it holds that $n'_l = \max\{0, g(i+j+k) - |x_l|\}$. But then for each $l \in \{1, \dots, i+j+k\}$, it follows that $n'_l = n_l$. Thus $(x\sigma_{[f,g]}y)\sigma_{[f,g]}z = x\sigma_{[f,g]}(y\sigma_{[f,g]}z)$. We conclude that $\sigma_{[f,g]}$ is associative. □

The next proposition provides bounds on the ambiguity of $\sigma_{[f,g]}$.

Proposition 4.5. *For each total, nondecreasing $g : \mathbb{N} \to \mathbb{N}$, define $p : \mathbb{N} \to \mathbb{N}$ on input $n \in \mathbb{N}$ as $p(n) = \max\{m \mid g(m) \leqslant n\}$. If for some total $f : \Sigma^* \to \Sigma^*$ and some total, nondecreasing $q : \mathbb{N} \to \mathbb{N}$, f is q-to-one, then $\sigma_{[f,g]}$ is $(4q^2(n) + p(n))$-to-one.*

Proof. Choose total, nondecreasing $g : \mathbb{N} \to \mathbb{N}$, total $f : \Sigma^* \to \Sigma^*$, total, nondecreasing $q : \mathbb{N} \to \mathbb{N}$ such that f is q-to-one, and $z \in \mathrm{im}(\sigma_{[f,g]})$. Define $p : \mathbb{N} \to \mathbb{N}$ on input $n \in \mathbb{N}$ as $\max\{m \mid g(m) \leqslant n\}$.

By number 2 of Proposition 4.3, there exist a $k \in \mathbb{N}$, $x_1, \dots, x_k \in \Sigma^*$, and $m_1, \dots, m_k \in \mathbb{N}$ such that $k > 1$ and $z = \langle x_1 10^{m_1}, \dots, x_k 10^{m_k} \rangle$. For each $i \in \{1, \dots, k-1\}$, let L_i (respectively, R_{i+1}) be the set of all y such that $y \in \mathrm{im}(\gamma_{[f,g]})$ and for some $n_1, \dots, n_i \in \mathbb{N}$ (respectively, $n_{i+1}, \dots, n_k \in \mathbb{N}$), $y = \langle x_1 10^{n_1}, \dots, x_i 10^{n_i} \rangle$ (respectively, $y = \langle x_{i+1} 10^{n_{i+1}}, \dots, x_k 10^{n_k} \rangle$). By the definition of $\sigma_{[f,g]}$, if $(x', y') \in \sigma^{-1}_{[f,g]}(z)$, then for some $i \in \{1, \dots, k-1\}$ it holds that $\gamma_{[f,g]}(x') \in L_i$ and $\gamma_{[f,g]}(y') \in R_{i+1}$. Clearly, then, $||\sigma^{-1}_{[f,g]}(z)|| \leqslant \sum_{i=1}^{k-1} ||\{x \in \Sigma^* \mid \gamma_{[f,g]}(x) \in L_i\}|| \cdot ||\{y \in \Sigma^* \mid \gamma_{[f,g]}(y) \in R_{i+1}\}||$.

We now calculate for each $i \in \{1, \dots, k-1\}$ the product $||\{x \in \Sigma^* \mid \gamma_{[f,g]}(x) \in L_i\}|| \cdot ||\{y \in \Sigma^* \mid \gamma_{[f,g]}(y) \in R_{i+1}\}||$. By number 4 of Proposition 4.3, the cardinality of each L_i or R_{i+1} is either one or zero.

If $i = 1$, then by number 5 of Proposition 4.3, if $\langle x_1 10^{n_1} \rangle \in L_i$, then $n_1 = 0$ and $||\gamma^{-1}_{[f,g]}(\langle x_1 1 \rangle)|| \leqslant 2 \cdot ||f^{-1}(x_1)||$. By Eq. (2) and since q is nondecreasing, $2 \cdot ||f^{-1}(x_1)|| \leqslant 2q(|x_1 1|) \leqslant 2q(|z|)$. Since the cardinality of L_i is either one or zero, $||\{x \in \Sigma^* \mid \gamma_{[f,g]}(x) \in L_i\}|| \leqslant 2q(|z|)$.

