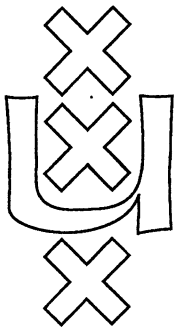
Institute for Language, Logic and Information

QUASI-INJECTIVE REDUCTIONS

Lane A. Hemachandra
Edith Spaan

ITLI Prepublication Series
for Computation and Complexity Theory CT-91-11



University of Amsterdam

The ITLI Prepublication Series

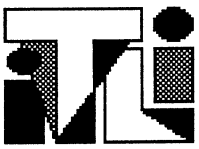
1986
86-01 The Institute of Language, Logic and Information
86-02 Peter van Emde Boas — A Semantical Model for Integration and Modularization of Rules
86-03 Johan van Benthem — Categorial Grammar and Lambda Calculus
86-04 Reinhard Muskens — A Relational Formulation of the Theory of Types
86-05 Kenneth A. Bowen, Dick de Jongh — Some Complete Logics for Branched Time, Part I Well-founded Time,
86-06 Johan van Benthem — Logical Syntax Forward looking Operators

1987 87-01 Jeroen Groenendijk, Martin Stokhof — Type shifting Rules and the Semantics of Interrogatives
87-02 Renate Bartsch — Frame Representations and Discourse Representations
87-03 Jan Willem Klop, Roel de Vrijer — Unique Normal Forms for Lambda Calculus with Surjective Pairing
87-04 Johan van Benthem — Polyadic quantifiers
87-05 Víctor Sánchez Valencia — Traditional Logicians and de Morgan's Example
87-06 Eleonore Oversteegen — Temporal Adverbials in the Two Track Theory of Time
87-07 Johan van Benthem — Categorial Grammar and Type Theory
87-08 Renate Bartsch — The Construction of Properties under Perspectives
87-09 Herman Hendriks — Type Change in Semantics: The Scope of Quantification and Coordination

1988 LP-88-01 Michiel van Lambalgen — *Logic, Semantics and Philosophy of Language:* Algorithmic Information Theory
LP-88-02 Yde Venema — Expressiveness and Completeness of an Interval Tense Logic
LP-88-03 — Year Report 1987
LP-88-04 Reinhard Muskens — Going partial in Montague Grammar
LP-88-05 Johan van Benthem — Logical Constants across Varying Types
LP-88-06 Johan van Benthem — Semantic Parallels in Natural Language and Computation
LP-88-07 Renate Bartsch — Tenses, Aspects, and their Scopes in Discourse
LP-88-08 Jeroen Groenendijk, Martin Stokhof — Context and Information in Dynamic Semantics
LP-88-09 Theo M.V. Janssen — A mathematical model for the CAT framework of Eurotra
LP-88-10 Anneke Kleppe — A Blissymbolics Translation Program
ML-88-01 Jaap van Oosten — *Mathematical Logic and Foundations:* Lifschitz' Realizability
ML-88-02 M.D.G. Swaen — The Arithmetical Fragment of Martin Löf's Type Theories with weak Σ-elimination
ML-88-03 Dick de Jongh, Frank Veltman — Provability Logics for Relative Interpretability
ML-88-04 A.S. Troelstra — On the Early History of Intuitionistic Logic
ML-88-05 A.S. Troelstra — Remarks on Intuitionism and the Philosophy of Mathematics
CT-88-01 Ming Li, Paul M.B.Vitanyi — *Computation and Complexity Theory:* Two Decades of Applied Kolmogorov Complexity
CT-88-02 Michiel H.M. Smid — General Lower Bounds for the Partitioning of Range Trees
CT-88-03 Michiel H.M. Smid, Mark H. Overmars, Leen Torenvliet, Peter van Emde Boas — Maintaining Multiple Representations of Dynamic Data Structures
CT-88-04 Dick de Jongh, Lex Hendriks, Gerard R. Renardel de Lavalette — Computations in Fragments of Intuitionistic Propositional Logic
CT-88-05 Peter van Emde Boas — Machine Models and Simulations (revised version)
CT-88-06 Michiel H.M. Smid — A Data Structure for the Union-find Problem having good Single-Operation Complexity
CT-88-07 Johan van Benthem — Time, Logic and Computation
CT-88-08 Michiel H.M. Smid, Mark H. Overmars, Leen Torenvliet, Peter van Emde Boas — Multiple Representations of Dynamic Data Structures
CT-88-09 Theo M.V. Janssen — Towards a Universal Parsing Algorithm for Functional Grammar
CT-88-10 Edith Spaan, Leen Torenvliet, Peter van Emde Boas — Nondeterminism, Fairness and a Fundamental Analogy
CT-88-11 Sieger van Denneheuvel, Peter van Emde Boas — Towards implementing RL
X-88-01 Marc Jumelet — *Other prepublications:* On Solovay's Completeness Theorem

