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

LANE A. HEMASPAANDRA, University of Rochester, Rochester, USA
MANDAR JUVEKAR, University of Rochester, Rochester, USA
ARIAN NADJIMZADAH, University of Rochester, Rochester, USA
PATRICK A. PHILLIPS, University of Rochester, Rochester, USA

Cai and Hemachandra used iterative constant-setting to prove that Few $\subseteq \oplus$P (and thus that FewP $\subseteq \oplus$P). In this article, 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 "nongappiness") 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 $(O(1) + \log\log n)$-ambiguity NP sets are in the restricted counting class $\mathrm{RC}_{\mathrm{PRIMES}}$.

CCS Concepts: • **Theory of computation → Complexity classes;**

Additional Key Words and Phrases: Structural complexity theory, computational complexity theory, ambiguity-limited NP, restricted counting classes, P-printable sets

ACM Reference Format:
Lane A. Hemaspaandra, Mandar Juvekar, Arian Nadjimzadah, and Patrick A. Phillips. 2024. Gaps, Ambiguity, and Establishing Complexity-Class Containments via Iterative Constant-Setting. *ACM Trans. Comput. Theory* 16, 4, Article 20 (November 2024), 26 pages. https://doi.org/10.1145/3652851

M. Juvekar's work on this article was done in part while at Boston University. A. Nadjimzadah's work on this article was done in part while at UCLA. P. A. Phillips's work on this article was done in part while at Riverside Research. A preliminary version of this article appeared in the *Proceedings of the 47th International Symposium on Mathematical Foundations of Computer Science (MFCS 2022)* [32].
This work was supported in part by NSF grants CCF-2006496 and DUE-2135431.
Authors' Current Contact Information: Mandar Juvekar, Department of Computer Science, Boston University, Boston, MA, 02215, USA; Arian Nadjimzadah, Department of Mathematics, UCLA, Los Angeles, CA, 90095, USA; Patrick A. Phillips, General Dynamics, Reston, VA, 20190, USA.
Authors' Contact Information: Lane A. Hemaspaandra, University of Rochester, Rochester, NY, USA; e-mail: lane@cs.rochester.edu; Mandar Juvekar, University of Rochester, Rochester, NY, USA; e-mail: mandarj@bu.edu; Arian Nadjimzadah, University of Rochester, Rochester, NY, USA; e-mail: anad@math.ucla.edu; Patrick A. Phillips, University of Rochester, Rochester, NY, USA; e-mail: pphill10@u.rochester.edu.

ACM 1942-3454/2024/11-ART20
https://doi.org/10.1145/3652851

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 [9] is defined by $\mathrm{RC}_S = \{L \mid (\exists f \in \#\mathrm{P})(\forall x \in \Sigma^*)[(x \notin L \implies f(x) = 0) \wedge (x \in L \implies f(x) \in S)]\}$, where #P is Valiant's [48] counting version of NP (see Section 2). In other words, 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, although this is an extreme case, $\mathrm{NP} = \mathrm{RC}_{\mathbb{N}^+}$.

In the 1970s, Valiant [47] started the study of ambiguity-limited versions of NP by introducing the class UP, unambiguous polynomial time, which in the preceding notation is simply $\mathrm{RC}_{\{1\}}$. (The ambiguity (limit) of an NPTM refers to an upper bound on how many *accepting* 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 (the class FewP of Allender and Rubinstein [3]) have been defined and studied.

In this article, we show that many ambiguity-limited counting classes—including ones based on types of logarithmic ambiguity, loglog ambiguity, and logloglog ambiguity—are contained in various collections of restricted counting classes. We do so primarily through two general theorems (Theorems 4.6 and 4.10) that help make clear how, as the size of the "holes" allowed in the sets underpinning the restricted counting classes becomes smaller, one can handle more ambiguity. Building on and generalizing earlier framings [9], we will quantify a set's lack of large holes as its "nongappiness." Our basic notion capturing this (see Definition 4.5) is that a nonempty set is F-nongappy if for each element m in the set there exists an $m' > m$ such that m' also is in the set and satisfies $|m'| \leq F(|m|)$. 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 et al. [6], strengthening Cai and Hemachandra's [16] result $\mathrm{FewP} \subseteq \oplus\mathrm{P}$, proved that $\mathrm{FewP} \subseteq \mathrm{RC}_{\{1,3,5,\ldots\}}$, and Borchert et al. [9] noted that $\mathrm{FewP} \subseteq \mathrm{RC}_T$ for each nonempty set $T \subseteq \mathbb{N}^+$ that has an easily presented (formally, P-printable [30], whose definition will be given in Section 2) subset V that is $(n + O(1))$-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 article 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 work, 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

Table 1. Summary of Containment Results

If $T \subseteq \mathbb{N}^+$ X, then Y		
X	Y	Reference
has an $(n + O(1))$-nongappy, P-printable subset	FewP $\subseteq$ RC$_T$	[9]
has an $O(n)$-nongappy, P-printable subset	UP$_{\leq O(\log n)} \subseteq$ RC$_T$	Theorem 4.9
has an $O(n \log n)$-nongappy, P-printable subset	UP$_{\leq O(\sqrt{\log n})} \subseteq$ RC$_T$	
for any $c \in \mathbb{N}^+$ has an $n^{2^{c/2}}$-nongappy, P-printable subset	UP$_{\leq O(1)+\frac{\log \log n}{c}} \subseteq$ RC$_T$	Theorem 4.11
for any $k \in \mathbb{N}^+$ has an $n^{(\log n)^k}$-nongappy, P-printable subset	UP$_{\leq O(1)+\frac{1}{\lceil \log(k+1)+1 \rceil}\log\log\log n} \subseteq$ RC$_T$	Theorem 4.21
has a 2^n-nongappy, P-printable subset S	UP$_{\leq \max(1, \lfloor \frac{\log^*(n)-\log^*(\log^*(n)+1)-1}{\lambda} \rfloor)} \subseteq$ RC$_T$, where $\lambda = 4 + \min_{s \in S, \lvert s \rvert \geq 2}(\lvert s \rvert)$	Theorem 4.21
is infinite	UP$_{\leq O(1)} \subseteq$ RC$_T$	Corollary 4.4

Note: Theorem 4.21 also gives a slightly stronger form of the 2^n-nongappiness result than the version stated here.

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 4.6 and 4.10, 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 [16] FewP $\subseteq \oplus$P result was proven (as was an even more general result about a class known as "Few") by the iterative constant-setting technique. Beigel et al. [6], 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 $\subseteq$ RC$_{\{1,3,5,\ldots\}}$ simply and directly rather than by iterative constant-setting. The even more general result of Borchert et al. [9], noted earlier, for its proof resurrected the iterative constant-setting technique, using it to understand one particular level of ambiguity. This present article 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 earlier, 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. The result of Borchert et al. [9] implies that if the set of primes has an $(n+O(1))$-nongappy, P-printable subset, then FewP $\subseteq$ RC$_{\text{PRIMES}}$. However, it is a long-open research issue whether there exists *any* infinite, P-printable subset of the primes, much less an $(n+O(1))$-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 RC$_{\text{PRIMES}}$. 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 [43, 49] (regarding the asymptotic density of the Mersenne primes) implies that UP$_{\leq O(1)+\log\log n} \subseteq$ RC$_{\text{PRIMES}}$. The Lenstra–Pomerance–Wagstaff Conjecture is characterized in Wikipedia [51] as being "widely accepted," the fact that it disagrees with a different conjecture (Gillies' Conjecture [26]) notwithstanding.

2 Definitions

$\mathbb{N} = \{0, 1, 2, \dots\}$. $\mathbb{N}^+ = \{1, 2, \dots\}$. 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 $= \{i \in \mathbb{N} \mid i \text{ is a prime}\} = \{2, 3, 5, 7, 11, \dots\}$. A composite number is one that has at least one positive divisor other than 1 and itself; COMPOSITES $= \{i \in \mathbb{N} \mid i \text{ is a composite number}\} = \{4, 6, 8, 9, 10, 12, \dots\}$. $\mathbb{R}$ 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 logarithms in this article—including those involved in log, loglog, and logloglog, those invoked by the definitions of $\log^{[i]}$ and $\log^*$ in the next paragraph, and also those in the definition of our new $\log^{\circledast}$ which appears later—are base 2. Additionally, each call of the log function in this article, $\log(\cdot)$, 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 work except incidentally when iterated logs drop something into it, and also in the definitions of $\log^*$ and $\log^{\circledast}$, but in those cases we will argue that the max happens not to change what those evaluate to there.)

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 $\log^{[0]}(0) = 0$.[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 [48] 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 $x \in L \iff f(x) \equiv 1 \pmod 2$ [27, 42].