If $i > 1$, then by number 6 of Proposition 4.3, if $\langle x_1 10^{n_1}, \dots, x_i 10^{n_i} \rangle \in L_i$, then $||\gamma^{-1}_{[f,g]}(\langle x_1 10^{n_1}, \dots, x_i 10^{n_i} \rangle)|| \leqslant 1$. Since the cardinality of L_i is either one or zero, $||\{x \in \Sigma^* \mid \gamma_{[f,g]}(x) \in L_i\}|| \leqslant 1$.

By a similar argument, if $i = k-1$, then $||\{x \in \Sigma^* \mid \gamma_{[f,g]}(x) \in R_{i+1}\}|| \leqslant 2q(|z|)$, and if $i < k-1$, then $||\{y \in \Sigma^* \mid \gamma_{[f,g]}(y) \in R_{i+1}\}|| \leqslant 1$.

Now, if $k = 2$, there is only one possible choice for i, in which case $i = 1 = k-1$, so $||\sigma^{-1}_{[f,g]}(z)|| \leqslant 4q^2(|z|)$. If $k > 2$, then there are at least two choices for i, one of which is 1, another of which is $k-1$, and $k-1 \neq 1$. For the remaining $k-3$ choices, i is neither 1 nor $k-1$. Thus $||\sigma^{-1}_{[f,g]}(z)|| \leqslant 4q(|z|) + k - 3$.

By the definition of $\sigma_{[f,g]}$, for each $l \in \{1, \dots, k\}$ it holds that $|x_l 10^{m_l}| \geqslant g(k)$. From this and by Eq. (2) it follows that $|z| \geqslant g(k)$. But then, by the definition of p, $k \leqslant p(|z|)$.

We conclude that $\sigma_{[f,g]}$ is $(4q^2(n) + p(n))$-to-one. □

We are now ready to prove Theorem 4.1.

Proof of Theorem 4.1. Let $p : \mathbb{N} \to \mathbb{N}$ be total, nondecreasing, and unbounded. Define $g : \mathbb{N} \to \mathbb{N}$ on input n as $g(n) = \min\{m \in \mathbb{N} \mid p(m) - 4 \geqslant n\}$. Thus, for all $a \in \mathbb{N}$ it holds that $\max\{b \in \mathbb{N} \mid g(b) \leqslant a\} \leqslant p(a) - 4$. Note that g is total and nondecreasing and that if p is recursive, then so is g. Let $f : \Sigma^* \to \Sigma^*$ be the identity. Thus f is one-to-one and total. By Proposition 4.5, $\sigma_{[f,g]}$ is p-to-one. □

Lemma 4.6. *For each $d \in \mathbb{N}$ and each total $f \in \mathrm{FP}$, if $g : \mathbb{N} \to \mathbb{N}$ is defined on each $n \in \mathbb{N}$ as 2^{n^d}, then $\sigma_{[f,g]} \in \mathrm{FP}$. If $|f(z)|$ is $\mathcal{O}(|z|^{2^d})$, where $z \in \Sigma^*$, then $|x\sigma_{[f,g]}y|$ is $\mathcal{O}((\max\{|x|, |y|\})^{2^d})$, where $x, y \in \Sigma^*$.*

Proof. Choose $d \in \mathbb{N}$ and total $f \in \mathrm{FP}$. Define $g : \mathbb{N} \to \mathbb{N}$ on each $n \in \mathbb{N}$ as 2^{n^d}. Clearly, g is total and nondecreasing. Since f is in FP, $\gamma_{[f,g]}$ is clearly in FP. By number 1 of Proposition 4.5, $\sigma_{[f,g]}$ is total. Since essentially all $\sigma_{[f,g]}$ does is call $\gamma_{[f,g]}$ multiple (but polynomially bounded in the length of the input) times, pad the outputs of each call to $\gamma_{[f,g]}$ and group the padded outputs together via $\langle \cdot, \dots, \cdot \rangle$, and since $\gamma_{[f,g]}$ and $\langle \cdot, \dots, \cdot \rangle$ are in FP, all that remains to be proven in order to show that $\sigma_{[f,g]}$ is polynomial-time computable is that the padding can be performed in polynomial time.

