Gaps, Ambiguity, and Establishing Complexity-Class Containments via Iterative Constant-Setting

Lane A. Hemaspaandra
Department of Computer Science, University of Rochester, Rochester, NY, USA

Mandar Juvekar
Department of Computer Science, University of Rochester, Rochester, NY, USA

Arian Nadjimzadah
Department of Computer Science, University of Rochester, Rochester, NY, USA

Patrick A. Phillips
Riverside Research, Arlington, VA, USA

Abstract

Cai and Hemachandra used iterative constant-setting to prove that Few $\subseteq \oplus$P (and thus that FewP $\subseteq \oplus$P). In this paper, we note that there is a tension between the nondeterministic ambiguity of the class one is seeking to capture, and the density (or, to be more precise, the needed "nongappy"-ness) of the easy-to-find "targets" used in iterative constant-setting. In particular, we show that even less restrictive gap-size upper bounds regarding the targets allow one to capture ambiguity-limited classes. Through a flexible, metatheorem-based approach, we do so for a wide range of classes including the logarithmic-ambiguity version of Valiant's unambiguous nondeterminism class UP. Our work lowers the bar for what advances regarding the existence of infinite, P-printable sets of primes would suffice to show that restricted counting classes based on the primes have the power to accept superconstant-ambiguity analogues of UP. As an application of our work, we prove that the Lenstra–Pomerance–Wagstaff Conjecture implies that all $\mathcal{O}(\log \log n)$-ambiguity NP sets are in the restricted counting class $\mathrm{RC}_{\mathrm{PRIMES}}$.

2012 ACM Subject Classification Theory of computation → Complexity classes

Keywords and phrases structural complexity theory, computational complexity theory, ambiguity-limited NP, counting classes, P-printable sets

Digital Object Identifier 10.4230/LIPIcs.MFCS.2022.57

Funding Work supported in part by NSF Grant CCF-2006496.

Acknowledgements We thank B. Carleton, H. Welles, and the anonymous referees.

1 Introduction

We show that every NP set of low ambiguity belongs to broad collections of restricted counting classes.

We now describe the two types of complexity classes just mentioned. For any set $S \subseteq \mathbb{N}^+$, the restricted counting class RC_S [7] is defined by $\mathrm{RC}_S = \{L \mid (\exists f \in \#\mathrm{P})(\forall x \in \Sigma^*)[(x \notin L \implies f(x) = 0) \wedge (x \in L \implies f(x) \in S)]\}$. That is, a set L is in RC_S exactly if there is a nondeterministic polynomial-time Turing machine (NPTM) that on each string not in L has zero accepting paths and on each string in L has a number of accepting paths that belongs to the set S. For example, though this is an extreme case, $\mathrm{NP} = \mathrm{RC}_{\mathbb{N}^+}$.

In the 1970s, Valiant started the study of ambiguity-limited versions of NP by introducing the class UP [36], unambiguous polynomial time, which in the above notation is simply $\mathrm{RC}_{\{1\}}$. (The ambiguity (limit) of an NPTM refers to an upper bound on how many *accepting*

47th International Symposium on Mathematical Foundations of Computer Science (MFCS 2022).
Editors: Stefan Szeider, Robert Ganian, and Alexandra Silva; Article No. 57; pp. 57:1–57:15
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Table 1 Summary of containment results. (Theorem 4.19 also gives a slightly stronger form of the 2^n-nongappiness result than the version stated here.)

If $T \subseteq \mathbb{N}^+$ X, then Y

X	Y	Reference
has an $(n + \mathcal{O}(1))$-nongappy, P-printable subset	$\mathrm{FewP} \subseteq \mathrm{RC}_T$	[7]
has an $\mathcal{O}(n)$-nongappy, P-printable subset	$\mathrm{UP}_{\leq \mathcal{O}(\log n)} \subseteq \mathrm{RC}_T$	Thm. 4.10
has an $\mathcal{O}(n \log n)$-nongappy, P-printable subset	$\mathrm{UP}_{\leq \mathcal{O}(\sqrt{\log n})} \subseteq \mathrm{RC}_T$	Thm. 4.19
for some real number $k > 1$ has an n^k-nongappy, P-printable subset	$\mathrm{UP}_{\leq \mathcal{O}(1) + \frac{\log \log n}{2 \log k}} \subseteq \mathrm{RC}_T$	Thm. 4.13
has an $n^{\log n}$-nongappy, P-printable subset	$\mathrm{UP}_{\leq \mathcal{O}(1) + \frac{1}{2} \log \log \log n} \subseteq \mathrm{RC}_T$	Thm. 4.19
has an $n^{(\log n)^{\mathcal{O}(1)}}$-nongappy, P-printable subset	$\mathrm{UP}_{\leq \mathcal{O}(1) + \frac{1}{3} \log \log \log \log n} \subseteq \mathrm{RC}_T$	Thm. 4.19
has a 2^n-nongappy, P-printable subset S	$\mathrm{UP}_{\leq \max(1, \lfloor \frac{\log^*(n) - \log^*(\log^*(n)+1) - 1}{\lambda} \rfloor)}$ $\subseteq \mathrm{RC}_T$, where $\lambda = 4 + \min_{s \in S, \lvert s\rvert \geq 2}(\lvert s\rvert)$	Thm. 4.19
is infinite	$\mathrm{UP}_{\leq \mathcal{O}(1)} \subseteq \mathrm{RC}_T$	Cor. 4.4

paths it has as a function of the input's length. An NP language falls within a given level of ambiguity if it is accepted by some NPTM that happens to satisfy that ambiguity limit.) More generally, for each function $f : \mathbb{N} \to \mathbb{N}^+$ or $f : \mathbb{N} \to \mathbb{R}^{\geq 1}$, $\mathrm{UP}_{\leq f(n)}$ denotes the class of languages L for which there is an NPTM N such that, for each x, if $x \notin L$ then N on input x has no accepting paths, and if $x \in L$ then $1 \leq \#\mathrm{acc}_N(x) \leq \lfloor f(|x|) \rfloor$ (where $\#\mathrm{acc}_N(x)$ denotes the number of accepting computation paths of N on input x). (Since, for all N and x, $\#\mathrm{acc}_N(x) \in \mathbb{N}$, the class $\mathrm{UP}_{\leq f(n)}$ just defined would be unchanged if $\lfloor f(|x|) \rfloor$ were replaced by $f(|x|)$.) Ambiguity-limited nondeterministic classes whose ambiguity limits range from completely unambiguous ($\mathrm{UP}_{\leq 1}$, i.e., UP) to polynomial ambiguity (Allender and Rubinstein's class FewP [3]) have been defined and studied.

In this paper, we show that many ambiguity-limited counting classes – including ones based on types of logarithmic ambiguity, loglog ambiguity, logloglog ambiguity, and loglogloglog ambiguity – are contained in various collections of restricted counting classes. We do so primarily through two general theorems (Theorems 4.7 and 4.12) that help make clear how, as the size of the "holes" allowed in the sets underpinning the restricted counting classes becomes smaller (i.e., as the sets become more "nongappy"), one can handle more ambiguity. Table 1 summarizes our results about the containment of ambiguity-limited counting classes in restricted counting classes.

Only for polynomial ambiguity was a result of this sort previously known. In particular, Beigel, Gill, and Hertrampf [5], strengthening Cai and Hemachandra's result $\mathrm{FewP} \subseteq \oplus\mathrm{P}$ [13], proved that $\mathrm{FewP} \subseteq \mathrm{RC}_{\{1,3,5,\ldots\}}$, and Borchert, Hemaspaandra, and Rothe [7] noted that $\mathrm{FewP} \subseteq \mathrm{RC}_T$ for each nonempty set $T \subseteq \mathbb{N}^+$ that has an easily presented (formally, P-printable [25], whose definition will be given in Section 2) subset V that is $(n+\mathcal{O}(1))$-nongappy (i.e., for some k the set V never has more than k adjacent, empty lengths; that is, for each collection of $k+1$ adjacent lengths, V will always contain at least one string whose length is one of those $k+1$ lengths).

Our proof approach in the present paper connects somewhat interestingly to the history just mentioned. We will describe in Section 4 the approach that we will call *the iterative constant-setting technique*. However, briefly put, that refers to a process of sequentially setting a series of constants – first c_0, then c_1, then c_2, …, and then c_m – in such a way that, for each $0 \leq j \leq m$, the summation $\sum_{0 \leq \ell \leq j} c_\ell \binom{j}{\ell}$ falls in a certain "yes" or "no" target set, as required by the needs of the setting. For RC_S classes, the "no" target set will be $\{0\}$ and the "yes" target set will be S. In this paper, we will typically put sets into restricted counting classes by building Turing machines that guess (for each $0 \leq \ell \leq j$) cardinality-ℓ sets of accepting paths of another NPTM and then amplify each such successful accepting-path-set guess by – via splitting/cloning of the path – creating from it c_ℓ accepting paths.