We will use O in its standard sense—namely, if f and g are functions (from whose domain negative numbers are typically excluded), then we say $f(n) = O(g(n))$ 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 O expression as representing a set of functions (e.g., writing $f(n) \in O(g(n))$) [12, 13], 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 [50] implicitly and Beigel [5] explicitly studied the constant-ambiguity classes $\mathrm{RC}_{\{1,2,3,\dots,k\}}$ which, following the notation of Lange and Rossmanith [39], 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 $\mathrm{UP}_{\leq O(1)}$ 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 $\mathrm{UP}_{\leq O(1)}$ was defined in the literature more than a quarter of a century ago [35]. $\mathrm{UP}_{\leq O(1)}$ 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, $\mathrm{UP}_{\leq O(\log n)}$ 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 $\mathrm{FewP} = \{L \mid (\exists \text{ polynomial } f)[L \in \mathrm{UP}_{\leq f(n)}]\}$.

[1] Since the definition of $\log^*(\cdot)$ allows values on the interval [0, 1), one might worry that the fact that we have globally redefined $\log(\cdot)$ to implicitly be $\log(\max(1, \cdot))$ might be changing what $\log^*(\cdot)$ evaluates to. However, it is easy to see that, with or without the max, what this evaluates to in the range [0, 1) is 0, and so our implicit max is not changing the value of $\log^*$.

The $\mathrm{UP}_{\leq f(n)}$ classes, which will be central to this article'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.[2]

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.*

We say a function f is nondecreasing if $n \leq n'$ implies $f(n) \leq f(n')$. Proposition 2.1 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 $f : \mathbb{N} \to \mathbb{N}^+$. However, many concrete special cases are well known, and the proposition follows from the same argument as is used for those (see for example [33, 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 [29, 37]), $\mathrm{UP}_{\leq k}$ (for each $k \in \mathbb{N}^+$) and $\mathrm{UP}_{\leq O(1)}$ (in [5, 35]), FewP (in [3]), and (since the following is another name for NP) $\mathrm{UP}_{\leq 2^{n^{O(1)}}}$ (folklore, see [33, 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., $\mathrm{UP}_{\leq O(\log n)}$).

We pause from our presentation of definitions to discuss whether there even are sets that fall in such classes as $\mathrm{UP}_{\leq 2}$ or $\mathrm{UP}_{\leq O(\log n)}$ yet are not also obviously even in UP. In terms of directly defined, highly concrete, natural examples, to the best of our knowledge, none are yet known. But the lack of currently known concrete sets does not mean that the study is without value. Ambiguity is a natural resource, and complexity tries to better understand the relationships between different model and resource restrictions, such as between limited ambiguity and restricted counting classes.

However, we in fact will now give three different types of indirect constructions that put sets into, for example, such limited ambiguity classes as $\mathrm{UP}_{\leq O(\log n)}$. In each of our three construction types, there is no obvious argument that the sets constructed belong to UP. Thus, the approaches are providing candidates sets for, for example, $\mathrm{UP}_{\leq O(\log n)} - \mathrm{UP}$.

One type is implicit in the proofs underpinning Proposition 2.1 and the results in the paragraph that follows it. Using logarithmic ambiguity as our example, each $O(\log n)$-to-1 honest, polynomial-time computable function f implicitly (from the construction underpinning Proposition 2.1) defines a set L_f that is in $\mathrm{UP}_{\leq O(\log n)}$. (Additionally, L_f has the property that if $L_f \in \mathrm{P}$, then f is polynomial-time invertible.) We see no obvious way of showing that L_f will be in UP. Similar claims hold for the other density bounds. So low-ambiguity sets are in fact closely tied, via Proposition 2.1, to whether low-injectivity (complexity-theoretic) one-way functions exist.

The second type of construction of sets in, for example, $\mathrm{UP}_{\leq O(\log n)}$ comes from looking at downward disjunctive reducibility cones—that is, taking an "or" of a collection of queries to a UP set. Namely, the class $\mathrm{R}^p_{O(\log n)\text{-dtt}}(\mathrm{UP})$ is clearly contained in $\mathrm{UP}_{\leq O(\log n)}$ (and so is $\mathrm{R}^p_{O(\log n)\text{-T}}(\mathrm{UP})$, since that equals $\mathrm{R}^p_{O(\log n)\text{-dtt}}(\mathrm{UP})$). Briefly, a set L is in $\mathrm{R}^p_{O(\log n)\text{-dtt}}(\mathrm{UP})$ if there is a UP set A_L, such that on input x we can in polynomial time compute a list of $O(\log |x|)$ strings such that $x \in L$ exactly

[2] 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 $g(h(y)) = y$) [29]. 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-1 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, although Proposition 2.1 shows that the notions are closely connected.)

if at least one string in our list belongs to A_L. The class $\mathrm{R}^{p}_{O(\log n)\text{-T}}(\mathrm{UP})$ is defined the same way except instead of nonadaptive queries the machine can ask $O(\log n)$ sequential (i.e., adaptive) oracle queries to A_L, but must accept exactly if at least one belongs to A_L. To make this a bit more concrete, note that from each UP set, A, we get the following simple example of such an $\mathrm{R}^{p}_{O(\log n)-\mathrm{dtt}}(\mathrm{UP})$ set, which by the preceding comment will also belong to $\mathrm{UP}_{\leq O(\log n)}$: At-Least-One-of-Short-List$_A$ = $\{(I_1, I_2, I_3, \ldots, I_k) \mid k \leq \log(\sum_{1 \leq i \leq k} |I_i|) \wedge \{I_1, I_2, I_3, \ldots I_k\} \cap A \neq \emptyset\}$—that is, the set of all lists of potential instances of A such that at least one member of the list belongs to A and the number of items in the list is quite small relative to the size of the list's encoding. If A in fact belongs to UP $\cap$ coUP then At-Least-One-of-Short-List$_A$ in fact is itself in UP $\cap$ coUP (since $\mathrm{P}^{\mathrm{UP} \cap \mathrm{coUP}} = \mathrm{UP} \cap \mathrm{coUP}$); so for this example to have any possible chance of escaping UP, we need A to be a set in UP $-$ coUP.[3]

There exists a third approach to placing sets within bounded-ambiguity classes, which comes from Theorem 5 of an article by Allender and Rubinstein [3]. That approach—which Allender and Rubinstein do for the case of FewP but which, with the natural adjustment of changing the degree of sparseness, would also apply to our classes—however creates, via prefix sets, *sparse* sets in FewP (or our other bounded-ambiguity classes). And that is a higher hurdle than merely putting *some* sets interestingly in our classes. In fact, the preceding one-way functions approach completely characterizes whether the classes collapse to P, and the Allender–Rubinstein approach completely characterizes whether the sparse sets in the class collapse to the sparse sets in P. In both cases, the issue of whether the constructed sets are in UP is an open one; we see no obvious argument that the sets will be in UP, but that is not a guarantee.

Returning to definitions, a set L is said to be P-printable [30] 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 article. Borchert et al. [9] 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 article.

Definition 2.2 ([9]). A set $S \subseteq \mathbb{N}^+$ is said to be nongappy$_{\text{value}}$ 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. In other words, 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. Note that throughout this article, for strings x, we use $|x|$ to refer to the number of characters in the string x but, as one can see in the following proposition, for natural numbers m, we use $|m|$ to refer to the length of the binary representation of m.

[3]Most complexity theorists probably suspect that UP $\neq$ coUP (equivalently, UP $-$ coUP $\neq \emptyset$), although likely with less conviction than they suspect its famous ambiguity-unbounded analogue, NP $\neq$ coNP. Both of those results in fact are known to hold with probability one relative to a random oracle (respectively by Hemaspaandra and Zimand [36] and by the seminal work of Bennett and Gill [7]), although that is not known to be determinative of whether they hold in the unrelativized world.

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 et al. [9].

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

The issue of sets having nongappy (in various strengths of that notion), P-printable subsets will be very important to our work. Let us give a simple example that helps illustrate some of these notions, and does so by giving a nongappy, P-printable subset of SAT (naturally encoded). It is not known whether all $(n + O(1))$-nongappy NP-complete sets have $(n + O(1))$-nongappy, P-printable subsets (or even have any infinite, P-printable subset at all). (We mention in passing that it is not hard to see there are NP-complete sets that are not $(n + O(1))$-nongappy. Those sets trivially cannot have $(n+O(1))$-nongappy subsets, which is why in this example, to be fair, we focus only on $(n + O(1))$-nongappy NP-complete sets.) However, in its natural encoding, SAT clearly does have $(n + O(1))$-nongappy, P-printable subsets—for example, {"v", "$v \vee v$", "$v \vee v \vee v$", ...}, where v is some fixed variable name. We thus have an example where SAT has a simplicity property (namely, having a $(n + O(1))$-nongappy, P-printable subset) that is not currently known to hold for all $(n + O(1))$-nongappy NP-complete sets.