Choose $x, y \in \Sigma^*$. Thus, by number 2 of Proposition 4.3, for some $i, j \in \mathbb{N}$ and some $x_1, \dots, x_i, y_1, \dots, y_j \in \Sigma^* - 0^*$ it follows that $\langle x_1, \dots, x_i \rangle = \gamma_{[f,g]}(x)$ and $\langle y_1, \dots, y_j \rangle = \gamma_{[f,g]}(y)$.

Suppose without loss of generality that $i \geqslant j$. Consider the two cases, which cover all possibilities, below.

First, suppose that $i = j = 1$. Then $\langle x_1, \dots, x_i \rangle = \langle x_1 \rangle$, $\langle y_1, \dots, y_j \rangle = \langle y_1 \rangle$, and $x\sigma y = \langle x_1 0^{l_1}, y_1 0^{l_2} \rangle$, where l_1 and l_2 are both less than 2^{2^d}, which is constant in $\max\{|x|, |y|\}$. Thus, $\sigma_{[f,g]}$ is polynomial-time computable when restricted to strings satisfying the constraints of this case.

Next, suppose that $i > 1$. By number 6 of Proposition 4.3, $x = \langle x_1, \dots, x_i \rangle$. For each $x' \in \{x_1, \dots, x_i\}$ and by the definition of $\gamma_{[f,g]}$, $|x'| \geqslant 2^{i^d}$, from which it follows (due to Eq. (2)) that $\max\{|x|, |y|\} \geqslant i2^{i^d}$. Furthermore, by the definition of $\sigma_{[f,g]}$, $x\sigma_{[f,g]}y = \langle x_1 0^{l_1}, \dots, x_i 0^{l_i}, y_1 0^{l_{i+1}}, \dots, y_j 0^{l_{i+j}} \rangle$, where each $l \in \{l_1, \dots, l_{i+j}\}$ is less than or equal to $2^{(2i)^d} = (2^{i^d})^{2^d}$ and thus is less than or equal to $(\max\{|x|, |y|\})^{2^d}$. It follows that $\sigma_{[f,g]}$ can pad such inputs in polynomial time, and is thus polynomial-time computable (via a polynomial of degree at least 2^d) when restricted to strings satisfying the constraints of this case. Because $\sigma_{[f,g]}$ is polynomial-time computable when restricted to either case, $\sigma_{[f,g]}$ is polynomial-time computable.

Now, suppose that $|f(z)|$ is $\mathcal{O}(|z|^{2^d})$. By the definition of $\gamma_{[f,g]}$, then, there exists a $c \in \mathbb{N}$ such that for all $x, y, x_1, x_2, \dots, x_i, y_1, y_2, \dots, y_j \in \Sigma^*$ chosen as in the first part of the proof it holds that $|x_1| + \cdots + |x_i| + |y_1| + \cdots + |y_j| \leqslant c(\max\{|x|, |y|\})^{2^d} + c$. Since each $l \in \{l_1, \dots, l_{i+j}\}$ is less than or equal to $(2^{i^d})^{2^d}$, it follows, by Eqs. (2) and(3) (and recall that, by assumption, $2i \geqslant i + j$),

$$\begin{aligned}
|\langle x_1 0^{l_1}, \dots, x_i 0^{l_i}, y_1 0^{l_{i+1}}, \dots, y_j 0^{l_{i+j}} \rangle| &\leqslant 4i + 2(c(\max\{|x|, |y|\})^{2^d} + c + 2i(2^{i^d})^{2^d}) \\
&\leqslant 4(\max\{|x|, |y|\} + 1) \\
&\quad + 2(c(\max\{|x|, |y|\})^{2^d} + c \\
&\quad + 2(\max\{|x|, |y|, 2\})^{2^d}).
\end{aligned}$$