A technically novel aspect of the proofs of the two main theorems (Theorems 4.7 and 4.12, each in effect a metatheorem) is that those proofs each provide, in a unified way for a broad class of functions, an analysis of value-growth in the context of iterated functions.

Cai and Hemachandra's [13] result FewP $\subseteq$ $\oplus$P was proven (as was an even more general result about a class known as "Few") by the iterative constant-setting technique. Beigel, Gill, and Hertrampf [5], while generously noting that "this result can also be obtained by a close inspection of Cai and Hemachandra's proof," proved the far stronger result FewP $\subseteq \mathrm{RC}_{\{1,3,5,\ldots\}}$ simply and directly rather than by iterative constant-setting. Borchert, Hemaspaandra, and Rothe's [7] even more general result, noted above for its proof, resurrected the iterative constant-setting technique, using it to understand one particular level of ambiguity. This present paper is, in effect, an immersion into the far richer world of possibilities that the iterative constant-setting technique can offer, if one puts in the work to analyze and bound the growth rates of certain constants central to the method. In particular, as noted above we use the iterative constant-setting method to obtain a broad range of results (see Table 1) regarding how ambiguity-limited nondeterminism is not more powerful than appropriately nongappy restricted counting classes.

Each of our results has immediate consequences regarding the power of the primes as a restricted-counting acceptance type. Borchert, Hemaspaandra, and Rothe's result implies that if the set of primes has an $(n + \mathcal{O}(1))$-nongappy, P-printable subset, then FewP $\subseteq \mathrm{RC}_{\mathrm{PRIMES}}$. However, it is a long-open research issue whether there exists *any* infinite, P-printable subset of the primes, much less an $(n + \mathcal{O}(1))$-nongappy one. Our results lower the bar on what one must assume about how nongappy hypothetical infinite, P-printable subsets of the primes are in order to imply that some superconstant-ambiguity-limited nondeterministic version of NP is contained in $\mathrm{RC}_{\mathrm{PRIMES}}$. We prove that even infinite, P-printable sets of primes with merely exponential upper bounds on the size of their gaps would yield such a result. We also prove – by exploring the relationship between density and nongappiness – that the Lenstra–Pomerance–Wagstaff Conjecture [35, 38] (regarding the asymptotic density of the Mersenne primes) implies that $\mathrm{UP}_{\leq \mathcal{O}(\log \log n)} \subseteq \mathrm{RC}_{\mathrm{PRIMES}}$. The Lenstra–Pomerance–Wagstaff Conjecture is characterized in Wikipedia [41] as being "widely accepted," the fact that it disagrees with a different conjecture (Gillies' Conjecture [22]) notwithstanding.

Additional results, discussions and comments, and the omitted proofs of Theorems 4.3, 4.12, 4.13, 4.14, and 4.19, Propositions 2.5, 4.9, and 4.17, and Corollary 4.15 can be found our full technical report version [26].

2 Definitions

$\mathbb{N} = \{0, 1, 2, \ldots\}$. $\mathbb{N}^+ = \{1, 2, \ldots\}$. Each positive natural number, other than 1, is prime or composite. A prime number is a number that has no positive divisors other than 1 and itself. PRIMES $= \{i \in \mathbb{N} \mid i \text{ is a prime}\} = \{2, 3, 5, 7, 11, \ldots\}$. A composite number is one that has at least one positive divisor other than 1 and itself; COMPOSITES $= \{i \in \mathbb{N} \mid i \text{ is a composite number}\} = \{4, 6, 8, 9, 10, 12, \ldots\}$. $\mathbb{R}$ is the set of all real numbers,

$\mathbb{R}^+ = \{x \in \mathbb{R} \mid x > 0\}$, and $\mathbb{R}^{\geq 1} = \{x \in \mathbb{R} \mid x \geq 1\}$. All logs in this paper (thus those involved in log, loglog, logloglog, loglogloglog, and $\log^{[i]}$, and also those called within the definitions of $\log^*$ and our new $\log^{\circledast}$) are base 2. Also, each call of the log function in this paper, $\log(\cdot)$, is implicitly a shorthand for $\log(\max(1, \cdot))$. We do this so that formulas such as $\log\log\log(\cdot)$ do not cause domain problems on small inputs. (Admittedly, this is also distorting log in the domain-valid open interval (0,1). However, that interval never comes into play in our paper except incidentally when iterated logs drop something into it, and also in the definitions of $\log^*$ and $\log^{\circledast}$ but in those two cases – see the discussion in Footnotes 2 and 8 of [26] – the max happens not to change what those evaluate to on (0,1).)

As mentioned earlier, for any NPTM N and any string x, $\#\mathrm{acc}_N(x)$ will denote the number of accepting computation paths of N on input x. #P [37] is the counting version of NP: $\#\mathrm{P} = \{f : \Sigma^* \to \mathbb{N} \mid (\exists \text{ NPTM } N)(\forall x \in \Sigma^*)[\#\mathrm{acc}_N(x) = f(x)]\}$. $\oplus$P ("Parity P") is the class of sets L such that there is a function $f \in \#\mathrm{P}$ such that, for each string x, it holds that $x \in L \iff f(x) \equiv 1 \pmod 2$ [34, 23].

We will use $\mathcal{O}$ in its standard sense, namely, if f and g are functions (from whose domain negative numbers are typically excluded), then we say $f(n) = \mathcal{O}(g(n))$ exactly if there exist positive integers c and n_0 such that $(\forall n \geq n_0)[f(n) \leq cg(n)]$. We sometimes will also, interchangeably, speak of or write a $\mathcal{O}$ expression as representing a set of functions (e.g., writing $f(n) \in \mathcal{O}(g(n))$) [10, 11], which in fact is what the "big O" notation truly represents.

The notions RC_S, UP, and $\mathrm{UP}_{\leq f(n)}$ are as defined in Section 1. For each $k \geq 1$, Watanabe [39] implicitly and Beigel [4] explicitly studied the constant-ambiguity classes $\mathrm{RC}_{\{1,2,3,\ldots,k\}}$ which, following the notation of Lange and Rossmanith [32], we will usually denote $\mathrm{UP}_{\leq k}$. We extend the definition of $\mathrm{UP}_{\leq f(n)}$ to classes of functions as follows. For classes $\mathcal{F}$ of functions mapping $\mathbb{N}$ to $\mathbb{N}^+$ or $\mathbb{N}$ to $\mathbb{R}^{\geq 1}$, we define $\mathrm{UP}_{\leq \mathcal{F}} = \bigcup_{f \in \mathcal{F}} \mathrm{UP}_{\leq f(n)}$. We mention that the class $\mathrm{UP}_{\leq \mathcal{O}(1)}$ is easily seen to be equal to $\bigcup_{k \in \mathbb{N}^+} \mathrm{UP}_{\leq k}$, which is a good thing since that latter definition of the notion is how $\mathrm{UP}_{\leq \mathcal{O}(1)}$ was defined in the literature more than a quarter of a century ago [29]. $\mathrm{UP}_{\leq \mathcal{O}(1)}$ can be (informally) described as the class of all sets acceptable by NPTMs with constant-bounded ambiguity. Other related classes will also be of interest to us. For example, $\mathrm{UP}_{\leq \mathcal{O}(\log n)}$ captures the class of all sets acceptable by NPTMs with logarithmically-bounded ambiguity. Allender and Rubinstein [3] introduced and studied FewP, the polynomial-ambiguity NP languages, which can be defined by $\mathrm{FewP} = \{L \mid (\exists \text{ polynomial } f)[L \in \mathrm{UP}_{\leq f(n)}]\}$.

The $\mathrm{UP}_{\leq f(n)}$ classes, which will be central to this paper's study, capture ambiguity-bounded versions of NP. They are also motivated by the fact that they completely characterize the existence of ambiguity-bounded (complexity-theoretic) one-way functions.[1]

▶ **Proposition 2.1.** *Let f be any function mapping from $\mathbb{N}$ to $\mathbb{N}^+$. $\mathrm{P} \neq \mathrm{UP}_{\leq f(n)}$ if and only if there exists an $f(n)$-to-one one-way function.*

[1] A (possibly nontotal) function g is said to be a one-way function exactly if (a) g is polynomial-time computable, (b) g is honest (i.e., there exists a polynomial q such that, for each y in the range of g, there exists a string x such that $g(x) = y$ and $|x| \leq q(|y|)$; simply put, each string y mapped to by g is mapped to by some string x that is not much longer than y), and (c) g is not polynomial-time invertible (i.e., there exists no (possibly nontotal) polynomial-time function h such that for each y in the range of g, it holds that $h(y)$ is defined and $g(h(y))$ is defined and $g(h(y)) = y$) [24]. For each $f : \mathbb{N} \to \mathbb{N}^+$ and each (possibly nontotal) function $g : \Sigma^* \to \Sigma^*$, we say that g is $f(n)$-to-one exactly if, for each $y \in \Sigma^*$, $\|\{x \mid g(x) = y\}\| \leq f(|y|)$. When g is a one-way function, the function f is sometimes referred to as an ambiguity limit on the function g, and the special case of $f(n) = 1$ is the case of unambiguous one-way functions. (This is a different notion of ambiguity than that used for NPTMs, though Proposition 2.1 shows that the notions are closely connected.)