1989 LP-89-01 Johan van Benthem — *Logic, Semantics and Philosophy of Language:* The Fine-Structure of Categorial Semantics
LP-89-02 Jeroen Groenendijk, Martin Stokhof — Dynamic Predicate Logic, towards a compositional, non-representational semantics of discourse
LP-89-03 Yde Venema — Two-dimensional Modal Logics for Relation Algebras and Temporal Logic of Intervals
LP-89-04 Johan van Benthem — Language in Action
LP-89-05 Johan van Benthem — Modal Logic as a Theory of Information
LP-89-06 Andreja Prijatelj — Intensional Lambek Calculi: Theory and Application
LP-89-07 Heinrich Wansing — The Adequacy Problem for Sequential Propositional Logic
LP-89-08 Víctor Sánchez Valencia — Peirce's Propositional Logic: From Algebra to Graphs
LP-89-09 Zhisheng Huang — Dependency of Belief in Distributed Systems
ML-89-01 Dick de Jongh, Albert Visser — *Mathematical Logic and Foundations:* Explicit Fixed Points for Interpretability Logic
ML-89-02 Roel de Vrijer — Extending the Lambda Calculus with Surjective Pairing is conservative
ML-89-03 Dick de Jongh, Franco Montagna — Rosser Orderings and Free Variables
ML-89-04 Dick de Jongh, Marc Jumelet, Franco Montagna — On the Proof of Solovay's Theorem
ML-89-05 Rineke Verbrugge — Σ-completeness and Bounded Arithmetic
ML-89-06 Michiel van Lambalgen — The Axiomatization of Randomness
ML-89-07 Dirk Roorda — Elementary Inductive Definitions in HA: from Strictly Positive towards Monotone
ML-89-08 Dirk Roorda — Investigations into Classical Linear Logic
ML-89-09 Alessandra Carbone — Provable Fixed points in $I\Delta_0+\Omega_1$
CT-89-01 Michiel H.M. Smid — *Computation and Complexity Theory:* Dynamic Deferred Data Structures
CT-89-02 Peter van Emde Boas — Machine Models and Simulations
CT-89-03 Ming Li, Herman Neuféglise, Leen Torenvliet, Peter van Emde Boas — On Space Efficient Simulations
CT-89-04 Harry Buhrman, Leen Torenvliet — A Comparison of Reductions on Nondeterministic Space
CT-89-05 Pieter H. Hartel, Michiel H.M. Smid, Leen Torenvliet, Willem G. Vree — A Parallel Functional Implementation of Range Queries
CT-89-06 H.W. Lenstra, Jr. — Finding Isomorphisms between Finite Fields
CT-89-07 Ming Li, Paul M.B. Vitanyi — A Theory of Learning Simple Concepts under Simple Distributions and Average Case Complexity for the Universal Distribution (Prel. Version)
CT-89-08 Harry Buhrman, Steven Homer, Leen Torenvliet — Honest Reductions, Completeness and Nondeterminstic Complexity Classes
CT-89-09 Harry Buhrman, Edith Spaan, Leen Torenvliet — On Adaptive Resource Bounded Computations
CT-89-10 Sieger van Denneheuvel — The Rule Language RL/1
CT-89-11 Zhisheng Huang, Sieger van Denneheuvel, Peter van Emde Boas — Towards Functional Classification of Recursive Query Processing
X-89-01 Marianne Kalsbeek — *Other Prepublications:* An Orey Sentence for Predicative Arithmetic
X-89-02 G. Wagemakers — New Foundations: a Survey of Quine's Set Theory
X-89-03 A.S. Troelstra — Index of the Heyting Nachlass
X-89-04 Jeroen Groenendijk, Martin Stokhof — Dynamic Montague Grammar, a first sketch
X-89-05 Maarten de Rijke — The Modal Theory of Inequality
X-89-06 Peter van Emde Boas — Een Relationele Semantiek voor Conceptueel Modelleren: Het RL-project

1990 SEE INSIDE BACK COVER



Instituut voor Taal, Logica en Informatie
Institute for Language, Logic and Information

Faculteit der Wiskunde en Informatica
(Department of Mathematics and Computer Science)
Plantage Muidergracht 24
1018TV Amsterdam

Faculteit der Wijsbegeerte
(Department of Philosophy)
Nieuwe Doelenstraat 15
1012CP Amsterdam

QUASI-INJECTIVE REDUCTIONS

Lane A. Hemachandra
Department of Computer Science
University of Rochester
Edith Spaan
Department of Mathematics and Computer Science
University of Amsterdam

ITLI Prepublication Series
for Computation and Complexity Theory
ISSN 0924-8374

Received August 1991

Quasi-Injective Reductions

Lane A. Hemachandra[*]
Department of Computer Science
University of Rochester
Rochester, NY 14627

Edith Spaan[†]
Faculteit der Wiskunde en Informatica
Universiteit van Amsterdam
Plantage Muidergracht 24
1018 TV Amsterdam

July 24, 1991

Abstract

A reduction is said to be quasi-injective if no element of the range is mapped to by infinitely many elements. Via two natural families of quasi-injective reductions, we study the connection between degree of injectivity and strength of reduction. In particular, we completely determine the relative strengths of polynomial-time $f(n)$-$\widehat{\text{to}}$-1 reductions, and of polynomial-time k-to-k' reductions.

1 Introduction

A many-one reduction may, in general, map infinitely many domain elements to the same range element. A one-to-one reduction (often referred to as an *injective* reduction) maps at most one domain element to a given element of the co-domain. In some settings, these different degrees of injectivity coincide; a famous example is provided by the Myhill Isomorphism Theorem (see, e.g., [Soa87]), which implies that all sets $\leq_m$-complete for the r.e. sets are indeed $\leq_{\text{1-to-1}}$-complete for the r.e. sets. In some other settings, it is not known whether differing degrees of injectivity coincide; the question of whether $\leq^p_m$-completeness and $\leq^p_{\text{1-to-1}}$-completeness coincide for NP remains a central unresolved problem, and is a weaker version of the Berman-Hartmanis Isomorphism Conjecture ([BH77], see also the survey [You90]). In this paper, we study the extent to which lack of injectivity gives power to polynomial-time reductions.

[*]Research supported in part by the National Science Foundation under grant CCR-8957604.
[†]Research supported in part by the NWO under grant SIR 13-785.