Thus $|\langle x_1 0^{l_1}, \dots, x_i 0^{l_i}, y_1 0^{l_{i+1}}, \dots, y_j 0^{l_{i+j}} \rangle|$ is $\mathcal{O}((\max\{|x|, |y|\})^{2^d})$.

Lemma 4.7 below shows that if f is a total, one-way function and g is chosen properly, then $\sigma_{[f,g]}$ is a strong, total, associative, one-way function.

Lemma 4.7. *For each $d \in \mathbb{N}$, if $g : \mathbb{N} \to \mathbb{N}$ is defined on each input $n \in \mathbb{N}$ as 2^{n^d} and $f : \Sigma^* \to \Sigma^*$ is a total, one-way function, then $\sigma_{[f,g]}$ is a strong, total, associative, one-way function.*

Proof. Choose $d \in \mathbb{N}$, define $g(n) = 2^{n^d}$, and choose f to be a total, one-way function. By Proposition 4.4, $\sigma_{[f,g]}$ is associative. By Lemma 4.6, $\sigma_{[f,g]}$ is in FP (and thus total). By number 7 of Proposition 4.3, $\sigma_{[f,g]}$ is honest and s-honest. Suppose there is some function $h \in \mathrm{FP}$ such that for each $z \in \mathrm{im}(\sigma_{[f,g]})$ it holds that $\sigma_{[f,g]}(h(z)) = z$. We could then invert f in polynomial time as follows.

> On input $y \in \Sigma^*$, let $(x_1, x_2) = h(\langle y10^l, y10^l \rangle)$, where $l = \max\{0, g(2) - |y1|\}$. By the definition of $\sigma_{[f,g]}$, either $f(x_1) = y$ or there exists an $x \in \Sigma^*$ such that $\langle x \rangle = x_1$ and $f(x) = y$. If such an x exists, then output it. Otherwise output x_1.

To see that $\sigma_{[f,g]}$ is strongly noninvertible, suppose that there exists a function $h \in \mathrm{FP}$ such that for each $x, y, z \in \Sigma^*$ such that $x\sigma y = z$ it holds that $h(z, y)\sigma y = z$ (the proof is analogous if we instead assume that there exists a function $h \in \mathrm{FP}$ such that for each $x, y, z \in \Sigma^*$ such that $x\sigma y = z$ it holds that $x\sigma h(z, x) = z$). We could then invert f in polynomial time as follows.

> On input $y \in \Sigma^*$, let $x' = h(\langle y10^{l_1}, f(0)10^{l_2}\rangle, \langle 0\rangle)$, where $l_1 = \max\{0, g(2) - |y1|\}$ and $l_2 = \max\{0, g(2) - |f(0)1|\}$. By the definition of $\sigma_{[f,g]}$, either $f(x') = y$ or there exists an $x \in \Sigma^*$ such that $\langle x\rangle = x'$ and $f(x) = y$. If such an x exists, then output it. Otherwise output x'.

We conclude that $\sigma_{[f,g]}$ is a strong, total, associative, one-way function. □

We now prove Theorem 4.2.