That claim holds even if f is not nondecreasing, and holds even if f is not a computable function. To the best of our knowledge, Proposition 2.1 has not been stated before for the generic case of any function $f : \mathbb{N} \rightarrow \mathbb{N}^+$. However, many concrete special cases are well known, and the proposition follows from the same argument as is used for those (see for example [27, Proof of Theorem 2.5] for a tutorial presentation of that type of argument). In particular, the proposition's special cases are known already for UP (due to [24, 30]), $\mathrm{UP}_{\leq k}$ (for each $k \in \mathbb{N}^+$) and $\mathrm{UP}_{\leq \mathcal{O}(1)}$ (in [29, 6]), FewP (in [3]), and (since the following is another name for NP) $\mathrm{UP}_{\leq 2^{n^{\mathcal{O}(1)}}}$ (folklore, see [27, Theorem 2.5, Part 1]). The proposition holds not just for single functions f, but also for classes that are collections of functions, e.g., $\mathrm{UP}_{\leq \mathcal{O}(\log n)}$.

For any function f, we use $f^{[n]}$ to denote function iteration: $f^{[0]}(\alpha) = \alpha$ and inductively, for each $n \in \mathbb{N}$, $f^{[n+1]}(\alpha) = f(f^{[n]}(\alpha))$. For each real number $\alpha \geq 0$, $\log^*(\alpha)$ ("(base 2) log star of α") is the smallest natural number k such that $\log^{[k]}(\alpha) \leq 1$. Although the logarithm of 0 is not defined, note that $\log^*(0)$ is well-defined, namely it is 0 since $\log^{[0]}(0) = 0$.

A set L is said to be P-printable [25] exactly if there is a deterministic polynomial-time Turing machine such that, for each $n \in \mathbb{N}$, the machine when given as input the string 1^n prints (in some natural coding, such as printing each of the strings of L in lexicographical order, inserting the character # after each) exactly the set of all strings in L of length less than or equal to n.

Notions of whether a set has large empty expanses between one element and the next will be central to our work in this paper. Borchert, Hemaspaandra, and Rothe [7] defined and used such a notion, in a way that is tightly connected to our work. We present here the notion they called "nongappy," but here, we will call it "nongappy$_{\text{value}}$" to distinguish their value-centered definition from the length-centered definitions that will be our norm in this paper.

▶ **Definition 2.2** ([7]). *A set $S \subseteq \mathbb{N}^+$ is said to be nongappy$_{value}$ if $S \neq \emptyset$ and $(\exists k > 0)(\forall m \in S)(\exists m' \in S)[m' > m \wedge m'/m \leq k]$.*

This says that the gaps between one element of the set and the next greater one are, as to the *values* of the numbers, bounded by a multiplicative constant. Note that, if we view the natural numbers as naturally coded in binary, that is equivalent to saying that the gaps between one element of the set and the next greater one are, as to the *lengths* of the two strings, bounded by an additive constant. That is, a nonempty set $S \subseteq \mathbb{N}^+$ is said to be nongappy$_{\text{value}}$ by this definition if the gaps in the lengths of elements of S are bounded by an additive constant, and thus we have the following result that clearly holds.

▶ **Proposition 2.3.** *A set $S \subseteq \mathbb{N}^+$ is nongappy$_{value}$ if and only if $S \neq \emptyset$ and $(\exists k > 0)(\forall m \in S)(\exists m' \in S)[m' > m \wedge |m'| \leq |m| + k]$.*

In Section 4 we define other notions of nongappiness that allow larger gaps than the above does. We will always focus on lengths, and so we will consistently use the term "nongappy" in our definitions to speak of gaps quantified in terms of the *lengths* of the strings involved. We now introduce a new notation for the notion nongappy$_{\text{value}}$, and show that our definition does in fact refer to the same notion as that of Borchert, Hemaspaandra, and Rothe.

▶ **Definition 2.4.** *A set $S \subseteq \mathbb{N}^+$ is $(n + \mathcal{O}(1))$-nongappy if $S \neq \emptyset$ and $(\exists f \in \mathcal{O}(1))(\forall m \in S)(\exists m' \in S)[m' > m \wedge |m'| \leq |m| + f(|m|)]$.*

While at first glance this might seem to be different from Borchert, Hemaspaandra, and Rothe's definition, it is easy to see that both definitions are equivalent.

▶ **Proposition 2.5.** *A set S is $(n + \mathcal{O}(1))$-nongappy if and only if it is nongappy$_{value}$.*

3 Related Work

The most closely related work has already largely been covered in the nonappendix part of the paper, but we now briefly mention that work and its relationship to this paper. In particular, the most closely related papers are the work of Cai and Hemachandra [13], Hemaspaandra and Rothe [28], and Borchert, Hemaspaandra, and Rothe [7], which introduced and studied the iterative constant-setting technique as a tool for exploring containments of counting classes. The former two (and also the important related work of Borchert and Stephan [8]) differ from the present paper in that they are not about restricted counting classes, and unlike the present paper, Borchert, Hemaspaandra, and Rothe's paper, as to containment of ambiguity-limited classes, addresses only FewP. (It is known that FewP is contained in the class known as SPP and is indeed so-called SPP-low [31, 17, 18], however that does not make our containments in restricted counting classes uninteresting, as it seems unlikely that SPP is contained in *any* restricted counting class, since SPP's "no" case involves potentially exponential numbers of accepting paths, not zero such paths.) The interesting, recent paper of Cox and Pay [16] draws on the result of Borchert, Hemaspaandra, and Rothe [7] that appears as our Theorem 4.1 to establish that FewP $\subseteq \mathrm{RC}_{\{2^t-1 \,|\, t\in\mathbb{N}^+\}}$ (note that the right-hand side is the restricted counting class defined by the Mersenne numbers), a result that itself implies FewP $\subseteq \mathrm{RC}_{\{1,3,5,\ldots\}}$.

"RC" (restricted counting) classes [7] are central to this paper. The literature's earlier "CP" classes [12] might at first seem similar, but they don't restrict rejection to the case of having zero accepting paths. Leaf languages [9], a different framework, do have flexibility to express "RC" classes, and so are an alternate notation one could use, though in some sense they would be overkill as a framework here due to their extreme descriptive power. The class $\mathrm{RC}_{\{1,3,5,\ldots\}}$ first appeared in the literature under the name $\mathrm{ModZ_2P}$ [5]. Ambiguity-limited classes are also quite central to this paper, and among those we study (see Section 2) are ones defined, or given their notation that we use, in the following papers: [36, 4, 39, 3, 32].

P-printability is due to Hartmanis and Yesha [25]. Allender [2] established a sufficient condition, which we will discuss later, for the existence of infinite, P-printable subsets of the primes. As discussed in the text right after Corollary 4.2 and in Footnote 2, none of the results of Ford, Maynard, Tao, and others [20, 33, 19] about "infinitely often" lower bounds on gaps in the primes, nor any possible future bounds, can possibly be strong enough to be the sole obstacle to a FewP $\subseteq \mathrm{RC}_{\mathrm{PRIMES}}$ construction.

4 Gaps, Ambiguity, and Iterative Constant-Setting

What is the power of NPTMs whose number of accepting paths is 0 for each string not in the set and is a prime for each string in the set? In particular, does that class, $\mathrm{RC}_{\mathrm{PRIMES}}$, contain FewP or, for that matter, any interesting ambiguity-limited nondeterministic class? That is the question that motivated this work.

Why might one hope that $\mathrm{RC}_{\mathrm{PRIMES}}$ might contain some ambiguity-limited classes? Well, we clearly have that NP $\subseteq \mathrm{RC}_{\mathrm{COMPOSITES}}$, so having the composites as our acceptance targets allows us to capture all of NP. Why? For any NP machine N, we can make a new machine N' that mimics N, except it clones each accepting path into four accepting paths, and so when N has zero accepting paths N' has zero accepting paths, and when N has at least one accepting path N' has a composite number of accepting paths.