We focus on what we will call quasi-injective reductions—reductions that map at most a finite number of domain elements to a given element in their range. In particular, we study $f(n)$-$\widehat{\text{to}}$-1 reductions[1] and k-to-k' reductions. We observe that an $f(n)$-$\widehat{\text{to}}$-1 reduction is more powerful than a $g(n)$-$\widehat{\text{to}}$-1 reduction exactly when $f(n)$ is greater than $g(n)$ infinitely often. However, this result is definition-sensitive; it fails for $f(n)$-to-1 reductions. For the case of k-to-k' reductions—reductions for which no k' elements of the range are mapped to by more than k domain elements—we completely characterize when a c-to-d reduction is more powerful than an a-to-b reduction, namely when:

$$\left(\left\lfloor\frac{a}{b}\right\rfloor < \left\lfloor\frac{c}{d}\right\rfloor\right) \vee \left[\left(\left\lfloor\frac{a}{b}\right\rfloor = \left\lfloor\frac{c}{d}\right\rfloor\right) \wedge \left(a - b\left\lfloor\frac{a}{b}\right\rfloor < c - d\left\lfloor\frac{a}{b}\right\rfloor\right)\right].$$

2 Preliminaries

Σ will represent any fixed finite alphabet. Our reductions will in general be from Σ^* to Σ^*. However, at times we will use $\mathcal{N}$ instead of Σ^*, implicitly taking advantage of the standard nice correspondence between these two sets. Let $|x|$ denote the length of string x, and let $||S||$ denote the cardinality of set S. We will use the quantification symbol $(\exists_\infty x)$ to indicate "there exist infinitely many distinct x."

Let FP denote the class of total functions computable in polynomial time. We will usually assume that such functions map from Σ^* to Σ^* (equivalently $\mathcal{N} \to \mathcal{N}$). However, in certain cases we will allow more flexible co-domains (such as $\Sigma^* \bigcup \{\text{YES}, \text{NO}\}$).

Recall the standard definition of many-one reductions: $A \leq_m^p B$ if there is a function $h \in \text{FP}$ such that $(\forall x \in \Sigma^*)[x \in A \iff h(x) \in B]$ [HU79]. We will call a finite-to-one reduction quasi-injective.

Definition 2.1 We will say that $h \in \text{FP}$ is *quasi-injective* if $(\forall y \in \Sigma^*)[\{x \in \Sigma^* \mid h(x) = y\}$ is a finite set].

Definitions 2.2 and 2.3 present the families of quasi-injective reductions that we will study.

Definition 2.2 We say that $A \leq_{f(n)\text{-to-}1}^p B$ if $A \leq_m^p B$ via a reduction $h \in \text{FP}$ satisfying $(\forall y \in \Sigma^*)[||\{x \in \Sigma^* \mid h(x) = y\}|| \leq f(|y|)]$.

Definition 2.3 We say that $A \leq_{k\text{-to-}k'}^p B$ if $A \leq_m^p B$ via a reduction $h \in \text{FP}$ satisfying $(\forall S \subseteq \Sigma^*)[||S|| \leq k' \Rightarrow ||\{x \in \Sigma^* \mid h(x) \in S\}|| \leq k]$.

[1]The hat indicates reductions that can simply state acceptance or rejection ([AS87], see also [DGHM89]). This paper will also discuss the structure of reductions that lack this ability.

In Definition 2.2, the special case $f(n) = 1$ ($\leq^p_{\text{1-to-1}}$ reducibility) has been extensively studied, and is related to issues of isomorphism, one-way functions, and cryptography [BH77,GS88,KMR90,You90]. In Definition 2.2, the special case $f(n) = n^{\mathcal{O}(1)}$ (polynomial-time polynomial-to-one reducibility) has been studied by Allender and Rubinstein, who related this notion to the P = FewP question [AR88].

Unfortunately, the standard definition of many-one reductions gives problems in certain settings. For example, $\Sigma^* \not\leq^p_m \emptyset$, though both sets are computationally trivial. More generally, a many-one reduction from A to B may "know" whether its input is a member of A, but may not be able to find an appropriate string (in B or $\overline{B}$) to map to. Ambos-Spies proposed dealing with this by allowing a many-one reduction from A to B to either reduce a given input to an appropriate output, or to directly proclaim whether its input is in A [AS87,DGHM89]. This is reflected in the definition below.

Definition 2.4

1. **[AS87]** We say that $A \leq^p_{\widehat{m}} B$ if there is a a reduction $h : \Sigma^* \to \Sigma^* \bigcup \{\text{YES}, \text{NO}\}$, $h \in \text{FP}$, satisfying $(\forall x \in \Sigma^*)[(h(x) = \text{YES} \Rightarrow x \in A) \wedge (h(x) = \text{NO} \Rightarrow x \notin A) \wedge (h(x) \in \Sigma^* \Rightarrow (h(x) \in B \iff x \in A))]$, where YES and NO are symbols not in Σ.

2. We say that $A \leq^p_{f(n)\text{-}\widehat{\text{to}}\text{-1}} B$ if $A \leq^p_{\widehat{m}} B$ via a reduction $h : \Sigma^* \to \Sigma^* \bigcup \{\text{YES}, \text{NO}\}$, $h \in \text{FP}$, satisfying $(\forall y \in \Sigma^*)[||\{x \in \Sigma^* \mid h(x) = y\}|| \leq f(|y|)]$.

Note that, in the latter part of the above definition, those strings x for which $h(x) \in \{\text{YES}, \text{NO}\}$ do not "count against" the injectivity restriction.

At times, we will want to argue that there are maps from A to B with certain quasi-injectivity properties, but that no such map can be computed quickly. The following notion will be useful; it should be compared with Goldsmith's related notion of sets to which both Σ^* and $\emptyset$ (and thus *every* set) reduce via reductions that are at most polynomially length-increasing (see [Gol89, Lemma 2.2.2]).