While at first glance Definition 2.4 might seem to be different from the definition of Borchert et al. [9], it is easy to see that both definitions are equivalent.

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

Proof. Both directions follow immediately from Proposition 2.3. In particular, if S is $(n + O(1))$-nongappy, then there is some function f as in Definition 2.4. Since $f \in O(1)$, clearly there exists a constant $k > 0$ such that $(\forall m \in \mathbb{N}^+)[f(|m|) \leq k]$. Conversely, if S is nongappy$_{\text{value}}$, then there is a constant k as in Proposition 2.3, and since the constant function k is of course $O(1)$, we then have that S is $(n + O(1))$-nongappy. ❑

Finally, the end of the fifth paragraph of Section 1 gave an on-the-fly, quite simple characterization of the $(n + O(1))$-nongappy sets as being the class of all sets $S \subseteq \mathbb{N}^+$ such that, for some $k > 0$, S never has more than k adjacent lengths containing no strings ($k = 0$ was not excluded, but w.l.o.g. we may assume $k > 0$, since if it holds for $k = 0$ it holds for $k = 1$). For completeness, we briefly explain why that indeed is a correct characterization of that notion. In particular, in light of Proposition 2.5, we need only show that, for each set $S \subseteq \mathbb{N}^+$, the just-mentioned characterization holds exactly if the right-hand side of Proposition 2.3 holds. If the former holds with k set to k', then the right-hand side of Proposition 2.3 clearly holds with k set to $k' + 1$. If the right-hand side of Proposition 2.3 holds with k (recall, $k > 0$ there) set to k', then the characterization from Section 1 clearly holds with k set to $\max(k' - 1, \min_{m \in S}(|m|))$.

3 Related Work

The most closely related work has already largely been covered in the preceding sections, but we now briefly mention that work and its relationship to our work. In particular, the most closely related works are those of Cai and Hemachandra [16], Hemaspaandra and Rothe [34], and Borchert et al. [9], 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 [10]) differ from the present article in that they are not about restricted counting classes, and unlike the present article, the work of Borchert et al. [9], 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 [21, 22, 38]; 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 important work of Cox and Pay [20]—along with many other interesting results on counting classes—draws on the result of Borchert et al. [9] that appears as our Theorem 4.1 to establish that FewP $\subseteq \mathrm{RC}_{\{2^t-1 \mid t \in \mathbb{N}^+\}}$ (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 [9] are central to this work. The literature's earlier "CP" classes [15] might at first seem similar, but they do not restrict rejection to the case of having zero accepting paths. Leaf languages [11], a different framework, do have flexibility to express "RC" classes, and so are an alternate notation one could use, although 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 $\mathrm{ModZ}_2\mathrm{P}$ [6]. Ambiguity-limited classes are also quite central to this work, and among those we study (see Section 2) are ones defined, or given their notation that we use, in several works [3, 5, 39, 47, 50].

The counting classes studied in this article are all *language* classes, although each is or can be defined via #P functions. (For example, FewP is the class of all sets L such that, for some polynomial p and some #P function f, we have that for each $x \in \Sigma^*$ it holds that (a) $x \notin L \implies f(x) = 0$, and (b) $x \in L \implies 1 \leq f(x) \leq p(|x|)$. Note that there is a restriction in play there, namely, that the #P function underpinning L will on no input x take on any value strictly greater than $p(|x|)$.) The direct study of *counting classes of functions*, and the properties and interrelations of those classes, is an active research area, although we mention that to the best of our knowledge the results of the present article do not follow from any currently known results in that area. As a pointer to some of the interesting current research in that area, we mention the work of Antonopoulos et al. [4] and Chalki [18]. Finally, interesting but fundamentally different in flavor from our work is the broad stream of work focused on completely classifying the complexity of various *families of counting problems* see, e.g., [14].

P-printability is due to Hartmanis and Yesha [30]. 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 5, none of the results of Ford, Maynard, Tao, and others [23, 24, 40] 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.[4]

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 et al. [9] and Cox and Pay [20]. In particular, Borchert et al. showed, by the iterative constant-setting technique, the following theorem.

Theorem 4.1 ([9, Theorem 3.4]). *If $T \subseteq \mathbb{N}^+$ has an $(n + O(1))$-nongappy, P-printable subset, then* $\mathrm{FewP} \subseteq \mathrm{RC}_T$.

From this, we immediately have the following corollary.

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

Does PRIMES contain an $(n + O(1))$-nongappy, P-printable subset? The Bertrand–Chebyshev Theorem [19] states that for each natural number $k > 3$, there exists a prime p such that $k < p < 2k - 2$. Thus, PRIMES clearly has an $(n + O(1))$-nongappy subset.[5] Indeed, since—with p_i denoting the ith prime—$(\forall \epsilon > 0)(\exists N)(\forall n > N)[p_{n+1} - p_n < (p_n)^{\frac{3}{4}+\epsilon}]$ [46], it certainly 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 $(n + O(1))$-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 RP [25] and the existence of secure extenders. However, that result does not promise that the infinite, P-printable set of primes is $(n + O(1))$-nongappy—not even now, when it is known that primality is not merely in the class RP 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 means that our length gaps between adjacent elements of our P-printable set must be bounded by an additive constant. Can we

[4] One should not think that the fact that $\mathrm{NP} \subseteq \mathrm{RC}_{\mathrm{COMPOSITES}}$ (equivalently, $\mathrm{NP} = \mathrm{RC}_{\mathrm{COMPOSITES}}$) holds means that $\mathrm{coNP} \subseteq \mathrm{RC}_{\mathrm{PRIMES}}$; the latter in fact would immediately imply that NP = coNP, since for each $S \subseteq \mathbb{N}^+$ it holds that $\mathrm{RC}_S \subseteq \mathrm{NP}$. As to whether the fact that $\mathrm{NP} \subseteq \mathrm{RC}_{\mathrm{COMPOSITES}}$ holds means that $\mathrm{coNP} \subseteq \mathrm{RC}_{\mathbb{N}-\mathrm{COMPOSITES}}$ holds, the latter is not even well defined, since the RC classes are defined only for sets S satisfying $S \subseteq \mathbb{N}^+$. But even if one removes 0, and asks about $\mathrm{coNP} \subseteq \mathrm{RC}_{\mathbb{N}^+-\mathrm{COMPOSITES}}$, for the same reason just mentioned that containment would imply NP = coNP.

[5] We mention in passing that it follows from the fact that PRIMES clearly *does* have an $(n + O(1))$-nongappy subset that none of the powerful results by Ford, Maynard, Tao, and others [23, 24, 40] 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—that is, whether there is such an $(n + O(1))$-nongappy subset of the primes that is P-printable.

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 tradeoff 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.

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 [34, p. 210] of an NP-many-one-hardness result of Borchert and Stephan [10] and a $\mathrm{UP}_{\leq k}$-1-truth-table-hardness result. In particular, both of those results are in the *un*restricted setting, and so neither implies Theorem 4.3.

The proof of Theorem 4.3 is in Appendix A. However, we recommend that the reader read it, if at all, only after reading the proof of Theorem 4.6, whose proof also uses (and within this article, is the first presentation of) iterative constant-setting, and is a more interesting use of that approach.

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

So constant-ambiguity nondeterminism can be done by the restrictive counting class based on the primes (as Corollary 4.4 immediately yields $\mathrm{UP}_{\leq O(1)} \subseteq \mathrm{RC}_{\mathrm{PRIMES}}$). 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 ($\mathrm{UP}_{\leq O(1)}$) and polynomial ambiguity (FewP). Just as Corollary 4.2 follows from Theorem 4.1, so also do each of our Theorems 4.9 and 4.21 (Parts 1 through 3) each have the obvious analogous corollary regarding $\mathrm{RC}_{\mathrm{PRIMES}}$.

We first define a broader notion of nongappiness.

Definition 4.5. 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 $(\forall m \in S)(\exists m' \in S)[m' > m \wedge |m'| \leq F(|m|)]$.[6]

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 noninteger 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.

[6]In two later definitions, 4.7 and 4.20, we apply Definition 4.5 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 (Definition 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 (although the definition given in Definition 2.4 is consistent with the lifting reading, give or take the fact that we have now broadened our focus to the reals rather than the naturals).

The following theorem generalizes the iterative constant-setting technique that Borchert et al. [9] used to prove Theorem 4.1.