On the other hand, why might one suspect that interesting ambiguity-limited nondeterministic classes such as FewP might *not* be contained in $\mathrm{RC}_{\mathrm{PRIMES}}$? Well, it is not even clear that FewP is contained in the class of sets that are accepted by NPTMs that accept via having a prime number of accepting paths, and reject by having a nonprime number of accepting paths (rather than being restricted to rejecting only by having zero accepting paths, as is $\mathrm{RC}_{\mathrm{PRIMES}}$). That is, even a seemingly vastly more flexible counting class does not seem to in any obvious way contain FewP.

This led us to revisit the issue of identifying the sets $S \subseteq \mathbb{N}^+$ that satisfy $\mathrm{FewP} \subseteq \mathrm{RC}_S$, studied previously by, for example, Borchert, Hemaspaandra, and Rothe [7] and Cox and Pay [16]. In particular, Borchert, Hemaspaandra, and Rothe showed, by the iterative constant-setting technique, the following theorem. From it, we immediately have Cor. 4.2.

▶ **Theorem 4.1** ([7, Theorem 3.4]). *If $T \subseteq \mathbb{N}^+$ has an $(n + \mathcal{O}(1))$-nongappy, P-printable subset, then* $\mathrm{FewP} \subseteq \mathrm{RC}_T$.

▶ **Corollary 4.2.** *If* PRIMES *contains an $(n + \mathcal{O}(1))$-nongappy, P-printable subset, then* $\mathrm{FewP} \subseteq \mathrm{RC}_{\mathrm{PRIMES}}$.

Does PRIMES contain an $(n+\mathcal{O}(1))$-nongappy, P-printable subset? The Bertrand–Chebyshev Theorem [15] states that for each natural number $k > 3$, there exists a prime p such that $k < p < 2k - 2$. Thus PRIMES clearly has an $(n + \mathcal{O}(1))$-nongappy subset.[2] Indeed, since – with p_i denoting the ith prime – $(\forall \epsilon > 0)(\exists N)(\forall n > N)[p_{n+1} - p_n < \epsilon p_n]$ [40], it holds that represented in binary there are primes at all but a finite number of bit-lengths. Unfortunately, to the best of our knowledge it remains an open research issue whether there exists *any* infinite, P-printable subset of the primes, much less one that in addition is $(n + \mathcal{O}(1))$-nongappy. In fact, the best sufficient condition we know of for the existence of an infinite, P-printable set of primes is a relatively strong hypothesis of Allender [2, Corollary 32 and the comment following it] about the probabilistic complexity class R [21] and the existence of secure extenders. However, that result does not promise that the infinite, P-printable set of primes is $(n + \mathcal{O}(1))$-nongappy – not even now, when it is known that primality is not merely in the class R but even is in the class P [1].

So the natural question to ask is: Can we at least lower the bar for what strength of advance – regarding the existence of P-printable sets of primes and the nongappiness of such sets – would suffice to allow $\mathrm{RC}_{\mathrm{PRIMES}}$ to contain some interesting ambiguity-limited class?

In particular, the notion of nongappiness used in Theorem 4.1 above means that our length gaps between adjacent elements of our P-printable set must be bounded by an additive constant. Can we weaken that to allow larger gaps, e.g., gaps of multiplicative constants, and still have containment for some interesting ambiguity-limited class?

We show that the answer is yes. More generally, we show that there is a tension and trade-off between gaps and ambiguity. As we increase the size of gaps we are willing to tolerate, we can prove containment results for restrictive counting classes, but of increasingly small levels of ambiguity. On the other hand, as we lower the size of the gaps we are willing to tolerate, we increase the amount of ambiguity we can handle.

[2] We mention in passing that it follows from the fact that PRIMES clearly *does* have an $(n + \mathcal{O}(1))$-nongappy subset that none of the powerful results by Ford, Maynard, Tao, and others [20, 33, 19] about "infinitely often" lower bounds for gaps in the primes, or in fact any results purely about lower bounds on gaps in the primes, can possibly prevent there from being a set of primes whose gaps are small enough that the set could, if sufficiently accessible, be used in a Cai–Hemachandra-type iterative constant-setting construction seeking to show that $\mathrm{FewP} \subseteq \mathrm{RC}_{\mathrm{PRIMES}}$. (In fact – keeping in mind that the difference between the value of a number and its coded length is exponential – the best such gaps known are almost exponentially too weak to preclude a Cai–Hemachandra-type iterative constant-setting construction.) Rather, the only obstacle will be the issue of whether there is such a set that in addition is computationally easily accessible/thin-able, i.e., whether there is such an $(n + \mathcal{O}(1))$-nongappy subset of the primes that is P-printable.

It is easy to see that the case of constant-ambiguity nondeterminism is so extreme that the iterative constant-setting method works for all infinite sets regardless of how nongappy they are. (It is even true that the containment $\mathrm{UP}_{\leq k} \subseteq \mathrm{RC}_T$ holds for some finite sets T, such as $\{1, 2, 3, \ldots, k\}$; but our point here is that it holds for *all* infinite sets $T \subseteq \mathbb{N}^+$.)

▶ **Theorem 4.3.** *For each infinite set $T \subseteq \mathbb{N}^+$ and for each natural $k \geq 1$, $\mathrm{UP}_{\leq k} \subseteq \mathrm{RC}_T$.*

Theorem 4.3 should be compared with the discussion by Hemaspaandra and Rothe [28, p. 210] of an NP-many-one-hardness result of Borchert and Stephan [8] and a $\mathrm{UP}_{\leq k}$-1-truth-table-hardness result. In particular, both those results are in the *un*restricted setting, and so neither implies Theorem 4.3. The proof of Theorem 4.3 can be found as Appendix A of our [26]. However, we recommend that the reader read it, if at all, only after reading the proof of Theorem 4.7, whose proof also uses (and within this paper, is the key presentation of) iterative constant-setting, and is a more interesting use of that approach.

▶ **Corollary 4.4.** *For each infinite set $T \subseteq \mathbb{N}^+$, $\mathrm{UP}_{\leq \mathcal{O}(1)} \subseteq \mathrm{RC}_T$.*

▶ **Corollary 4.5.** $\mathrm{UP}_{\leq \mathcal{O}(1)} \subseteq \mathrm{RC}_{\mathrm{PRIMES}}$.

So constant-ambiguity nondeterminism can be done by the restrictive counting class based on the primes. However, what we are truly interested in is whether we can achieve a containment for superconstant levels of ambiguity. We in fact can do so, and we now present such results for a range of cases between constant ambiguity ($\mathrm{UP}_{\leq \mathcal{O}(1)}$) and polynomial ambiguity (FewP). We first define a broader notion of nongappiness.

▶ **Definition 4.6.** *Let F be any function mapping $\mathbb{R}^+$ to $\mathbb{R}^+$. A set $S \subseteq \mathbb{N}^+$ is F-nongappy if $S \neq \emptyset$ and $(\forall m \in S)(\exists m' \in S)[m' > m \wedge |m'| \leq F(|m|)]$.*[3]

This definition sets F's domain and codomain to include real numbers, despite the fact that the underlying F-nongappy set S is of the type $S \subseteq \mathbb{N}^+$. The codomain is set to include real numbers because many notions of nongappiness we examine rely on non-integer values. Since we are often iterating functions, we thus set F's domain to be real numbers as well. Doing so does not cause problems as to computability because F is a function that is never actually computed by the Turing machines in our proofs; it is merely one that is mathematically reasoned about in the analysis of the nongappiness of sets underpinning restricted counting classes.

The following theorem generalizes the iterative constant-setting technique that Borchert, Hemaspaandra, and Rothe used to prove Theorem 4.1.

▶ **Theorem 4.7.** *Let F be a function mapping from $\mathbb{R}^+$ to $\mathbb{R}^+$ and let n_0 be a positive natural number such that F restricted to the domain $\{t \in \mathbb{R}^+ \mid t \geq n_0\}$ is nondecreasing and for all $t \geq n_0$ we have (a) $F(t) \geq t + 2$ and (b) $(\forall c \in \mathbb{N}^+)[cF(t) \geq F(ct)]$. Let j be a function, mapping from $\mathbb{N}$ to $\mathbb{N}^+$, that is at most polynomial in the value of its input and is computable in time polynomial in the value of its input. Suppose $T \subseteq \mathbb{N}^+$ has an F-nongappy, P-printable subset S. Let $\lambda = 4 + |s|$ where s is the smallest element of S with $|s| \geq n_0$. If for some $\beta \in \mathbb{N}^+$, $F^{[j(n)]}(\lambda) = \mathcal{O}(n^\beta)$, then $\mathrm{UP}_{\leq j(n)} \subseteq \mathrm{RC}_T$.*

[3] In two later definitions, 4.8 and 4.18, we apply Definition 4.6 to classes of functions. In each case, we will directly define that, but in fact will do so as the natural lifting (namely, saying a set is $\mathcal{F}$-nongappy exactly if there is an $F \in \mathcal{F}$ such that the set is F-nongappy). The reason we do not directly define lifting as applying to all classes $\mathcal{F}$ is in small part that we need it only in those two definitions, and in large part because doing so could cause confusion, since an earlier definition (Def. 2.4) that is connecting to earlier work is using as a syntactic notation an expression that itself would be caught up by such a lifting (though the definition given in Def. 2.4 is consistent with the lifting reading, give or take the fact that we've now broadened our focus to the reals rather than the naturals).