Proof of Theorem 4.2. For part 2, if $\mathrm{P} \neq \mathrm{UP}$, then by the well-known result of Grollmann and Selman [GS88] (and independently Ko [Ko85] and, essentially, Berman [Ber77]), there exists a one-to-one, total, one-way function f where the length of each output is linear in the length of the corresponding input. Choose $d \in \mathbb{N}^+$ and define $g : \mathbb{N} \to \mathbb{N}$ on input n to be $g(n) = 2^{n^d}$. Clearly, $|f(z)|$ is $\mathcal{O}(|z|^{2^d})$, where $z \in \Sigma^*$. By Proposition 4.5, $\sigma_{[f,g]}$ is $(4 + \log^{\frac{1}{d}} n)$-to-one. Clearly, $4 + \log^{\frac{1}{d}} n$ is $\mathcal{O}(\log^{\frac{1}{d}} n)$. By Lemma 4.7, $\sigma_{[f,g]}$ is a strong, total, associative, one-way function. By Proposition 4.6, $|x\sigma_{[f,g]}y|$ is $\mathcal{O}((\max\{|x|, |y|\})^{2^d})$, where $x, y \in \Sigma^*$.

For the right-to-left direction of part 3 of Theorem 4.2, suppose that for some $d \in \mathbb{R}^+$ and some $\mathcal{O}(\log^d n)$ function $q : \mathbb{N} \to \mathbb{N}$, σ is a q-to-one, strong, total, associative, one-way function. Let $h : \mathbb{N} \to \mathbb{N}$ witness that σ is honest. We may assume without loss of generality that h is total and nondecreasing. Then the language $\{\langle x, y, z\rangle \in \Sigma^* \mid (\exists \langle x', y'\rangle \in \Sigma^*)[x'\sigma y' = z$ and $\max\{|x'|, |y'|\} \leqslant h(|z|)$ and $\langle x', y'\rangle$ is lexicographically greater than $\langle x, y\rangle]\}$ is in NP via a nondeterministic Turing machine that runs in polynomial time and on input $\langle x, y, z\rangle \in \Sigma^*$ nondeterministically guesses a pair of strings $\langle x', y'\rangle$ such that $\max\{|x'|, |y'|\} \leqslant h(|z|)$ and accepts $\langle x, y, z\rangle$ if and only if $\langle x', y'\rangle$ is both lexicographically greater than $\langle x, y\rangle$, and $x'\sigma y' = z$. Since σ is q-to-one, there are at most $q(|z|)$ such pairs $\langle x', y'\rangle$. Since σ is honest via h, if $z \in \mathrm{im}(\sigma)$, then there is at least one such pair $\langle x', y'\rangle$. Since, by Eq. (2), $|\langle x, y, z\rangle| \geqslant |z|$ and since q is nondecreasing, $q(|\langle x, y, z\rangle|) \geqslant q(|z|)$. Thus the nondeterministic Turing machine described above has on any input w at most $q(|w|)$ accepting paths. Thus the language in question is in PolylogP. Also, the language is not in P, since otherwise we could invert σ in polynomial time via binary search.

For the left-to-right direction, suppose that $\mathrm{P} \neq \mathrm{PolylogP}$ via a polynomial-time Turing machine M for which there exists a $d \in \mathbb{R}^+$ such that for some $\mathcal{O}(\log^d n)$ function $q : \mathbb{N} \to \mathbb{N}$ it holds that for all $x \in \Sigma^*$, M has at most $q(|x|)$ accepting paths. We may assume without loss of generality that q is total and nondecreasing. Adapting the construction of Grollmann and Selman [GS88] for creating a one-to-one, one-way function if $\mathrm{P} \neq \mathrm{UP}$, we can create a q-to-one, one-way function $f : \Sigma^* \to \Sigma^*$. Choose $e \in \mathbb{N}$ such that $e \geqslant d$. We then define $g : \mathbb{N} \to \mathbb{N}$ on input n to be 2^{n^e}. By

Proposition 4.5, $\sigma_{[f,g]}$ is $(4q^2(n) + \log^{\frac{1}{e}} n)$-to-one. Clearly, for some $d' \in \mathbb{R}^+$, $4q^2(n) + \log^{\frac{1}{e}} n$ is $\mathcal{O}(\log^{d'} n)$. By Lemma 4.7, $\sigma_{[f,g]}$ is a strong, total, associative, one-way function.