Definition 2.5

1. We say that $A \leq^{\textit{poly-length}}_{f(n)\text{-to-1}} B$ if there exist a function h and polynomial p satisfying:

   (a) $(\forall x \in \Sigma^*)[(x \in A \iff h(x) \in B) \wedge |h(x)| \leq p(|x|)]$ and

   (b) $(\forall y \in \Sigma^*)[||\{x \in \Sigma^* \mid h(x) = y\}|| \leq f(|y|)]$.

2. We say that $A \leq^{\textit{poly-length}}_{k\text{-to-}k'} B$ if there exist a function h and polynomial p satisfying:

   (a) $(\forall x \in \Sigma^*)[(x \in A \iff h(x) \in B) \wedge |h(x)| \leq p(|x|)]$ and

(b) $(\forall S \subseteq \Sigma^*)[||S|| \leq k' \Rightarrow ||\{x \in \Sigma^* \mid h(x) \in S\}|| \leq k]$.

As a final introductory note, we stress that we are comparing reductions between sets. If one looks at reductions of sets to classes, non-injective reductions can often be made injective. For example, it is easy to see the following, since if $A \in \mathrm{R}^p_{(n\mathcal{O}(1))\text{-to-}1}(\mathrm{SPARSE})$,[2] as certified by reduction f and sparse set S, then A is polynomial-time equivalent to the sparse set $\{\langle x, y\rangle \mid f(x) = y \wedge y \in S\}$.

Observation 2.6 $\mathrm{R}^p_{(n\mathcal{O}(1))\text{-to-}1}(\mathrm{SPARSE}) = \mathrm{R}^p_{1\text{-to-}1}(\mathrm{SPARSE}) \subseteq \mathrm{E}^p_{(n\mathcal{O}(1))\text{-}\widehat{\text{to}}\text{-}1}(\mathrm{SPARSE}) = \mathrm{E}^p_{1\text{-}\widehat{\text{to}}\text{-}1}(\mathrm{SPARSE})$.

3 Results

We first look at finite-to-one reductions, and then turn to the study of k-to-k' reductions. The following theorem completely characterizes whether $f(n)$-$\widehat{\text{to}}$-1 reducibility is more powerful than $g(n)$-$\widehat{\text{to}}$-1 reducibility.

Theorem 3.1 Let $f, g \in \mathrm{FP}$, $f, g : \mathcal{N} \to \mathcal{N}$.

$$(\exists_\infty n)[f(n) > g(n)]$$

$$\Longleftrightarrow$$

$$(\exists A, B)[A \leq^p_{f(n)\text{-}\widehat{\text{to}}\text{-}1} B \ \wedge \ A \not\leq^p_{g(n)\text{-}\widehat{\text{to}}\text{-}1} B].$$

The left to right direction of Theorem 3.1 also holds for the case of $f(n)$-to-1 reductions. However, to make the theorem non-trivial (e.g., to ban separating 2-to-1 reductions from 1-to-1 reductions via sets A and B with $||A|| = 2$ and $||B|| = 1$), we must note that the sets witnessing $A \not\leq^p_{g(n)\text{-to-}1} B$ also have the property that A plausibly might reduce to B: $A \leq^{\textit{poly-length}}_{g(n)\text{-to-}1} B$.

Theorem 3.2 Let $f, g \in \mathrm{FP}$, $f, g : \mathcal{N} \to \mathcal{N}$. If $(\exists_\infty n)[f(n) > g(n)]$, then $(\exists A, B)[A \leq^p_{f(n)\text{-to-}1} B$ and $A \leq^{\textit{poly-length}}_{g(n)\text{-to-}1} B$, yet $A \not\leq^p_{g(n)\text{-to-}1} B]$.

[2]Notation: SPARSE denotes the class of sparse sets. A set S is said to be *sparse* if there is a polynomial p such that $(\forall n)[||\{x \mid |x| = n \wedge x \in S\}|| \leq p(n)]$. $\mathrm{R}^p_\tau(\mathcal{C}) = \{L \mid (\exists A \in \mathcal{C})[L \leq^p_\tau A]\}$; we'll also use the notation $\mathrm{E}^p_\tau(\mathcal{C}) = \{L \mid (\exists A \in \mathcal{C})[L \leq^p_\tau A \ \wedge \ A \leq^p_\tau L]\}$. For discussion of reductions and equivalence to sparse sets, see [BK88,GW91,AH,AHOW,TB].

Theorems 3.1 and 3.2 are proven by direct diagonalizations, and are omitted. Though Theorem 3.2 shows that one direction of Theorem 3.1 holds for $f(n)$-to-1 reductions, the same claim cannot be made for the other direction.

Theorem 3.3 There are functions f, $g \in \mathrm{FP}$, $f, g : \mathcal{N} \to \mathcal{N}$, and sets A and B such that:

1. $f(n) \leq g(n)$ almost everywhere,
2. $A \leq^{p}_{f(n)\text{-to-}1} B$, and
3. $A \leq^{\textit{poly-length}}_{g(n)\text{-to-}1} B$, yet
4. $A \not\leq^{p}_{g(n)\text{-to-}1} B$.

The proof of Theorem 3.3 is a simplified version of the proof of Theorem 3.4, and thus is omitted. However, it should be noted that the counter-example described in the above theorem can be easily taken to be the case where $f(0) = 2$, $g(0) = 1$, and $(\forall n \geq 1)[f(n) = g(n) = 1]$.

Now we turn to our second family of quasi-injective reductions—k-to-k' reductions. We will refer to $\left\lfloor \frac{k}{k'} \right\rfloor$ as the *base* of the k-to-k' reduction, and $k - k'\left\lfloor \frac{k}{k'} \right\rfloor$ as the *excess* of the reduction. Intuitively, the base indicates the level of non-injectivity that can be tolerated infinitely often, and the excess indicates a cap on the total amount of non-injectivity beyond the base level. As an example, a 4-to-2 reduction can be (at most) 2-to-1 everywhere, or it can be (at most) 3-to-1 on one range point and (at most) 1-to-1 elsewhere.