This theorem has a nice interpretation: a sufficient condition for an ambiguity-limited class $\mathrm{UP}_{\leq j(n)}$ to be contained in a particular restricted counting class is for there to be at least $j(n)$ elements that are reachable in polynomial time in an F-nongappy subset of the set that defines the counting class, assuming that the nongappiness of the counting class and the ambiguity of the $\mathrm{UP}_{\leq j(n)}$ class satisfy the above conditions.

Proof of Theorem 4.7. Let F, j, n_0, T, and S be as per the theorem statement. Suppose $(\exists \beta' \in \mathbb{N}^+)[F^{[j(n)]}(\lambda) = \mathcal{O}(n^{\beta'})]$, and fix a value $\beta \in \mathbb{N}^+$ such that $F^{[j(n)]}(\lambda) = \mathcal{O}(n^{\beta})$.

We start our proof by defining three sequences of constants that will be central in our iterative constant-setting argument, and giving bounds on their growth. Set c_1 to be the least element of S with $|c_1| \geq n_0$. For $n \in \{2, 3, \ldots\}$, given $c_1, c_2, \ldots, c_{n-1}$, we set

$$b_n = \sum_{1 \leq \ell \leq n-1} c_\ell \binom{n}{\ell}. \tag{1}$$

With b_n set, we define a_n to be the least element of S such that $a_n \geq b_n$. Finally, we set $c_n = a_n - b_n$. We now show that $\max_{1\leq \ell \leq j(n)} |a_\ell|$ and $\max_{1\leq \ell \leq j(n)} |c_\ell|$ are both at most polynomial in n. Take any $i \in \{2, 3, \ldots\}$. By the construction above and since S is F-nongappy, we have $|c_i| \leq |a_i| \leq F(|b_i|)$. Using our definition of b_i from Eq. 1 we get $b_i = \sum_{1 \leq k \leq i-1} c_k \binom{i}{k} \leq (i-1)(\max_{1\leq k\leq i-1} c_k)\binom{i}{\lceil \frac{i}{2} \rceil} \leq (\max_{1\leq k \leq i-1} c_k)(2^{2i})$. Thus we can bound the length of b_i by $|b_i| \leq 2i + \max_{1 \leq k \leq i-1} |c_k| \leq 2i + \max_{1\leq k \leq i} |c_k|$. Since this is true for all $i \in \{2, 3, \ldots\}$, it follows that if $\max_{1 \leq \ell \leq j(n)} |c_\ell|$ is at most polynomial in n, then $\max_{1\leq \ell \leq j(n)} |b_\ell|$ is at most polynomial in n, and since for all i, $a_i = b_i + c_i$, $\max_{1 \leq \ell \leq j(n)} |a_\ell|$ is at most polynomial in n. We now show that $\max_{1 \leq \ell \leq j(n)} |c_\ell|$ is in fact polynomial in n.

Let $n \in \{2, 3, \ldots\}$ be arbitrary. For each $i \in \{2, 3, \ldots, j(n)\}$, we have that $|b_i| \geq |c_1| \geq n_0$. Since F restricted to $\{t \in \mathbb{R}^+ \mid t \geq n_0\}$ is nondecreasing,

$$|c_i| \leq F(|b_i|) \leq F(2i + \max_{1 \leq k \leq i-1} |c_k|). \tag{2}$$

Since Eq. 2 holds for $2 \leq i \leq j(n)$ we can repeatedly apply it inside the max to get

$$|c_i| \leq F(2i + F(2(i-1) + F(\cdots 2 \cdot 4 + F(2 \cdot 3 + F(2 \cdot 2 + |c_1|)) \cdots))). \tag{3}$$

Recall that $\lambda = 4 + |c_1|$. From condition (a) of the theorem statement and since $|c_1| \geq n_0$, we have $F(\lambda) \geq 2 + \lambda = 2 + 4 + |c_1| \geq 6$, and thus $|c_i| \leq F(2i + F(2(i-1) + F(\cdots 2 \cdot 4 + F(2F(\lambda)) \cdots)))$. Since it follows from our theorem's assumptions that $(\forall t \geq \lambda)(\forall c \in \mathbb{N}^+)[cF(t) \geq F(ct)]$, we have $|c_i| \leq F(2i + F(2(i-1) + F(\cdots 2 \cdot 4 + 2F(F(\lambda)) \cdots)))$. Continuing to use the inequalities $(\forall k \geq 3)[2 \cdot k \leq F^{[k-2]}(\lambda)]$ and $(\forall t \geq \lambda)(\forall c \in \mathbb{N}^+)[cF(t) \geq F(ct)]$ we get $|c_i| \leq (i-1)(F^{[i-1]}(\lambda))$. Since $(\forall t \geq \lambda)[F(t) \geq t]$ and $i \leq j(n)$, we have that $|c_i| \leq (i-1)(F^{[i-1]}(\lambda)) \leq j(n)F^{[j(n)]}(\lambda)$. Since this bound holds for all $i \in \{2, 3, \ldots, j(n)\}$, it follows that $\max_{2 \leq \ell \leq n} |c_\ell| \leq j(n)F^{[j(n)]}(\lambda)$, and thus $\max_{1 \leq \ell \leq n} |c_\ell| \leq j(n)F^{[j(n)]}(\lambda) + |c_1|$. By supposition, $F^{[j(n)]}(\lambda) = \mathcal{O}(n^{\beta})$. Also, from our theorem's assumptions, $j(n)$ is polynomial in the value n, which means we can find some β'' such that $j(n) = \mathcal{O}(n^{\beta''})$. Hence we have $j(n)F^{[j(n)]}(\lambda) = \mathcal{O}(n^{\beta + \beta''})$. Since $|c_1|$ is a finite constant, this means $j(n)F^{[j(n)]}(\lambda) + |c_1|$ is polynomially bounded, and so $\max_{1 \leq \ell \leq j(n)} |c_\ell|$ is at most polynomial in n. By the argument in the preceding paragraph, $\max_{1 \leq \ell \leq j(n)} |a_\ell|$ is at most polynomial in n.

We now show that $\mathrm{UP}_{\leq j(n)} \subseteq \mathrm{RC}_T$. Let L be in $\mathrm{UP}_{\leq j(n)}$, witnessed by an NPTM $\hat{N}$. To show $L \in \mathrm{RC}_T$ we describe an NPTM N that, on each input x, has 0 accepting paths if $x \notin L$, and has $\#\mathrm{acc}_N(x) \in T$ if $x \in L$. On input x, our machine N computes $j(|x|)$ and then computes the constants $c_1, c_2, \ldots, c_{j(|x|)}$ as described above. Then N nondeterministically guesses an integer $i \in \{1, 2, \ldots, j(|x|)\}$, and nondeterministically guesses a cardinality-i set of paths of $\hat{N}(x)$. If all the paths guessed in a cardinality-i set are accepting paths, then N branches into c_i accepting paths; otherwise, that branch of N rejects. If $\hat{N}(x)$ has fewer than i paths, then the subtree of N that guessed i will have 0 accepting paths, since we cannot guess i distinct paths of $\hat{N}(x)$. We claim that N shows $L \in \mathrm{RC}_T$.

Consider any input x. If $x \notin L$, then clearly for all $i \in \{1, 2, \ldots, j(|x|)\}$ each cardinality-i set of paths of $\hat{N}$ guessed will have at least one rejecting path, and so N will have no accepting path. Suppose $x \in L$. Then $\hat{N}$ must have some number of accepting paths k. Since $\hat{N}$ witnesses $L \in \mathrm{UP}_{\leq j(n)}$, we must have $1 \leq k \leq j(|x|)$. Our machine N will have c_1 accepting paths for each accepting path of $\hat{N}$, c_2 additional accepting paths for each pair of accepting paths of $\hat{N}$, c_3 additional accepting paths for each triple of accepting paths of $\hat{N}$, and so on. Of course, for any cardinality-i set where $i > k$, at least one of the paths must be rejecting, and so N will have no accepting paths from guessing each $i > k$. Thus we have $\#\mathrm{acc}_N(x) = \sum_{1 \leq \ell \leq k} c_\ell \binom{k}{\ell}$. If $k = 1$, we have $\#\mathrm{acc}_N(x) = c_1$. If $2 \leq k \leq j(|x|)$, then $\#\mathrm{acc}_N(x) = c_k + \sum_{1 \leq \ell \leq k-1} c_\ell \binom{k}{\ell} = c_k + b_k = a_k$. In either case, $\#\mathrm{acc}_N(x) \in S$, and hence $\#\mathrm{acc}_N(x) \in T$. To complete our proof for $L \in \mathrm{RC}_T$ we need to check that N is an NPTM.