The argument for part 1 is similar to the argument for part 2 except that we let $f : \Sigma^* \to \Sigma^*$ be the identity. □

5. Conclusion

We extend a result of Rabi and Sherman [RS97], who showed no strong, total, associative, one-way function is one-to-one. We prove that for every total, associative, polynomial-time computable function $\sigma : \Sigma^* \times \Sigma^* \to \Sigma^*$ there exists a $d \in \mathbb{N}^+$ such that for each $\mathcal{O}(\log^{\frac{1}{d}} n)$ function $h : \mathbb{N} \to \mathbb{N}$, σ is not h-to-one. We prove that this lower bound is tight. Moreover, if $\mathrm{P} = \mathrm{UP}$, then this lower bound is also tight when restricted to the class of strong, total, associative, one-way functions. We provide a complete complexity-theoretic characterization for the existence of strong, total, associative, one-way functions whose ambiguity approaches the lower bounds we provide, namely that $\mathrm{P} \neq \mathrm{PolylogP}$ if and only if there exists a $d \in \mathbb{R}^+$, a $\mathcal{O}(\log^d n)$ function $h : \mathbb{N} \to \mathbb{N}$, and an h-to-one, strong, total, associative, one-way function. Finally, we prove that no total, associative function over an infinite universe is constant-to-one, and that this bound is tight.

We mention possible future directions. Do any of our results translate into average-case (i.e., cryptographic) one-way function theory? Also, as average-case complexity is to worst-case complexity, can we study average-case ambiguity as an alternate to the "worst-case" ambiguity defined and studied in this paper? What properties might associative functions with average-case ambiguity constraints exhibit?

Acknowledgments

I am grateful to Lane Hemaspaandra for suggesting this topic and for his continual guidance and encouragement and to Alina Beygelzimer, Edith Elkind, Lane Hemaspaandra, Harald Hempel, Jörg Rothe, Alan Selman, Rahul Tripathi, and Mayur Thakur for their careful reviews and numerous suggestions.

References

[AR88] E. Allender, R. Rubinstein, P-printable sets, SIAM J. Comput. 17 (6) (1988) 1193–1202.

[Bei89] R. Beigel, On the relativized power of additional accepting paths, in: Proceedings of the Fourth Annual Conference on Structure in Complexity Theory, 1989, pp. 216–224. Note added in [Bei95].

[Bei95] R. Beigel, On the relativized power of additional accepting paths, 1995. Manuscript. Updates [Bei89].

[Ber77] L. Berman, Polynomial reducibilities and complete sets, Ph.D. Thesis, Cornell University, Ithaca, NY, 1977.

[GS88] J. Grollmann, A. Selman, Complexity measures for public-key cryptosystems, SIAM J. Comput. 17 (2) (1988) 309–335.

[HPR01] L. Hemaspaandra, K. Pasanen, J. Rothe, If P≠NP then some strongly noninvertible functions are invertible, in: Proceedings of the 13th International Symposium on Fundamentals of Computation Theory, Riga, Latvia, 2001, pp. 162–171.

[HR99] L. Hemaspaandra, J. Rothe, Creating strong, total, commutative, associative one-way functions from any one-way function in complexity theory, J. Comput. System Sci. 58 (3) (1999) 648–659.

[Ko85] K. Ko, On some natural complete operators, Theoret. Comput. Sci. 37 (1) (1985) 1–30.

[RS97] M. Rabi, A. Sherman, An observation on associative one-way functions in complexity theory, Inform. Process. Lett. 64 (2) (1997) 239–244.

[Sel92] A. Selman, A survey of one-way functions in complexity theory, Math. Systems Theory 25 (3) (1992) 203–221.

[Val76] L. Valiant, The relative complexity of checking and evaluating, Inform. Process. Lett. 5 (1) (1976) 20–23.

[Val79] L. Valiant, The complexity of enumeration and reliability problems, SIAM J. Comput. 8 (3) (1979) 410–421.

[Wat88] O. Watanabe, On hardness of one-way functions, Inform. Process. Lett. 27 (1988) 151–157.