For k-to-k' reductions with large values of k and k', the range of possibilities expands dramatically. Nonetheless, the notions of base and excess offer a complete characterization of the relative strength of k-to-k' reductions. In the sense made formal by Theorem 3.4, a c-to-d reduction is more flexible than an a-to-b reduction exactly when the former has a larger base, or, in the case of identical bases, when the former has a larger excess.

Theorem 3.4 Let $a, b, c, d \in \{1, 2, 3, \ldots\}$, $c \geq d$, $a \geq b$.

$$\left(\left\lfloor \frac{a}{b} \right\rfloor < \left\lfloor \frac{c}{d} \right\rfloor\right) \vee \left[\left(\left\lfloor \frac{a}{b} \right\rfloor = \left\lfloor \frac{c}{d} \right\rfloor\right) \wedge \left(a - b\left\lfloor \frac{a}{b} \right\rfloor < c - d\left\lfloor \frac{a}{b} \right\rfloor\right)\right]$$

$$\Longleftrightarrow$$

$$(\exists A, B)[A \leq^{p}_{c\text{-to-}d} B \text{ and } A \leq^{\textit{poly-length}}_{a\text{-to-}b} B, \text{ yet } A \not\leq^{p}_{a\text{-to-}b} B].$$

Indeed, in the case where $(\lfloor \frac{a}{b} \rfloor < \lfloor \frac{c}{d} \rfloor) \vee [(\lfloor \frac{a}{b} \rfloor = \lfloor \frac{c}{d} \rfloor) \wedge (a - b\lfloor \frac{a}{b} \rfloor < c - d\lfloor \frac{a}{b} \rfloor)]$ does not hold, it follows that $(\forall A, B : B \text{ and } \overline{B} \text{ are infinite})\,[A \leq^{p}_{c\text{-to-}d} B \Rightarrow A \leq^{p}_{a\text{-to-}b} B]$.

Before proving Theorem 3.4, we state and prove a useful lemma.

Lemma 3.5 If g is an a-to-b reduction and $||S|| \geq b$, then $||g^{-1}(S)|| \leq a + (||S|| - b)\lfloor \frac{a}{b} \rfloor$.

Proof of Lemma 3.5

Let S' be a subset of S of size b such that $(\forall m \in S')(\forall m' \in S - S')[||g^{-1}(m)|| \geq ||g^{-1}(m')||]$. Since $||g^{-1}(S')|| \leq a$, there is an element m of S' such that $||g^{-1}(m)|| \leq \lfloor \frac{a}{b} \rfloor$. So $||g^{-1}(m')|| \leq \lfloor \frac{a}{b} \rfloor$ for all $m' \in S - S'$. It follows that $||g^{-1}(S)|| = ||g^{-1}(S')|| + ||g^{-1}(S - S')|| \leq a + (||S|| - b)\lfloor \frac{a}{b} \rfloor$. ∎

Proof of Theorem 3.4

($\Rightarrow$) Suppose $(\lfloor \frac{a}{b} \rfloor < \lfloor \frac{c}{d} \rfloor) \vee [(\lfloor \frac{a}{b} \rfloor = \lfloor \frac{c}{d} \rfloor) \wedge (a - b\lfloor \frac{a}{b} \rfloor < c - d\lfloor \frac{a}{b} \rfloor)]$. It follows immediately that there is an $m_0 \geq b$ such that $a + (m_0 - b)\lfloor \frac{a}{b} \rfloor < c + (m_0 - d)\lfloor \frac{c}{d} \rfloor$. Let $f : \mathcal{N} \to \mathcal{N}$ satisfy:

- $n \leq n' \Rightarrow f(n) \leq f(n')$,
- $||f^{-1}(0)|| = c + (1 - d)\lfloor \frac{c}{d} \rfloor$,
- $||f^{-1}(m)|| = \lfloor \frac{c}{d} \rfloor$ for $1 \leq m < m_0$, and
- $||f^{-1}(m)|| = \lfloor \frac{a}{b} \rfloor$ for $m \geq m_0$.

Clearly, f is uniquely defined and is computable in time polynomial in the size of its input. Since $\lfloor \frac{a}{b} \rfloor \leq \lfloor \frac{c}{d} \rfloor \leq c + (1 - d)\lfloor \frac{c}{d} \rfloor$, for any set S of size d it holds that $||f^{-1}(S)|| \leq c + (1 - d)\lfloor \frac{c}{d} \rfloor + (d - 1)\lfloor \frac{c}{d} \rfloor = c$. Thus, for any set B, $f^{-1}(B) \leq^p_{c\text{-to-}d} B$, as certified by polynomial-time reduction f. We will construct $B = \bigcup_{i \geq 0} B_i$ in stages so that $f^{-1}(B) \not\leq^p_{a\text{-to-}b} B$, and $f^{-1}(B) \leq^{poly\text{-}length}_{a\text{-to-}b} B$. Let $\sigma_1, \sigma_2, \cdots$ be an enumeration of all polynomial-time a-to-b reductions.[3]

Stage 0: Set $B_0 = \{0, \ldots, m_0\}$.

Stage i: Let m be the largest element of B_{i-1}.
Choose n such that $f(n) \in B_{i-1}$ and $\sigma_i(n) \notin B_{i-1}$.
If $\sigma_i(n) > m$ then set $B_i = B_{i-1} \cup \{\sigma_i(n) + 1\} \cup \{j \mid m + 1 \leq j \leq \sigma_i(n) - 1\}$,
else set $B_i = B_{i-1}$.