Theorem 4.6. *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 $\beta \in \mathbb{N}^+$, $F^{[j(n)]}(\lambda) = O(n^\beta)$, then $\mathrm{UP}_{\leq j(n)} \subseteq \mathrm{RC}_T$.*

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 conditions from the theorem statement.

Proof of Theorem 4.6. Let F, j, n_0, T, and S be as per the theorem statement. Suppose $(\exists \beta' \in \mathbb{N}^+)[F^{[j(n)]}(\lambda) = O(n^{\beta'})]$, and fix a value $\beta \in \mathbb{N}^+$ such that $F^{[j(n)]}(\lambda) = O(n^\beta)$. 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 $a_n > b_n$. Finally, we set $c_n = a_n - b_n$. We now show that $\max_{2 \leq \ell \leq j(n)} |a_\ell|$ 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 construction and since S is F-nongappy, we have $|c_i| \leq |a_i| \leq F(|b_i|)$. Using our definition of b_i from Equation (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 $|b_i| \leq 2i + \max_{1 \leq k \leq i-1} |c_k|$. 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 $\max_{2 \leq \ell \leq j(n)} |b_\ell|$ is at most polynomial in n, and since for all i, $a_i = b_i + c_i$, $\max_{2 \leq \ell \leq j(n)} |a_\ell|$ 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 via the following claim, which we prove by induction: for all $i \in \{2, 3, \ldots\}$, $\max_{1 \leq \ell \leq i} |c_\ell| \leq (i-1)F^{[(i-1)]}(\lambda)$. We showed in the previous paragraph that for any $i \in \{2, 3, \ldots\}$, $|c_i| \leq F(|b_i|)$ and $|b_i| \leq 2i + \max_{1 \leq k \leq i-1} |c_k|$. For each $i \in \{2, 3, \ldots\}$, we have $|b_i| \geq |c_1| \geq n_0$. Since F restricted to $\{t \in \mathbb{R}^+ \mid t \geq n_0\}$ is nondecreasing, for all $i \in \{2, 3, \ldots, n\}$,

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

Recall that $\lambda = 4 + |c_1|$. For the base case of our induction, notice that substituting $i = 2$ into Equation (2) gives $|c_2| \leq F(4 + |c_1|) = F(\lambda)$. Additionally, by condition (a) and the fact that $|c_1| \geq n_0$, we have $|c_1| < F(|c_1|) \leq F(4 + |c_1|) = F(\lambda)$. Thus, $\max_{1 \leq \ell \leq 2} |c_\ell| \leq F(\lambda)$, which is the claimed inequality for $i = 2$. Suppose, for induction, that the claim holds for some $i \geq 2$. Since $|c_1| \geq n_0$, condition (a) and the fact that F restricted to $\{t \in \mathbb{R}^+ \mid t \geq n_0\}$ is nondecreasing give us $F^{[i-1]}(\lambda) = F^{[i-1]}(4 + |c_1|) \geq 2(i-1) + 4 + |c_1| \geq 2(i+1)$. Plugging $i+1$ into Equation (2) and using the fact that all the inputs to F involved are greater than n_0 (and so are in the domain where F is nondecreasing),

we have

$$\begin{aligned}
|c_{i+1}| &\le F(2(i+1) + \max_{1\le \ell \le i} |c_\ell|) \\
&\le F(2(i+1) + (i-1)F^{[i-1]}(\lambda)) && \text{(by the inductive hypothesis)} \\
&\le F(F^{[i-1]}(\lambda) + (i-1)F^{[i-1]}(\lambda)) \\
&= F(iF^{[i-1]}(\lambda)) \\
&\le iF^{[i]}(\lambda). && \text{(by condition (b))}
\end{aligned}$$

Since $\max_{1\le \ell \le i} |c_\ell| \le (i-1)F^{[i-1]}(\lambda) \le iF^{[i]}(\lambda)$, we have $\max_{1\le \ell \le i+1} |c_\ell| \le iF^{[i]}(\lambda)$, which is the claimed inequality for $i+1$. By induction, the claim holds.

Substituting $i = j(n)$ into the inequality we just proved, we get $\max_{1\le \ell \le j(n)} |c_\ell| \le j(n)F^{[j(n)]}(\lambda)$. Since $F^{[j(n)]}(\lambda) = O(n^\beta)$ and by hypothesis $j(n)$ is at most polynomial in n, $j(n)F^{[j(n)]}(\lambda)$ is at most polynomial in n. Hence, $\max_{1\le \ell \le j(n)} |c_\ell|$ is at most polynomial in n.

We now proceed to show that $\mathrm{UP}_{\le j(n)} \subseteq \mathrm{RC}_T$. Let L be a language in $\mathrm{UP}_{\le j(n)}$, witnessed by an NPTM $\hat{N}$. To show $L \in \mathrm{RC}_T$, we give a description of 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 earlier. Note that this computation relies on the P-printability of S, which ensures that the constants a_i (which must be computed to compute c_i) are computable. 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. Of course, if $\hat{N}(x)$ has fewer than i paths, then the subtree of N that guessed i will have zero 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 $L \in \mathrm{UP}_{\le j(n)}$, we must have $1 \le k \le j(|x|)$. 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 $\#\mathrm{acc}_N(x) = \sum_{1\le \ell \le k} c_\ell \binom{k}{\ell}$. If $k = 1$, we have $\#\mathrm{acc}_N(x) = c_1$. If $2 \le k \le j(|x|)$, then $\#\mathrm{acc}_N(x) = c_k + \sum_{1\le \ell \le k-1} c_\ell \binom{k}{\ell} = c_k + b_k = a_k$. 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 $\max_{1\le i \le j(|x|)} |a_i|$ is at most polynomial in $|x|$, finding the constants a_i can be done in time polynomial in $|x|$. Additionally, since $\max_{1\le i \le j(|x|)} |c_i|$ 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 Equation (1)).

Theorem 4.6 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 4.9—that this notion of nongappiness allows us to accept all sets of logarithmic ambiguity.

Definition 4.7. A set $S \subseteq \mathbb{N}^+$ is $O(n)$-nongappy if $S \neq \emptyset$ and $(\exists f \in O(n))(\forall m \in S)(\exists m' \in S)[m' > m \wedge |m'| \leq f(|m|)]$.

As Fact 4.8, we note that one can view this definition in a form similar to the definition of Borchert et al. [9] to see that $O(n)$-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.)

Fact 4.8. *A set $S \subseteq \mathbb{N}^+$ is $O(n)$-nongappy if and only if there exists $k \in \mathbb{N}^+$ such that S is kn-nongappy.*

Proof. As to the "only if" direction, suppose S is $O(n)$-nongappy. By definition of $O(n)$-nongappy, $S \neq \emptyset$ and there is a function $f \in O(n)$ such that $(\forall m \in S)(\exists m' \in S)[m' > m \wedge |m'| \leq f(|m|)]$. Since f is $O(n)$, we can find constants k_0 and n_0 in $\mathbb{N}^+$ such that $(\forall t \geq n_0)[f(t) \leq k_0 t]$. Let $k = \max(f(1), f(2), \ldots, f(n_0), k_0)$. Then for all $n \in \mathbb{N}^+$, $f(n) \leq kn$. (Even though f has domain $\mathbb{R}^+$, it is enough to have this bound just for the positive natural numbers since our definition of nongappy only invokes the function on positive naturals.) It is easy to see that this k is such that S is kn-nongappy. As to the "if" direction, kn is certainly $O(n)$. ❑

Theorem 4.9. *If $T \subseteq \mathbb{N}^+$ has an $O(n)$-nongappy, P-printable subset, then $\mathrm{UP}_{\leq O(\log n)} \subseteq \mathrm{RC}_T$.*

Proof. Suppose $T \subseteq \mathbb{N}^+$ has an $O(n)$-nongappy, P-printable subset. By the "only if" direction of Fact 4.8, 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 4.6 since for all $t \geq 2$, $F(t) = kt \geq t + 2$, $(\forall c \in \mathbb{N}^+)[cF(n) = ckn = F(cn)]$, 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 $g(n) = O(\log n)$, 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 4.6 since $j(n)$ can be computed in time polynomial in n (e.g., by doing a linear search for the largest $i \in \mathbb{N}$ such that $2^i \leq (n+2)^d$) and has value at most polynomial in n. Applying Theorem 4.6, 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 $F^{[j(n)]}(\lambda) = O(n^\beta)$. So it suffices to show that for some $\beta \in \mathbb{N}^+$ and for sufficiently large 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 there exists β such that for sufficiently large n, $k^{j(n)}\lambda \leq n^\beta$, or (taking logs) equivalently that for large n, $\lfloor d \log(n+2) \rfloor \log k + \log \lambda \leq \beta \log n$. The left-hand side of this inequality is at most $d \log(n+2) \log k + \log \lambda \leq \log(n)[2d \log k + \log \lambda]$ which, for all $\beta \geq 2d \log k + \log \lambda$, is at most $\beta \log n$. Thus, there exits a constant β such that $F^{[j(n)]}(\lambda) = O(n^\beta)$. Hence, for any function $g : \mathbb{N} \to \mathbb{R}^{\geq 1}$ satisfying $g(n) = O(\log n)$, we have that there exists a function j such that $\mathrm{UP}_{\leq g(n)} \subseteq \mathrm{UP}_{\leq j(n)} \subseteq \mathrm{RC}_T$. ❑

For the iterative constant-setting approach used in Theorem 4.6 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 4.6 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 4.6 is flexible enough to, by a proof similar to that of Theorem 4.9, imply the result of Borchert et al. [9] stated in Theorem 4.1 where j reaches its polynomial bound.