Note that, by assumption, $j(|x|)$ can be computed in time polynomial in $|x|$. Furthermore, the value $j(|x|)$ is at most polynomial in $|x|$, and so N's simulation of each cardinality-i set of paths of $\hat{N}$ can be done in time polynomial in $|x|$. Since S is P-printable and $\max_{1 \leq i \leq j(|x|)} |a_i|$ is at most polynomial in $|x|$, finding the constants a_i can be done in time polynomial in $|x|$. Also, since $\max_{1 \leq i \leq j(|x|)} |c_i|$ is at most polynomial in $|x|$, the addition and multiplication to compute each c_i can be done in time polynomial in $|x|$. All other operations done by N are also polynomial-time, and so N is an NPTM. ◀

It is worth noting that in general iterative constant-setting proofs it is sometimes useful to have a nonzero constant c_0 in order to add a constant number $c_0 \binom{i}{0} = c_0$ of accepting paths. However, when trying to show containment in a restricted counting class (as is the case here), we set $c_0 = 0$ to ensure that $\#\mathrm{acc}_N(x) = 0$ if $x \notin L$, and so we do not even have a c_0 but rather start iterative constant-setting and its sums with the c_1 case (as in Eq. 1).

Theorem 4.7 can be applied to get complexity-class containments. In particular, we now define a notion of nongappiness based on a multiplicative-constant increase in lengths, and we show – as Theorem 4.10 – that this notion of nongappiness allows us to accept all sets of logarithmic ambiguity.

▶ **Definition 4.8.** *A set $S \subseteq \mathbb{N}^+$ is $\mathcal{O}(n)$-nongappy if $S \neq \emptyset$ and $(\exists f \in \mathcal{O}(n))(\forall m \in S)(\exists m' \in S)[m' > m \wedge |m'| \leq f(|m|)]$.*

The following proposition notes that one can view this definition in a form similar to Borchert, Hemaspaandra, and Rothe's definition to see that $\mathcal{O}(n)$-nongappy sets are, as to the increase in the lengths of consecutive elements, bounded by a multiplicative constant. (In terms of values, this means that the gaps between the values of one element of the set and the next are bounded by a polynomial increase.)

▶ **Proposition 4.9.** *A set $S \subseteq \mathbb{N}^+$ is $\mathcal{O}(n)$-nongappy if and only if there exists $k \in \mathbb{N}^+$ such that S is kn-nongappy.*

▶ **Theorem 4.10.** *If $T \subseteq \mathbb{N}^+$ has an $\mathcal{O}(n)$-nongappy, P-printable subset, then $\mathrm{UP}_{\leq \mathcal{O}(\log n)} \subseteq \mathrm{RC}_T$.*

Proof. By the "only if" direction of Proposition 4.9, there exists a $k \in \mathbb{N}^+$ such that T has a kn-nongappy, P-printable subset. We can assume $k \geq 2$ since if a set has a $1n$-nongappy, P-printable subset then it also has a $2n$-nongappy, P-printable subset. Let $F : \mathbb{R}^+ \to \mathbb{R}^+$

be the function $F(t) = kt$. The function F satisfies the conditions from Theorem 4.7 since for all $t \geq 2$, $F(t) = kt \geq t + 2$, $(\forall c)[cF(n) = ckn = F(cn)]$, and F is nondecreasing on $\mathbb{R}^+$. Let $\lambda = 4 + |s|$ where s is the smallest element of the kn-nongappy, P-printable subset of T such that the conditions on F hold for all $t \geq |s|$, i.e., s is the smallest element of the kn-nongappy, P-printable subset of T such that $|s| \geq 2$. For any function $g : \mathbb{N} \to \mathbb{R}^{\geq 1}$ satisfying $g(n) = \mathcal{O}(\log n)$ it is not hard to see (since for each natural n it holds that $\log(n+2) \geq 1$) that there must exist some $d \in \mathbb{N}^+$ such that $(\forall n \in \mathbb{N}^+)[g(n) \leq d\log(n+2)]$, and hence $\mathrm{UP}_{\leq g(n)} \subseteq \mathrm{UP}_{\leq d\log(n+2)} = \mathrm{UP}_{\leq \lfloor d\log(n+2)\rfloor}$. Additionally, $j(n) = \lfloor d\log(n+2)\rfloor$ satisfies the conditions from Theorem 4.7 since $j(n)$ can be computed in time polynomial in n and has value at most polynomial in n. Applying Theorem 4.7, to prove that $\mathrm{UP}_{\leq j(n)} \subseteq \mathrm{RC}_T$ it suffices to show that there is some $\beta \in \mathbb{N}^+$ such that $F^{[j(n)]}(\lambda) = \mathcal{O}(n^\beta)$ where λ is given by the statement of the theorem. So it suffices to show that for some $\beta \in \mathbb{N}^+$ and for all but finitely many n, $F^{[j(n)]}(\lambda) \leq n^\beta$. Note that $F^{[j(n)]}(\lambda) = k^{j(n)}\lambda$. So it is enough to show that for all but finitely many n, $k^{j(n)}\lambda \leq n^\beta$, or (taking logs) equivalently that for all but finitely many n, $\lfloor d\log(n+2)\rfloor \log k + \log\lambda \leq \beta\log n$. Set β to be the least integer greater than $2d\log k + \log\lambda$. Then for all $n \geq 2$ we have $\beta\log n \geq 2d\log k\log n + \log\lambda\log n \geq d\log k\log(n^2) + \log\lambda\log n \geq d\log k\log(n+2) + \log\lambda \geq \lfloor d\log(n+2)\rfloor\log k + \log\lambda$, which is what we needed. Thus for any function $g : \mathbb{N} \to \mathbb{R}^{\geq 1}$ satisfying $g(n) = \mathcal{O}(\log n)$ we have that there exists a function j such that $\mathrm{UP}_{\leq g(n)} \subseteq \mathrm{UP}_{\leq j(n)} \subseteq \mathrm{RC}_T$. ◀

▶ **Corollary 4.11.** *If* PRIMES *has an $\mathcal{O}(n)$-nongappy, P-printable subset, then* $\mathrm{UP}_{\leq\mathcal{O}(\log n)} \subseteq \mathrm{RC}_{\mathrm{PRIMES}}$.

In order for the iterative constant-setting approach used in Theorem 4.7 to be applicable, it is clear that we need to consider UP classes that have at most polynomial ambiguity, because otherwise the constructed NPTMs could not guess large enough collections of paths within polynomial time. Since in the statement of Theorem 4.7 we use the function j to denote the ambiguity of a particular UP class, this requires j to be at most polynomial in the value of its input. Furthermore, since our iterative constant-setting requires having a bound on the number of accepting paths the UP machine could have had on a particular string, we also need to be able to compute the function j in time polynomial in the value of its input. Thus the limitations on the function j are natural and seem difficult to remove. Theorem 4.7 is flexible enough to, by a proof similar to that of Theorem 4.10, imply Borchert, Hemaspaandra, and Rothe's result stated in Theorem 4.1 where j reaches its polynomial bound. Another limitation of Theorem 4.7 is that it requires that for all t greater than or equal to a fixed constant n_0, $(\forall c \in \mathbb{N}^+)[cF(t) \geq F(ct)]$. It is possible to prove a similar result where for all t greater than or equal to a fixed constant n_0, $(\forall c \in \mathbb{N}^+)[cF(t) \leq F(ct)]$, which we now do as Theorem 4.12.

▶ **Theorem 4.12.** *Let F be a function mapping from $\mathbb{R}^+$ to $\mathbb{R}^+$ and let n_0 be a positive natural number such that F restricted to the domain $\{t \in \mathbb{R}^+ \mid t \geq n_0\}$ is nondecreasing and for all $t \geq n_0$ we have (a) $F(t) \geq t + 2$ and (b) $(\forall c \in \mathbb{N}^+)[cF(t) \leq F(ct)]$. Let j be a function mapping from $\mathbb{N}$ to $\mathbb{N}^+$ that is computable in time polynomial in the value of its input and whose output is at most polynomial in the value of its input. Suppose $T \subseteq \mathbb{N}^+$ has an F-nongappy, P-printable subset S. Let $\lambda = 4 + |s|$ where s is the smallest element of S with $|s| \geq n_0$. If for some β, $F^{[j(n)]}(j(n)\lambda) = \mathcal{O}(n^\beta)$, then* $\mathrm{UP}_{\leq j(n)} \subseteq \mathrm{RC}_T$.