If n can be chosen as described above, then $f^{-1}(B) \not\leq^p_{a\text{-to-}b} B$. Furthermore, $f^{-1}(B) \leq^{poly\text{-}length}_{a\text{-to-}b} B$, by the recursive reduction that is identical to f on elements not in $f^{-1}(B)$,[4] and that maps the nth element of $f^{-1}(B)$ to the $(n/\lfloor \frac{a}{b} \rfloor)$th element of B. This

[3] One can construct a list of exponential-time machines that enumerate the $\leq^p_{a\text{-to-}b}$ reductions. Thus, this step is effective; it is not hard to see that the sets B and $f^{-1}(B)$ will be recursive.

[4] Note that all such elements are greater than m_0.

reduction is *poly-length*, since f is $\lfloor \frac{a}{b} \rfloor$-to-1 almost everywhere, and no two consecutive elements are in $\overline{B}$.

To prove that n can be chosen as specified above, it suffices to show that for all $i \geq 1$, $||\sigma_i^{-1}(B_{i-1})|| < ||f^{-1}(B_{i-1})||$. Since $||B_{i-1}|| \geq m_0 \geq b$, it follows from Lemma 3.5 and our choice of m_0 that:

$$\begin{aligned} ||\sigma_i^{-1}(B_{i-1})|| &\leq a + (||B_{i-1}|| - b)\lfloor \tfrac{a}{b} \rfloor \\ &= a + (m_0 - b)\lfloor \tfrac{a}{b} \rfloor + (||B_{i-1}|| - m_0)\lfloor \tfrac{a}{b} \rfloor \\ &< c + (m_0 - d)\lfloor \tfrac{c}{d} \rfloor + (||B_{i-1}|| - m_0)\lfloor \tfrac{a}{b} \rfloor \\ &= ||f^{-1}(B_{i-1})||. \end{aligned}$$

($\Leftarrow$) Suppose $(\lfloor \frac{a}{b} \rfloor > \lfloor \frac{c}{d} \rfloor) \vee [(\lfloor \frac{a}{b} \rfloor = \lfloor \frac{c}{d} \rfloor) \wedge (a - b\lfloor \frac{a}{b} \rfloor \geq c - d\lfloor \frac{a}{b} \rfloor)]$. We will prove that $(\forall A, B : B \text{ and } \overline{B} \text{ are infinite})\, [A \leq^p_{c\text{-to-}d} B \Rightarrow A \leq^p_{a\text{-to-}b} B]$. This proves the theorem, since for any sets A and B, if $A \not\leq^p_{a\text{-to-}b} B$ and $A \leq^{poly\text{-}length}_{a\text{-to-}b} B$, then B and $\overline{B}$ are infinite.

Suppose $A \leq^p_{c\text{-to-}d} B$ via reduction f, B and $\overline{B}$ are infinite, and f is not a-to-b. Since f is $\lfloor \frac{c}{d} \rfloor$-to-1 (and therefore $\lfloor \frac{a}{b} \rfloor$-to-1) almost everywhere and finite-to-one everywhere, there exists a finite set X such that $(\forall m \in \mathcal{N})[||f^{-1}(m) - X|| \leq \lfloor \frac{a}{b} \rfloor]$. To transform f to an $\lfloor \frac{a}{b} \rfloor$-to-1 reduction from A to B, we need only change f on the (finite number of) elements in X. Since B and $\overline{B}$ are both infinite, it suffices to show that f is $(\lfloor \frac{a}{b} \rfloor - 1)$-to-1 almost everywhere.

This clearly is the case when $\lfloor \frac{a}{b} \rfloor > \lfloor \frac{c}{d} \rfloor$. In the case where $(\lfloor \frac{a}{b} \rfloor = \lfloor \frac{c}{d} \rfloor) \wedge (a - b\lfloor \frac{a}{b} \rfloor \geq c - d\lfloor \frac{a}{b} \rfloor)$ and $b < d$, let Y be such that $||Y|| = b$ and $||f^{-1}(Y)|| > a$. If—as will be the case if f is not $(\lfloor \frac{a}{b} \rfloor - 1)$-to-1 almost everywhere—for infinitely many m it holds that $||f^{-1}(m)|| \geq \lfloor \frac{a}{b} \rfloor$, then there exists a set $Y' \supsetneq Y$ such that $||Y'|| = d$ and $c \geq ||f^{-1}(Y')|| > a + (d - b)\lfloor \frac{a}{b} \rfloor$. Then $c - d\lfloor \frac{a}{b} \rfloor > a - b\lfloor \frac{a}{b} \rfloor$, which contradicts our assumptions. Therefore, in this case f is $(\lfloor \frac{a}{b} \rfloor - 1)$-to-1 almost everywhere, as desired. In the final case, $(\lfloor \frac{a}{b} \rfloor = \lfloor \frac{c}{d} \rfloor) \wedge (a - b\lfloor \frac{a}{b} \rfloor \geq c - d\lfloor \frac{a}{b} \rfloor)$ and $b \geq d$. In this case, f is already an a-to-b reduction, since by Lemma 3.5, for any subset Y of size b, $||f^{-1}(Y)|| \leq c + (b - d)\lfloor \frac{c}{d} \rfloor \leq a$. This contradicts our assumption that f is not a-to-b. ∎

Acknowledgments

We thank William Gasarch and Yenjo Han for helpful conversations and comments.

References

[AH] E. Allender and L. Hemachandra. Lower bounds for the low hierarchy. *Journal of the ACM.* To appear.

[AHOW] E. Allender, L. Hemachandra, M. Ogiwara, and O. Watanabe. Relating equivalence and reducibility to sparse sets. *SIAM Journal on Computing.* To appear.