Another limitation of Theorem 4.6 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, $(\forall c \in \mathbb{R}^{\geq 1})[cF(t) \leq F(ct)]$, which we now do as Theorem 4.10. For each of the F-nongappy set classes that seemed most interesting to us, one of these two conditions turned out to hold for F, and so one of the two results shown in Theorems 4.6 and 4.10 was applicable in finding the ambiguity-limited class that is contained in a restricted counting class associated with a set of natural numbers with some F-nongappy, P-printable subset.

Theorem 4.10. *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) $(\forall c \in \mathbb{R}^{\geq 1})[cF(t) \leq F(ct)]$. 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, $F^{[j(n)]}(j(n)\lambda) = O(n^\beta)$, then $\mathrm{UP}_{\leq j(n)} \subseteq \mathrm{RC}_T$.*

How does this theorem compare with our other metatheorem, Theorem 4.6? Since in both metatheorems F is nondecreasing after a prefix, speaking informally and broadly, the functions F where (after a prefix) $(\forall c \in \mathbb{R}^{\geq 1})[cF(t) \leq F(ct)]$ 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).

Proof of Theorem 4.10. The proof follows almost identically to the proof of Theorem 4.6. Let F, j, n_0, T, and S be as per the theorem statement. Suppose $(\exists \beta' \in \mathbb{N}^+)[F^{[j(n)]}(j(n)\lambda) = O(n^{\beta'})]$, and let $\beta \in \mathbb{N}^+$ be some specific, fixed β' value instantiating that. We define the sequences of constants a_n, b_n, and c_n exactly as in the proof of Theorem 4.6. We now show that $\max_{2 \leq \ell \leq j(n)} |a_\ell|$ and $\max_{1 \leq \ell \leq j(n)} |c_\ell|$ are at most polynomial in n. For the same reasons as in the proof of Theorem 4.6, if $\max_{1 \leq \ell \leq j(n)} |c_\ell|$ is at most polynomial in n, then $\max_{2 \leq \ell \leq j(n)} |a_\ell|$ is at most polynomial in n.

We prove that $\max_{1 \leq \ell \leq j(n)} |c_\ell|$ is at most polynomial in n by proving the following claim via induction: for all $i \in \{2, 3, \ldots\}$, $\max_{1 \leq \ell \leq i} |c_\ell| \leq F^{[i-1]}((i-1)\lambda)$. Notice that Equation (2) from the proof of Theorem 4.6, which says that $|c_i| \leq F(2i + \max_{1 \leq k \leq i-1} |c_k|)$ still holds, since deriving it did not use any of the assumptions that are different in that theorem. Plugging in $i = 2$ gives us $|c_2| \leq F(4 + |c_1|) = F(\lambda)$. Additionally, by condition (a) and the fact that $|c_1| \geq n_0$, $|c_1| < F(|c_1|)$ which, since F restricted on $\{t \in \mathbb{R}^+ \mid t \geq n_0\}$ is nondecreasing, is at most $F(\lambda)$. Thus, $\max_{1 \leq k \leq 2} |c_k| \leq F(\lambda)$, which is the $i = 2$ case of our claim. Suppose now that the claim holds for some $i \geq 2$. Since

$\lambda \geq 4$, we have $2(i+1) \leq 2(i+1)+\lambda-4$. Condition (a) implies $2(i+1) \leq F^{[i-1]}(\lambda) = \frac{i-1}{i-1}F^{[i-1]}(\lambda)$. Since it follows from condition (b) that for all $\ell \in \mathbb{N}^+$, $c \geq 1$, and $t \geq n_0$, $cF^{[\ell]}(t) \leq F^{[\ell]}(ct)$, we have $2(i+1) \leq \frac{1}{i-1}F^{[i-1]}((i-1)\lambda)$. Plugging $i+1$ into Equation (2), we have

$$\begin{aligned}
|c_{i+1}| &\leq F(2(i+1) + \max_{1\leq k\leq i}|c_k|) \\
&\leq F(2(i+1) + F^{[i-1]}((i-1)\lambda)) && \text{(by the inductive hypothesis)} \\
&\leq F\left(\frac{1}{i-1}F^{[i-1]}((i-1)\lambda) + F^{[i-1]}((i-1)\lambda)\right) \\
&= F\left(\frac{i}{i-1}F^{[i-1]}((i-1)\lambda)\right) \\
&\leq F^{[i]}(i\lambda). && \text{(by condition (b))}
\end{aligned}$$

Since $\max_{1\leq \ell\leq i}|c_\ell| \leq F^{[i-1]}((i-1)\lambda) \leq F^{[i]}(i\lambda)$, we have $\max_{1\leq \ell\leq i+1}|c_\ell| \leq F^{[i]}(i\lambda)$, which, by induction, proves the claim. Plugging $i = j(n)$ into the claim we just proved, we get that $\max_{1\leq \ell\leq j(n)}|c_\ell| \leq F^{[j(n)-1]}((j(n)-1)\lambda) \leq F^{[j(n)]}(j(n)\lambda) = O(n^\beta)$.

Consider any language $L \in \mathrm{UP}_{\leq j(n)}$ witnessed by machine $\hat{N}$. Given $\hat{N}$ and the sequences of constants we defined, we construct a machine N identically to the proof of Theorem 4.6. By the arguments in the proof of that theorem, N accepts L in an RC_T-like fashion, apart from the fact that we have not yet shown N to be an NPTM. As to that final issue, since we showed that $\max_{2\leq i\leq j(n)}|a_i|$ and $\max_{1\leq i\leq j(n)}|c_i|$ are at most polynomial in n, the arguments in the proof of Theorem 4.6 for why N is an NPTM still hold. Thus, $L \in \mathrm{RC}_T$, which completes our proof. ❑

We now discuss some other notions of nongappiness and obtain complexity-class containments regarding them using Theorem 4.10. Theorem 4.11 and its corollary, Corollary 4.13, were flawed in some of the previous versions of this article; we thank an anonymous ACM TOCT referee for spotting the problem.

Theorem 4.11. *For any number $k \in \mathbb{R}^+$ that can be expressed as $k = 2^{c/2}$ for some $c \in \mathbb{N}^+$, if $T \subseteq \mathbb{N}^+$ has an n^k-nongappy, P-printable subset, then $\mathrm{UP}_{\leq O(1)+\frac{\log\log n}{2\log k}} \subseteq \mathrm{RC}_T$.*

Proof. Let c be an arbitrary positive natural number, and let $k = 2^{c/2}$ (notice that $k \geq \sqrt{2}$). Suppose $T \subseteq \mathbb{N}^+$ is a set having an n^k-nongappy, P-printable subset. We argue that $\mathrm{UP}_{\leq O(1)+\frac{\log\log n}{2\log k}} \subseteq \mathrm{RC}_T$.