How does this theorem compare with our other metatheorem, Theorem 4.7? Since in both metatheorems F is nondecreasing after a prefix, speaking informally and broadly, the functions F where (after a prefix) $(\forall c \in \mathbb{N}^+)[cF(t) \leq F(ct)]$ holds grow faster than the functions F where (after a prefix) $(\forall c \in \mathbb{N}^+)[cF(t) \geq F(ct)]$ holds. (The examples we give of applying the two theorems reflect this.) So, this second metatheorem is accommodating larger gaps in the sets of integers that define our restricted counting class, but is also assuming a slightly stronger condition for the containment of an ambiguity-limited class to follow. More specifically, since we have the extra factor of $j(n)$ inside of the iterated application of F, we may need even more than $j(|x|)$ elements to be reachable in polynomial time (exactly how many more will depend on the particular function F).

We now discuss some other notions of nongappiness and obtain complexity-class containments regarding them using Theorem 4.12.

▶ **Theorem 4.13.** *If there exists a real number $k > 1$ such that $T \subseteq \mathbb{N}^+$ has an n^k-nongappy, P-printable subset, then* $\mathrm{UP}_{\leq \mathcal{O}(1)+\frac{\log\log n}{2\log k}} \subseteq \mathrm{RC}_T$.

Theorem 4.13 has an interesting consequence when applied to the Mersenne primes. In particular, as we now show, it can be used to prove that the Lenstra–Pomerance–Wagstaff Conjecture implies that the $\mathcal{O}(\log\log n)$-ambiguity sets in NP each belong to $\mathrm{RC}_{\mathrm{PRIMES}}$.

A Mersenne prime is a prime of the form $2^k - 1$. We will use the Mersenne prime counting function $\mu(n)$ to denote the number of Mersenne primes with length less than or equal to n (when represented in binary). The Lenstra–Pomerance–Wagstaff Conjecture [35, 38] (see also [14]) asserts that there are infinitely many Mersenne primes, and that $\mu(n)$ grows asymptotically as $e^\gamma \log n$ where $\gamma \approx 0.577$ is the Euler–Mascheroni constant. (Note: We say that $f(n)$ grows asymptotically as $g(n)$ when $\lim_{n\to\infty} f(n)/g(n) = 1$.) Having infinitely many Mersenne primes immediately yields an infinite, P-printable subset of the primes. In particular, on input 1^n we can print all Mersenne primes of length less than or equal to n in polynomial time by just checking (using a deterministic polynomial-time primality test [1]) each number of the form $2^k - 1$ whose length is less than or equal to n, and if it is prime then printing it. If the Lenstra–Pomerance–Wagstaff Conjecture holds, what can we also say about the gaps in the Mersenne primes? We address that with the following result.

▶ **Theorem 4.14.** *If the Lenstra–Pomerance–Wagstaff Conjecture holds, then for each $\epsilon > 0$ the primes (indeed, even the Mersenne primes) have an $n^{1+\epsilon}$-nongappy, P-printable subset.*

▶ **Corollary 4.15.** *If the Lenstra–Pomerance–Wagstaff Conjecture holds, then* $\mathrm{UP}_{\leq \mathcal{O}(\log\log n)} \subseteq \mathrm{RC}_{\mathrm{PRIMES}}$ *(indeed,* $\mathrm{UP}_{\leq \mathcal{O}(\log\log n)} \subseteq \mathrm{RC}_{\mathrm{MersennePRIMES}}$*).*

We will soon turn to discussing more notions of nongappiness and what containment theorems hold regarding them. However, to support one of those notions, we first define a function that will arise naturally in Theorem 4.19.

▶ **Definition 4.16.** *For any $\alpha \in \mathbb{R}$, $\alpha > 0$, $\log^{\circledast}(\alpha)$ is the largest natural number k such that $\log^{[k]}(\alpha) \geq k$. We define $\log^{\circledast}(0)$ to be 0.*

For $\alpha > 1$, taking $k = 0$ satisfies $\log^{[k]}(\alpha) \geq k$. Also, for all $\ell \geq \log^*(\alpha)$, $\log^{[\ell]}(\alpha) \leq \log^{[\log^*(\alpha)]}(\alpha) \leq 1 \leq \ell$, and so no $\ell \geq \log^*(\alpha)$ can be used as the k in the definition above. So there is at least one, but only finitely many k such that $\log^{[k]}(\alpha) \geq k$, which means that $\log^{\circledast}(\alpha)$ is well-defined. Using the def. of $\log^{\circledast}(\alpha)$ and the above, we get $\log^{\circledast}(\alpha) \leq \log^*(\alpha)$ when $\alpha > 1$. For $\alpha \leq 1$, 0 is the only natural number for which the condition from the def. holds, and so $\log^{\circledast}(\alpha) = 0$ if $\alpha \leq 1$. Thus for $\alpha \leq 1$, $\log^{\circledast}(\alpha) = \log^*(\alpha)$. As to the relationship of its values to those of $\log^*$, we have the following proposition.

▶ **Proposition 4.17.** *For all $\alpha \geq 0$, $\log^*(\alpha) - \log^*(\log^*(\alpha) + 1) - 1 \leq \log^{\circledast}(\alpha) \leq \log^*(\alpha)$.*

▶ **Definition 4.18.** *A nonempty set* $S \subseteq \mathbb{N}^+$ *is*

1. $\mathcal{O}(n \log n)$*-nongappy if* $(\exists f \in \mathcal{O}(n \log n))(\forall m \in S)(\exists m' \in S)[m' > m \wedge |m'| \leq f(|m|)]$, *and*
2. $n^{(\log n)^{\mathcal{O}(1)}}$*-nongappy if* $(\exists f \in \mathcal{O}(1))(\forall m \in S)(\exists m' \in S)[m' > m \wedge |m'| \leq |m|^{(\log |m|)^{f(|m|)}}]$.

Definitions of $n^{\log n}$-nongappy and 2^n-nongappy are provided via Definition 4.6, since $n^{\log n}$ and 2^n are each a single function, not a collection of functions. Those two notions, along with the two notions of Definition 4.18, will be the focus of Theorem 4.19. That theorem obtains the containments related to those four notions of nongappiness. As one would expect, as the allowed gaps become larger the corresponding UP classes become more restrictive in their ambiguity bounds. Theorem 4.19 also gives a corollary about primes.

▶ **Theorem 4.19.** *Let* T *be a subset of* $\mathbb{N}^+$.

1. *If* T *has an* $\mathcal{O}(n \log n)$*-nongappy, P-printable subset, then* $\mathrm{UP}_{\leq \mathcal{O}(\sqrt{\log n})} \subseteq \mathrm{RC}_T$.
2. *If* T *has an* $n^{\log n}$*-nongappy, P-printable subset, then* $\mathrm{UP}_{\leq \mathcal{O}(1) + \frac{1}{2} \log \log \log n} \subseteq \mathrm{RC}_T$.
3. *If* T *has an* $n^{(\log n)^{\mathcal{O}(1)}}$*-nongappy, P-printable subset, then* $\mathrm{UP}_{\leq \mathcal{O}(1) + \frac{1}{3} \log \log \log \log n} \subseteq \mathrm{RC}_T$.
4. *If* T *has a* 2^n*-nongappy, P-printable subset* S*, then* $\mathrm{UP}_{\leq \max(1, \lfloor \frac{\log^{\circledast} n}{\lambda} \rfloor)} \subseteq \mathrm{RC}_T$ *(and so certainly also* $\mathrm{UP}_{\leq \max(1, \lfloor \frac{\log^*(n) - \log^*(\log^*(n)+1) - 1)}{\lambda} \rfloor)} \subseteq \mathrm{RC}_T$*), where* $\lambda = 4 + \min_{s \in S, |s| \geq 2}(|s|)$.