[AR88] E. Allender and R. Rubinstein. P-printable sets. *SIAM Journal on Computing*, 17(6):1193–1202, 1988.

[AS87] K. Ambos-Spies. Honest polynomial reducibilities, recursively enumerable sets, and the P = ?NP problem. In *Proceedings of the 2nd Structure in Complexity Theory Conference*, pages 60–68. IEEE Computer Society Press, June 1987.

[BH77] L. Berman and J. Hartmanis. On isomorphisms and density of NP and other complete sets. *SIAM Journal on Computing*, 6(2):305–322, 1977.

[BK88] R. Book and K. Ko. On sets truth-table reducible to sparse sets. *SIAM Journal on Computing*, 17(5):903–919, 1988.

[DGHM89] R. Downey, W. Gasarch, S. Homer, and M. Moses. On honest polynomial reductions, relativizations, and P = NP. In *Proceedings of the 4th Structure in Complexity Theory Conference*, pages 3–14. IEEE Computer Society Press, June 1989.

[Gol89] J. Goldsmith. *Polynomial Isomorphisms and Near-Testable Sets.* PhD thesis, University of Wisconsin–Madison, Madison, WI, January 1989. Available as Technical Report 816.

[GS88] J. Grollmann and A. Selman. Complexity measures for public-key cryptosystems. *SIAM Journal on Computing*, 17:309–335, 1988.

[GW91] R. Gavaldà and O. Watanabe. On the computational complexity of small descriptions. In *Proceedings of the 6th Structure in Complexity Theory Conference*, pages 89–101. IEEE Computer Society Press, June/July 1991.

[HU79] J. Hopcroft and J. Ullman. *Introduction to Automata Theory, Languages, and Computation.* Addison-Wesley, 1979.

[KMR90] S. Kurtz, S. Mahaney, and J. Royer. The structure of complete degrees. In A. Selman, editor, *Complexity Theory Retrospective*, pages 108–146. Springer-Verlag, 1990.

[Soa87] R. Soare. *Recursively Enumerable Sets and Degrees: A Study of Computable Functions and Computably Generated Sets.* Perspectives in Mathematical Logic. Springer-Verlag, 1987.

[TB] S. Tang and R. Book. Reducibilities on tally and sparse sets. *Theoretical Informatics and Applications (RAIRO).* To appear. Preliminary version appears in *ICALP '88.*

[You90] P. Young. Juris Hartmanis: Fundamental contributions to isomorphism problems. In A. Selman, editor, *Complexity Theory Retrospective*, pages 28–58. Springer-Verlag, 1990.

The ITLI Prepublication Series

1990 *Logic, Semantics and Philosophy of Language*

LP-90-01 Jaap van der Does — A Generalized Quantifier Logic for Naked Infinitives
LP-90-02 Jeroen Groenendijk, Martin Stokhof — Dynamic Montague Grammar
LP-90-03 Renate Bartsch — Concept Formation and Concept Composition
LP-90-04 Aarne Ranta — Intuitionistic Categorial Grammar
LP-90-05 Patrick Blackburn — Nominal Tense Logic
LP-90-06 Gennaro Chierchia — The Variablity of Impersonal Subjects
LP-90-07 Gennaro Chierchia — Anaphora and Dynamic Logic
LP-90-08 Herman Hendriks — Flexible Montague Grammar
LP-90-09 Paul Dekker — The Scope of Negation in Discourse, towards a flexible dynamic Montague grammar
LP-90-10 Theo M.V. Janssen — Models for Discourse Markers
LP-90-11 Johan van Benthem — General Dynamics
LP-90-12 Serge Lapierre — A Functional Partial Semantics for Intensional Logic
LP-90-13 Zhisheng Huang — Logics for Belief Dependence
LP-90-14 Jeroen Groenendijk, Martin Stokhof — Two Theories of Dynamic Semantics
LP-90-15 Maarten de Rijke — The Modal Logic of Inequality
LP-90-16 Zhisheng Huang, Karen Kwast — Awareness, Negation and Logical Omniscience
LP-90-17 Paul Dekker — Existential Disclosure, Implicit Arguments in Dynamic Semantics

Mathematical Logic and Foundations

ML-90-01 Harold Schellinx — Isomorphisms and Non-Isomorphisms of Graph Models
ML-90-02 Jaap van Oosten — A Semantical Proof of De Jongh's Theorem
ML-90-03 Yde Venema — Relational Games
ML-90-04 Maarten de Rijke — Unary Interpretability Logic
ML-90-05 Domenico Zambella — Sequences with Simple Initial Segments
ML-90-06 Jaap van Oosten — Extension of Lifschitz' Realizability to Higher Order Arithmetic, and a Solution to a Problem of F. Richman
ML-90-07 Maarten de Rijke — A Note on the Interpretability Logic of Finitely Axiomatized Theories
ML-90-08 Harold Schellinx — Some Syntactical Observations on Linear Logic
ML-90-09 Dick de Jongh, Duccio Pianigiani — Solution of a Problem of David Guaspari
ML-90-10 Michiel van Lambalgen — Randomness in Set Theory
ML-90-11 Paul C. Gilmore — The Consistency of an Extended NaDSet