Set $F : \mathbb{R}^+ \to \mathbb{R}^+$ to be $F(t) = t^k$. F satisfies the conditions on the F in Theorem 4.10 because F is nondecreasing on $\mathbb{R}^+$ (since $k > 0$), and for all $t \geq 4$, we have (a) $t^k - t = t(t^{k-1}-1) \geq 4(4^{\sqrt{2}-1}-1) > 2$, which means $F(t) \geq t+2$, and (b) $(\forall c \in \mathbb{R}^{\geq 1})[cF(t) = ct^k \leq (ct)^k = F(ct)]$. Let $\lambda = 4 + |s|$, where s is the smallest element of the n^k-nongappy, P-printable subset of T where the conditions on F hold for all $t \geq |s|$, i.e., s is the smallest element of the n^k-nongappy, P-printable subset such that $|s| \geq 4$. For every function $g : \mathbb{N} \to \mathbb{R}^{\geq 1}$ satisfying $g(n) = O(1) + \frac{\log\log n}{2\log k}$, there exists a $d \in \mathbb{N}^+$ such that $g(n) \leq \lfloor d + \frac{\log\log n}{2\log k}\rfloor$, and hence $\mathrm{UP}_{\leq g(n)} \subseteq \mathrm{UP}_{\leq \lfloor d+\frac{\log\log n}{2\log k}\rfloor}$.[7] The function $j(n) = \lfloor d + \frac{\log\log n}{2\log k}\rfloor = \lfloor d + \frac{\log\log n}{c}\rfloor$ satisfies the conditions on j of Theorem 4.10, since $j(n)$ can be computed in time polynomial in the value n (since $\lfloor \frac{\log\log n}{c}\rfloor$ can be computed by doing

[7]Note that the expression $d + \frac{\log\log n}{2\log k}$ is not problematic despite the fact that 0 is a valid input since we have globally redefined $\log(\cdot)$ to mean $\log(\max(1,\cdot))$. The same is true for similar expressions that appear in the proof of Theorem 4.21.

a linear search for the largest natural number i such that $2^{2^{ci}} \leq n$) and $j(n)$ has value at most polynomial in the value n. Applying Theorem 4.10, to prove that $\mathrm{UP}_{\leq j(n)} \subseteq \mathrm{RC}_T$ it suffices to show that for some $\beta \in \mathbb{N}^+$ and for sufficiently large n, $F^{[j(n)]}(j(n)\lambda) \leq n^{\beta}$. Plugging in $F^{[j(n)]}(j(n)\lambda) = (j(n)\lambda)^{k^{j(n)}}$ and taking logarithms, we see that this is the same as showing that there exists β such that for sufficiently large n, $j(n)\log k + \log\log(j(n)\lambda) \leq \log\beta + \log\log n$. For large n, $j(n)\log k + \log\log(j(n)\lambda) \leq 2j(n)\log k \leq 2d\log k + \log\log n$.

Setting $\beta = 2^{2d\log k}$ gives us the desired inequality. Thus, for any function $g : \mathbb{N} \to \mathbb{R}^{\geq 1}$ satisfying $g(n) = O(1) + \frac{\log\log n}{2\log k}$, we have shown that there exists a function j such that $\mathrm{UP}_{\leq g(n)} \subseteq \mathrm{UP}_{\leq j(n)} \subseteq \mathrm{RC}_T$ (and so we have $\mathrm{UP}_{\leq g(n)} \subseteq \mathrm{RC}_T$). ❑

Theorem 4.11 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 $(O(1) + \log\log n)$-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 [43, 49] (see also the work of Caldwell [17]) 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 4.12. *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.*

Proof. Assuming the Lenstra–Pomerance–Wagstaff Conjecture, there must be an infinite number of Mersenne primes. For each $i \in \mathbb{N}^+$, let M_i denote the ith Mersenne prime.

The density assertion of the Lenstra–Pomerance–Wagstaff Conjecture implies that $(\forall\delta > 0)(\exists N(\delta) \in \mathbb{N}^+)(\forall n > N(\delta))[(1-\delta)(e^{\gamma}\log n) \leq \mu(n) \leq (1+\delta)(e^{\gamma}\log n)]$. Suppose, by way of seeking a contradiction, that for some $\epsilon > 0$ there are infinitely many n such that for two successive Mersenne primes M_n and M_{n+1}, $|M_{n+1}| > |M_n|^{1+\epsilon}$. Fix a δ satisfying $\delta < \frac{\epsilon}{2(\epsilon+2)}$, and let M_n and M_{n+1} be two consecutive Mersenne primes such that $|M_n| > \max(N(\delta), 2^{\frac{2}{e^{\gamma}\epsilon}})$ and $|M_{n+1}| > |M_n|^{1+\epsilon}$. We have $\mu(|M_n|) \leq (1+\delta)(e^{\gamma}\log|M_n|)$, and since there are no Mersenne primes between M_n and M_{n+1}, $\mu(|M_{n+1}|) \leq 1 + (1+\delta)(e^{\gamma}\log|M_n|)$.[8] We also have that

$$\begin{aligned}\mu(|M_{n+1}|) &\geq (1-\delta)(e^{\gamma}\log|M_{n+1}|)\\ &\geq (1-\delta)(e^{\gamma}\log(|M_n|^{1+\epsilon}))\\ &= (1-\delta)(1+\epsilon)(e^{\gamma}\log|M_n|).\end{aligned}$$

[8]This follows since there can be at most one Mersenne prime of each length, and so in particular M_{n+1} is the sole Mersenne prime of length $|M_{n+1}|$.

Now note that

$$\begin{aligned}
&1 + (1+\delta)(e^{\gamma}\log|M_n|) - (1-\delta)(1+\epsilon)(e^{\gamma}\log|M_n|) \\
&\qquad = 1 + e^{\gamma}(\log|M_n|)((1+\delta) - (1-\delta)(1+\epsilon)) \\
&\qquad < 1 + e^{\gamma}(\log|M_n|)\left(\left(1+\frac{\epsilon}{2(\epsilon+2)}\right) - \left(1-\frac{\epsilon}{2(\epsilon+2)}\right)(1+\epsilon)\right) \\
&\qquad = 1 - e^{\gamma}(\log|M_n|)\left(\frac{\epsilon}{2}\right).
\end{aligned}$$

For $|M_n| > 2^{\frac{2}{e^{\gamma}\epsilon}}$ we have $1 - e^{\gamma}(\log|M_n|)(\frac{\epsilon}{2}) < 0$, and thus for $|M_n| > 2^{\frac{2}{e^{\gamma}\epsilon}}$ we also have $1 + (1+\delta)(e^{\gamma}\log|M_n|) < (1-\delta)(1+\epsilon)(e^{\gamma}\log|M_n|)$. This last inequality yields a contradiction as we have also shown $(1-\delta)(1+\epsilon)(e^{\gamma}\log|M_n|) \leq \mu(|M_{n+1}|) \leq 1 + (1+\delta)(e^{\gamma}\log|M_n|)$.

So for any $\epsilon > 0$, there are only finitely many n such that the consecutive Mersenne primes M_n and M_{n+1} have $|M_{n+1}| > |M_n|^{1+\epsilon}$. Let n_0 be the least integer such that for all $n > n_0$, $|M_{n+1}| \leq |M_n|^{1+\epsilon}$. The set of Mersenne primes $\{M_i \mid i > n_0\}$ is an $n^{1+\epsilon}$-nongappy, P-printable subset of the primes. ❑

Corollary 4.13. *If the Lenstra–Pomerance–Wagstaff Conjecture holds, then* $\mathrm{UP}_{\leq O(1)+\log\log n} \subseteq \mathrm{RC}_{\mathrm{PRIMES}}$ *(indeed,* $\mathrm{UP}_{\leq O(1)+\log\log n} \subseteq \mathrm{RC}_{\mathrm{MersennePRIMES}}$*).*

Proof. Assume that the Lenstra–Pomerance–Wagstaff Conjecture holds. Since $2^{1/2} > 1$, by Theorem 4.12 the Mersenne primes have an $n^{2^{1/2}}$-nongappy, P-printable subset. The conditions of Theorem 4.11 are satisfied with $k = 2^{1/2}$, and so we have $\mathrm{UP}_{\leq O(1)+\frac{\log\log n}{2\log(2^{1/2})}} \subseteq \mathrm{RC}_{\mathrm{MersennePRIMES}}$, and hence $\mathrm{UP}_{\leq O(1)+\log\log n} \subseteq \mathrm{RC}_{\mathrm{MersennePRIMES}} \subseteq \mathrm{RC}_{\mathrm{PRIMES}}$. ❑

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 4.21.

Definition 4.14. 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 $\log^{[k]}(\alpha) \geq k$. Additionally, for all $\ell > \log^{*}(\alpha)$, $\log^{[\ell]}(\alpha) < \log^{[\log^{*}(\alpha)]}(\alpha) \leq 1 \leq \ell$, and so no $\ell > \log^{*}(\alpha)$ can be used as the k in the above definition. 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. Notice that using the definition of $\log^{\circledast}(\alpha)$ and the preceding, 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 definition holds, and so $\log^{\circledast}(\alpha) = 0$ if $\alpha \leq 1$. Thus, for $\alpha \leq 1$, $\log^{\circledast}(\alpha) = \log^{*}(\alpha)$. (Since Definition 4.14's first sentence allows values on the open interval $(0,1)$, one might worry that the fact that we have globally redefined $\log(\cdot)$ to implicitly be $\log(\max(1,\cdot))$ might be changing what $\log^{\circledast}(\alpha)$ evaluates to. However, it is easy to see that, with or without the max, what this evaluates to in the range $(0,1)$ is 0, and so our implicit max is not changing the value of $\log^{\circledast}$.)