▶ **Corollary 4.20.**

1. *If* PRIMES *has an* $\mathcal{O}(n \log n)$*-nongappy, P-printable subset, then* $\mathrm{UP}_{\leq \mathcal{O}(\sqrt{\log n})} \subseteq \mathrm{RC}_{\mathrm{PRIMES}}$.
2. *If* PRIMES *has an* $n^{\log n}$*-nongappy, P-printable subset, then* $\mathrm{UP}_{\leq \mathcal{O}(1) + \frac{1}{2} \log \log \log n} \subseteq \mathrm{RC}_{\mathrm{PRIMES}}$.
3. *If* PRIMES *has an* $n^{(\log n)^{\mathcal{O}(1)}}$*-nongappy, P-printable subset, then* $\mathrm{UP}_{\leq \mathcal{O}(1) + \frac{1}{3} \log \log \log \log n} \subseteq \mathrm{RC}_{\mathrm{PRIMES}}$.
4. *If* PRIMES *has a* 2^n*-nongappy, P-printable subset* S*, then* $\mathrm{UP}_{\leq \max(1, \lfloor \frac{\log^{\circledast} n}{\lambda} \rfloor)} \subseteq \mathrm{RC}_{\mathrm{PRIMES}}$ *(and so certainly also* $\mathrm{UP}_{\leq \max(1, \lfloor \frac{\log^*(n) - \log^*(\log^*(n)+1) - 1)}{\lambda} \rfloor)} \subseteq \mathrm{RC}_{\mathrm{PRIMES}}$*), where* $\lambda = 4 + \min_{s \in S, |s| \geq 2}(|s|)$.

5 Conclusions and Open Problems

We proved two flexible metatheorems that can be used to obtain containments of ambiguity-limited classes in restricted counting classes, and applied those theorems to prove containments for some of the most natural ambiguity-limited classes. Beyond the containments we derived based on Theorems 4.7 and 4.12, those two metatheorems themselves seem to reflect a trade-off between the ambiguity allowed in an ambiguity-limited class and the smallness of gaps in a set of natural numbers defining a restricted counting class. One open problem is to make explicit, in a smooth and complete fashion, this trade-off between gaps and ambiguity. Another challenge is to capture the relationship between $\log^{\circledast}$ and $\log^*$ more tightly than Proposition 4.17 does (see Section 4 of [26]). Finally, though it would be a major advance since not even any infinite, P-printable subsets of the primes are currently known, in light of Corollaries 4.11 and 4.20, a natural goal would be to prove that the primes have infinite, P-printable subsets that satisfy some, or all, of our nongappiness properties.

References

1 M. Agrawal, N. Kayal, and N. Saxena. PRIMES is in P. *Annals of Mathematics*, 160(2):781–793, 2004.

2 E. Allender. Some consequences of the existence of pseudorandom generators. *Journal of Computer and System Sciences*, 39(1):101–124, 1989.

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

4 R. Beigel. On the relativized power of additional accepting paths. In *Proceedings of the 4th Structure in Complexity Theory Conference*, pages 216–224. IEEE Computer Society Press, June 1989.

5 R. Beigel, J. Gill, and U. Hertrampf. Counting classes: Thresholds, parity, mods, and fewness. In *Proceedings of the 7th Annual Symposium on Theoretical Aspects of Computer Science*, pages 49–57. Springer-Verlag Lecture Notes in Computer Science #415, February 1990.

6 L. Berman. *Polynomial Reducibilities and Complete Sets.* PhD thesis, Cornell University, Ithaca, NY, 1977.

7 B. Borchert, L. Hemaspaandra, and J. Rothe. Restrictive acceptance suffices for equivalence problems. *London Mathematical Society Journal of Computation and Mathematics*, 3:86–95, 2000.

8 B. Borchert and F. Stephan. Looking for an analogue of Rice's Theorem in circuit complexity theory. *Mathematical Logic Quarterly*, 46(4):489–504, 2000.

9 D. Bovet, P. Crescenzi, and R. Silvestri. Complexity classes and sparse oracles. *Journal of Computer and System Sciences*, 50(3):382–390, 1995.

10 G. Brassard. Crusade for a better notation. *SIGACT News*, 17(1):60–64, 1985.

11 G. Brassard and P. Bratley. *Algorithmics: Theory & Practice.* Prentice Hall, 1988.

12 J.-Y. Cai, T. Gundermann, J. Hartmanis, L. Hemachandra, V. Sewelson, K. Wagner, and G. Wechsung. The boolean hierarchy II: Applications. *SIAM Journal on Computing*, 18(1):95–111, 1989.

13 J.-Y. Cai and L. Hemachandra. On the power of parity polynomial time. *Mathematical Systems Theory*, 23(2):95–106, 1990.

14 C. Caldwell. Heuristics model for the distribution of Mersennes. The PrimePages, 2021. URL verified 2022/6/22. URL: `https://primes.utm.edu/mersenne/heuristic.html`.

15 P. Chebyshev. Mémoire sur les nombres premiers. *Journal de Mathématiques Pures et Appliquées. Série 1*, 17:366–390, 1852.

16 J. Cox and T. Pay. An overview of some semantic and syntactic complexity classes. Technical report, Computing Research Repository, June 2018. `arXiv:1806.03501`.

17 S. Fenner, L. Fortnow, and S. Kurtz. Gap-definable counting classes. *Journal of Computer and System Sciences*, 48(1):116–148, 1994.

18 S. Fenner, L. Fortnow, and L. Li. Gap-definability as a closure property. *Information and Computation*, 130(1):1–17, 1996.

19 K. Ford, B. Green, S. Konyagin, J. Maynard, and T. Tao. Long gaps between primes. *Journal of the American Mathematical Society*, 31(1):65–105, 2018.

20 K. Ford, B. Green, S. Konyagin, and T. Tao. Large gaps between consecutive prime numbers. *Annals of Mathematics. Second Series*, 183(3):935–974, 2016.

21 J. Gill. Computational complexity of probabilistic Turing machines. *SIAM Journal on Computing*, 6(4):675–695, 1977.

22 D. Gillies. Three new Mersenne primes and a statistical theory. *Mathematics of Computation*, 18(85):93–97, 1964. Corrigendum 31(140):1051, 1977.

23 L. Goldschlager and I. Parberry. On the construction of parallel computers from various bases of boolean functions. *Theoretical Computer Science*, 43(1):43–58, 1986.

24 J. Grollmann and A. Selman. Complexity measures for public-key cryptosystems. *SIAM Journal on Computing*, 17(2):309–335, 1988. `doi:10.1137/0217018`.

25 J. Hartmanis and Y. Yesha. Computation times of NP sets of different densities. *Theoretical Computer Science*, 34(1–2):17–32, 1984.

26 L. Hemaspaandra, M. Juvekar, A. Nadjimzadah, and P. Phillips. Gaps, ambiguity, and establishing complexity-class containments via iterative constant-setting. Technical report, Computing Research Repository, September 2021. Revised, June 2022. `arXiv:2109.147648`.

27 L. Hemaspaandra and M. Ogihara. *The Complexity Theory Companion*. Springer-Verlag, 2002.

28 L. Hemaspaandra and J. Rothe. A second step towards complexity-theoretic analogs of Rice's Theorem. *Theoretical Computer Science*, 244(1–2):205–217, 2000.

29 L. Hemaspaandra and M. Zimand. Strong forms of balanced immunity. Technical Report TR-480, Department of Computer Science, University of Rochester, Rochester, NY, December 1993. Revised, May 1994.

30 K. Ko. On some natural complete operators. *Theoretical Computer Science*, 37(1):1–30, 1985.

31 J. Köbler, U. Schöning, S. Toda, and J. Torán. Turing machines with few accepting computations and low sets for PP. *Journal of Computer and System Sciences*, 44(2):272–286, 1992.

32 K.-J. Lange and P. Rossmanith. Unambiguous polynomial hierarchies and exponential size. In *Proceedings of the 9th Structure in Complexity Theory Conference*, pages 106–115. IEEE Computer Society Press, June/July 1994.

33 J. Maynard. Large gaps between primes. *Annals of Mathematics, Second Series*, 183(3):915–933, 2016.

34 C. Papadimitriou and S. Zachos. Two remarks on the power of counting. In *Proceedings of the 6th GI Conference on Theoretical Computer Science*, pages 269–276. Springer-Verlag Lecture Notes in Computer Science #145, January 1983.

35 C. Pomerance. Recent developments in primality testing. *The Mathematical Intelligencer*, 3(3):97–105, 1981.

36 L. Valiant. The relative complexity of checking and evaluating. *Information Processing Letters*, 5(1):20–23, 1976.

37 L. Valiant. The complexity of computing the permanent. *Theoretical Computer Science*, 8(2):189–201, 1979.

38 S. Wagstaff, Jr. Divisors of Mersenne numbers. *Mathematics of Computation*, 40(161):385–397, 1983.

39 O. Watanabe. On hardness of one-way functions. *Information Processing Letters*, 27(3):151–157, 1988.

40 Wikipedia. Prime gap. en.wikipedia.org/wiki/Prime_gap, 2021. URL verified 2022/6/22.

41 Wikipedia. Gillies' conjecture. en.wikipedia.org/wiki/Gillies%27_conjecture, 2022. URL verified 2022/6/22.