Computation and Complexity Theory

CT-90-01 John Tromp, Peter van Emde Boas — Associative Storage Modification Machines
CT-90-02 Sieger van Denneheuvel, Gerard R. Renardel de Lavalette — A Normal Form for PCSJ Expressions
CT-90-03 Ricard Gavaldà, Leen Torenvliet, Osamu Watanabe, José L. Balcázar — Generalized Kolmogorov Complexity in Relativized Separations
CT-90-04 Harry Buhrman, Edith Spaan, Leen Torenvliet — Bounded Reductions
CT-90-05 Sieger van Denneheuvel, Karen Kwast — Efficient Normalization of Database and Constraint Expressions
CT-90-06 Michiel Smid, Peter van Emde Boas — Dynamic Data Structures on Multiple Storage Media, a Tutorial
CT-90-07 Kees Doets — Greatest Fixed Points of Logic Programs
CT-90-08 Fred de Geus, Ernest Rotterdam, Sieger van Denneheuvel, Peter van Emde Boas — Physiological Modelling using RL
CT-90-09 Roel de Vrijer — Unique Normal Forms for Combinatory Logic with Parallel Conditional, a case study in conditional rewriting

Other Prepublications

X-90-01 A.S. Troelstra — Remarks on Intuitionism and the Philosophy of Mathematics, Revised Version
X-90-02 Maarten de Rijke — Some Chapters on Interpretability Logic
X-90-03 L.D. Beklemishev — On the Complexity of Arithmetical Interpretations of Modal Formulae
X-90-04 — Annual Report 1989
X-90-05 Valentin Shehtman — Derived Sets in Euclidean Spaces and Modal Logic
X-90-06 Valentin Goranko, Solomon Passy — Using the Universal Modality: Gains and Questions
X-90-07 V.Yu. Shavrukov — The Lindenbaum Fixed Point Algebra is Undecidable
X-90-08 L.D. Beklemishev — Provability Logics for Natural Turing Progressions of Arithmetical Theories
X-90-09 V.Yu. Shavrukov — On Rosser's Provability Predicate
X-90-10 Sieger van Denneheuvel, Peter van Emde Boas — An Overview of the Rule Language RL/1
X-90-11 Alessandra Carbone — Provable Fixed points in $I\Delta_0+\Omega_1$, revised version
X-90-12 Maarten de Rijke — Bi-Unary Interpretability Logic
X-90-13 K.N. Ignatiev — Dzhaparidze's Polymodal Logic: Arithmetical Completeness, Fixed Point Property, Craig's Property
X-90-14 L.A. Chagrova — Undecidable Problems in Correspondence Theory
X-90-15 A.S. Troelstra — Lectures on Linear Logic

1991 *Logic, Semantics and Philosophy of Langauge*

LP-91-01 Wiebe van der Hoek, Maarten de Rijke — Generalized Quantifiers and Modal Logic
LP-91-02 Frank Veltman — Defaults in Update Semantics
LP-91-03 Willem Groeneveld — Dynamic Semantics and Circular Propositions

Mathematical Logic and Foundations

ML-91-01 Yde Venema — Cylindric Modal Logic
ML-91-02 Alessandro Berarducci, Rineke Verbrugge — On the Metamathematics of Weak Theories
ML-91-03 Domenico Zambella — On the Proofs of Arithmetical Completeness for Interpretability Logic
ML-91-04 Raymond Hoofman, Harold Schellinx — Collapsing Graph Models by Preorders
ML-91-05 A.S. Troelstra — History of Constructivism in the Twentieth Century
ML-91-06 Inge Bethke — Finite Type Structures within Combinatory Algebras
ML-91-07 Yde Venema — Modal Derivation Rules
ML-91-08 Inge Bethke — Going Stable in Graph Models

Computation and Complexity Theory

CT-91-01 Ming Li, Paul M.B. Vitányi — Kolmogorov Complexity Arguments in Combinatorics
CT-91-02 Ming Li, John Tromp, Paul M.B. Vitányi — How to Share Concurrent Wait-Free Variables
CT-91-03 Ming Li, Paul M.B. Vitányi — Average Case Complexity under the Universal Distribution Equals Worst Case Complexity
CT-91-04 Sieger van Denneheuvel, Karen Kwast — Weak Equivalence
CT-91-05 Sieger van Denneheuvel, Karen Kwast — Weak Equivalence for Constraint Sets
CT-91-06 Edith Spaan — Census Techniques on Relativized Space Classes
CT-91-07 Karen L. Kwast — The Incomplete Database
CT-91-08 Kees Doets — Levationis Laus
CT-91-09 Ming Li, Paul M.B. Vitányi — Combinatorial Properties of Finite Sequences with high Kolmogorov Complexity
CT-91-10 John Tromp, Paul Vitányi — A Randomized Algorithm for Two-Process Wait-Free Test-and-Set
CT-91-11 Lane A. Hemachandra, Edith Spaan — Quasi-Injective Reductions

Other Prepublications

X-91-01 Alexander Chagrov, Michael Zakharyaschev — The Disjunction Property of Intermediate Propositional Logics
X-91-02 Alexander Chagrov, Michael Zakharyaschev — On the Undecidability of the Disjunction Property of Intermediate Propositional Logics
X-91-03 V. Yu. Shavrukov — Subalgebras of Diagonizable Algebras of Theories containing Arithmetic
X-91-04 K.N. Ignatiev — Partial Conservativity and Modal Logics
X-91-05 Johan van Benthem — Temporal Logic
X-91-06 — Annual Report 1990
X-91-07 A.S. Troelstra — Lectures on Linear Logic, Errata and Supplement
X-91-08 Giorgie Dzhaparidze — Logic of Tolerance
X-91-09 L.D. Beklemishev — On Bimodal Provability Logics for Π_1-axiomatized Extensions of Arithmetical Theories
X-91-10 Michiel van Lambalgen — Independence, Randomness and the Axiom of Choice
X-91-11 Michael Zakharyaschev — Canonical Formulas for K4. Part I: Basic Results
X-91-12 Herman Hendriks — Flexibele Categoriale Syntaxis en Semantiek: de proefschriften van Frans Zwarts en Michael Moortgat
X-91-13 Max I. Kanovich — The Multaplicative Fragment of Linear Logic is NP-Complete