We are using a "variant star" notation for $\log^{\circledast}$ because it in fact is related both definitionally and in terms of value to $\log^{*}$. As to its definition, $\log^{\circledast}$ can alternatively be defined as the following, which in form looks far closer to the definition of $\log^{*}$ than does the version in Definition 4.14: "For any $\alpha \in \mathbb{R}$, $\alpha > 0$, $\log^{\circledast}(\alpha)$ is -1 plus the smallest natural number k such that $\log^{[k]}(\alpha) < k$. We define $\log^{\circledast}(0)$ to be 0." As to the relationship of its values to those of $\log^{*}$, we have the following theorem.

Theorem 4.15. *For all* $\alpha \geq 0$, $\log^*(\alpha) - \log^*(\log^*(\alpha)+1) - 1 \leq \log^{\circledast}(\alpha) \leq \log^*(\alpha)$.

Proof. We have for all $\alpha \geq 0$, $\log^{\circledast}(\alpha) \leq \log^*(\alpha)$, which follows from the discussion before this theorem. Take any $\alpha \geq 0$. From the definition of $\log^{\circledast}$, it follows that $\log^{[\log^{\circledast}(\alpha)]}(\alpha) \leq 2^{\log^{\circledast}(\alpha)+1}$, for if not, then we must have $\log^{[\log^{\circledast}(\alpha)]}(\alpha) > 2^{\log^{\circledast}(\alpha)+1}$, which (taking the logarithm of both sides) implies that $\log^{[\log^{\circledast}(\alpha)+1]}(\alpha) > \log^{\circledast}(\alpha)+1$, contradicting the fact that $\log^{\circledast}(\alpha)$ is the greatest number for which such an inequality holds. Notice that for any x, since $\log^*(x)$ is the smallest number of logarithms one needs to apply to x to obtain a result less than or equal to 1, we have that for any $k \leq \log^*(x)$, $\log^*(x) = k + \log^*(\log^{[k]}(x))$. Plugging in $x = \alpha$ and $k = \log^{\circledast}(\alpha)$, we get $\log^*(\alpha) = \log^{\circledast}(\alpha) + \log^*(\log^{[\log^{\circledast}(\alpha)]}(\alpha)) \leq \log^{\circledast}(\alpha) + \log^*(2^{\log^{\circledast}(\alpha)+1}) \leq \log^{\circledast}(\alpha) + \log^*(2^{\log^*(\alpha)+1}) = \log^{\circledast}(\alpha)+\log^*(\log^*(\alpha)+1)+1$, where the second inequality holds from the upper bound. Rearranging gives us our lower bound. ❑

Theorem's 4.15 upper bound leaves open the possibility that $\log^{\circledast}(\alpha)$ and $\log^*(\alpha)$ might be the same, or if not then at least that the former might be less than the latter by no more than some global constant. However, we now will prove that this is not the case. That is, we will show as Theorem 4.18 that there is an infinite collection $\mathcal{T}$ of natural numbers such that for no constant d' does it hold, on every element of the collection, that $\log^{\circledast}$ is at most d' less than $\log^*$. In fact, we will show a slightly stronger result than that.

First, we introduce some useful mathematical notions.

Definition 4.16 (see [28, 41, 45]). For each $n \in \mathbb{N}$, the nth tetration of 2 is defined inductively by

$$ {}^{n}2 = \begin{cases} 1 & n = 0 \\ 2^{({}^{(n-1)}2)} & n > 0. \end{cases} $$

Here we are using the so-called "Rudy Rucker notation" for tetration introduced by Goodstein [28] and popularized by Rucker [45].

It is easy to see that the nth tetration of 2, $n \in \mathbb{N}$, is exactly $2^{2^{\cdot^{\cdot^{\cdot^{2}}}}}$ where there are n 2s in the tower (and, as a convention, we view a height zero tower of 2s as evaluating to the value 1). Since tetration is injective, it has an inverse defined on towers of 2s.

Definition 4.17 (see [44]). Let $\mathcal{T}$ be the set $\{{}^{n}2 \mid n \in \mathbb{N}\}$. The (base 2) superlogarithm, slog : $\mathcal{T} \to \mathbb{N}$ is the inverse operation to tetration. That is, for any $N = {}^{n}2$, slog $N = n$.

It is easy to see that slog is increasing. While Definition 4.17 only defines slog for towers of 2s, we can extend it to a function from $\mathbb{R}^{\geq 1}$ to the nonnegative real numbers as follows. First, we extend tetration of 2 to a function ${}^{t}2$ from the nonnegative real numbers to $\mathbb{R}^{\geq 1}$ via linear interpolation.[9] Note that this extension is surjective and increasing, so it has an inverse $\widetilde{\text{slog}} : \mathbb{R}^{\geq 1} \to \mathbb{R}^{\geq 0}$. This inverse agrees with slog on towers of 2s, so we may safely write slog in place of $\widetilde{\text{slog}}$.

With these notions in hand, we prove the following "infinitely often" superconstant separation result between $\log^{\circledast}$ and $\log^*$.

Theorem 4.18. *For* $n \in \mathbb{N}^{\geq 2}$, $\log^*({}^{n}2) - \log^{\circledast}({}^{n}2) \geq \text{slog}(\frac{2}{3}n)$.

Proof. Notice that the function $t + \text{slog}\, t$ from $\mathbb{R}^{\geq 1}$ to $\mathbb{R}^{\geq 1}$ is increasing and surjective, and thus has an inverse.[10] Let $\mathfrak{s} : \mathbb{R}^{\geq 1} \to \mathbb{R}^{\geq 1}$ be this inverse. We will use the following lemma.

[9] For any $f : \mathbb{N} \to \mathbb{R}^{\geq 1}$, the linear interpolation of f is the function $\tilde{f} : \mathbb{R}^{\geq 0} \to \mathbb{R}^{\geq 1}$ given by $\tilde{f}(x) = (1-(x-\lfloor x \rfloor))f(\lfloor x \rfloor) + (x - \lfloor x \rfloor)f(\lfloor x \rfloor + 1)$.

[10] That $t + \text{slog}\, t$ from $\mathbb{R}^{\geq 1}$ to $\mathbb{R}^{\geq 1}$ is surjective follows from the basic facts from mathematical analysis that increasing, surjective (real) functions are continuous, and that the range of an increasing, continuous function is an interval. The first

Lemma 4.19. *For all* $n \in \mathbb{N}^+$, $\log^*({}^n2) - \log^{\circledast}({}^n2) = (\mathfrak{s}(n) - \lfloor \mathfrak{s}(n) \rfloor) + \operatorname{slog}(\mathfrak{s}(n))$.

Proof of Lemma 4.19. From the definition of $\log^{\circledast}$, we have $\log^{\circledast}({}^n2) = \max\{k \in \mathbb{N} \mid \log^{[k]}({}^n2) \geq k\}$. Since $n \geq 1$, ${}^n2 \geq 2$, which means $\log^{[1]}({}^n2) \geq 1$. This means that the max in the previous equation is at least 1, and so we can let the max run over $\mathbb{N}^+$ without changing the value. Additionally, notice that $\log^{[n]}({}^n2) = 1$, which, since $n \geq 1$, means that for all $\ell > n$, $\log^{[\ell]}({}^n2) < \ell$. So any k in the set we are maxing over must be at most n, and thus $\log^{[k]}({}^n2) = {}^{n-k}2$. Hence, $\log^{\circledast}({}^n2) = \max\{k \in \mathbb{N}^+ \mid {}^{n-k}2 \geq k\} = \max\{k \in \mathbb{N}^+ \mid n - k \geq \operatorname{slog} k\} = \max\{k \in \mathbb{N}^+ \mid k + \operatorname{slog} k \leq n\}$.

Since $\mathfrak{s}$ is increasing with inverse $k + \operatorname{slog} k$, we get $\{k \in \mathbb{N}^+ \mid k + \operatorname{slog} k \leq n\} = \{k \in \mathbb{N}^+ \mid k \leq \mathfrak{s}(n)\}$, and thus $\log^{\circledast}({}^n2) = \lfloor \mathfrak{s}(n) \rfloor$.

On the other hand, we have $\log^*({}^n2) = n = \mathfrak{s}(n) + \operatorname{slog}(\mathfrak{s}(n))$, and thus $\log^*({}^n2) - \log^{\circledast}({}^n2) = (\mathfrak{s}(n) - \lfloor \mathfrak{s}(n) \rfloor) + \operatorname{slog}(\mathfrak{s}(n))$. This concludes the proof of this lemma. ❑

Let us get a handle on the function $\mathfrak{s}$. Notice that for real numbers $t \geq 0$ we have ${}^t2 \geq 2t$, since the inequality holds when t is a natural number, and taking linear interpolations of both sides preserves the inequality. Changing variables, we get that for all $t \geq 0$, ${}^{t/2}2 \geq t$. Applying slog when defined, we get that for all $t \geq 1$, $t/2 \geq \operatorname{slog} t$.

From the definition of $\mathfrak{s}$ as the inverse of $t + \operatorname{slog} t$, for each $n \in \mathbb{N}^+$ we have $n = \mathfrak{s}(n) + \operatorname{slog}(\mathfrak{s}(n))$, which, by the inequality just mentioned is less than or equal to $\frac{3}{2}\mathfrak{s}(n)$, so $\mathfrak{s}(n) \geq \frac{2}{3}n$. Combining this with Lemma 4.19 and using the fact that slog is increasing on its (now extended) domain $\mathbb{R}^{\geq 1}$, we get that for all $n \in \mathbb{N}^{\geq 2}$ we have $\log^*({}^n2) - \log^{\circledast}({}^n2) = (\mathfrak{s}(n) - \lfloor \mathfrak{s}(n) \rfloor) + \operatorname{slog}(\mathfrak{s}(n)) \geq \operatorname{slog}(\mathfrak{s}(n)) \geq \operatorname{slog}(\frac{2}{3}n)$, thus establishing the theorem's claim. The only reason the previous sentence, and the theorem's statement, exclude $n = 1$ and start at $n = 2$ is that slog is defined only on reals greater than or equal to 1, and thus simply is not defined at $\frac{2}{3}n$ when $n = 1$. ❑

We now return to our study of nongappy sets, where the notion of $\log^{\circledast}$ will play an important role.

Definition 4.20. A nonempty set $S \subseteq \mathbb{N}^+$ is $O(n \log n)$-nongappy if $(\exists f \in O(n \log n))(\forall m \in S)(\exists m' \in S)[m' > m \wedge |m'| \leq f(|m|)]$.

Definitions of $n^{(\log n)^k}$-nongappy for any constant $k \in \mathbb{N}^+$ and 2^n-nongappy are provided via Definition 4.5, since $n^{(\log n)^k}$ and 2^n are each a single function, not a collection of functions.[11] Those two notions, along with the notion defined in Definition 4.20, will be the focus of Theorem 4.21. That theorem obtains the containments related to those three 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 4.21. *Let* T *be a subset of* $\mathbb{N}^+$.

(1) *If* T *has an* $O(n \log n)$*-nongappy, P-printable subset, then* $\mathrm{UP}_{\leq O(\sqrt{\log n})} \subseteq \mathrm{RC}_T$.

(2) *For all* $k \in \mathbb{N}^+$, *if* T *has an* $n^{(\log n)^k}$*-nongappy, P-printable subset, then* $\mathrm{UP}_{\leq O(1) + \frac{1}{\lceil \log(k+1) + 1 \rceil} \log\log\log n} \subseteq \mathrm{RC}_T$.[12]

fact implies that our extension of slog is continuous, and hence that $t + \operatorname{slog} t$ is increasing and continuous. Since $t + \operatorname{slog} t$ on our domain attains a minimum value of 1 and is unbounded, its range is $[1, \infty)$, which is exactly what it means for it to be surjective onto $\mathbb{R}^{\geq 1}$.

[11] Note that $n^{(\log n)^k}$-nongappiness does not involve evaluating 0^0 even though it might at first seem to because Definition 4.5, which is used to define the notion, restricts the domain of "F" to $\mathbb{R}^+$, and because k is a positive natural number.

[12] Some earlier versions of this work claimed that if T has an $n^{(\log n)^{O(1)}}$-nongappy (which is defined analogously to other notions of nongappiness involving big-Os, e.g., Definition 2.4), P-printable subset, then $\mathrm{UP}_{\leq O(1) + \frac{1}{3}\log^{[4]}(n)} \subseteq \mathrm{RC}_T$ [32,

(3) *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* $\lambda = 4 + \min_{s \in S, |s| \geq 2}(|s|)$.

Proof. We prove each of the three parts of the theorem separately.

(Part 1) Suppose $T \subseteq \mathbb{N}^+$ has an $O(n \log n)$-nongappy, P-printable subset. It follows from the definition of $O(n \log n)$-nongappy that there is some $k \in \mathbb{N}^+$ such that T has a $kn \log n$-nongappy, P-printable subset. Set $F : \mathbb{R}^+ \to \mathbb{R}^+$ to be $F(t) = kt \log t$. The conditions from Theorem 4.10 are satisfied by $F(t)$ as for all $t \geq 4$, $F(t) = kt \log t \geq t + 2$ and $(\forall c \in \mathbb{R}^{\geq 1})$ $[cF(t) = ckt \log t \leq ckt \log ct = F(ct)]$, and F is nondecreasing on $\{t \in \mathbb{R}^+ \mid t \geq 4\}$. Let $\lambda = 4 + |s|$, where s is the smallest element of the $kn \log n$-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 $kn \log n$-nongappy, P-printable subset of T such that $|s| \geq 4$. For every function $g : \mathbb{N} \to \mathbb{R}^{\geq 1}$ satisfying $g(n) = O(\sqrt{\log n})$, it is easy to see that there exists a number d such that $(\forall n \in \mathbb{N})[g(n) \leq d(\sqrt{\log n} + 1)]$. Thus, $\mathrm{UP}_{\leq g(n)} \subseteq \mathrm{UP}_{\leq d(\sqrt{\log n}+1)} = \mathrm{UP}_{\leq \lfloor d(\sqrt{\log n}+1) \rfloor}$. The function $j(n) = \lfloor d(\sqrt{\log n} + 1) \rfloor$ satisfies the conditions of Theorem 4.10 as $j(n)$ can be computed in time polynomial in the value n (since $\lfloor d(\sqrt{\log n} + 1) \rfloor$ can be computed by doing a linear search for the largest natural number i such that $2^{i^2} \leq n^{d^2}$), and $j(n)$ has value at most polynomial in the value n. Applying Theorem 4.10, to prove that $\mathrm{UP}_{\leq j(n)} \subseteq \mathrm{RC}_T$ it suffices to show that there is some β such that $F^{[j(n)]}(j(n)\lambda) = O(n^\beta)$.

To this end, we show, via induction on ℓ, that for all $\ell \in \mathbb{N}^+$ and real $t \geq 1$,

$$F^{[\ell]}(t) \leq \ell! k^\ell t [\log((\ell - 1)! k^{\ell-1} t)]^\ell. \tag{3}$$

The base case $\ell = 1$ is an equality since the right-hand side for $\ell = 1$ is exactly the definition of $F(t)$. Assume that Equation (3) holds for some $\ell \geq 1$. Then

$$\begin{aligned}
F^{[\ell+1]}(t) &= kF^{[\ell]}(t) \log(F^{[\ell]}(t)) \\
&\leq k(\ell! k^\ell t [\log((\ell - 1)! k^{\ell-1} t)]^\ell) \log(\ell! k^\ell t [\log((\ell - 1)! k^{\ell-1} t)]^\ell) \\
&= \ell! k^{\ell+1} t [\log((\ell - 1)! k^{\ell-1} t)]^\ell (\log(\ell! k^\ell t) + \ell \log \log((\ell - 1)! k^{\ell-1} t)) \\
&\leq \ell! k^{\ell+1} t [\log((\ell - 1)! k^{\ell-1} t)]^\ell \cdot \log(\ell! k^\ell t) \\
&\leq (\ell + 1)! k^{\ell+1} t \log(\ell! k^\ell t)^{\ell+1},
\end{aligned}$$

closing the induction.

Applying Equation (3) with $\ell = j(n)$ and $t = j(n)\lambda$ and using $j(n)! \leq j(n)^{j(n)}$, we get

$$F^{[j(n)]}(j(n)\lambda) \leq j(n)^{j(n)} k^{j(n)} j(n) \lambda [\log(j(n)^{j(n)} k^{j(n)} j(n) \lambda)]^{j(n)}. \tag{4}$$

Theorem 4.19, Part 3] [31, Theorem 4.23, Part 3], although those versions either pointed to or included a flawed proof. An anonymous ACM TOCT referee both spotted the flaw and generously suggested a tighter inequality that, when used in the proof, would improve the result. By further tightening that inequality into an identity, we were able to prove the stronger result that appears here, namely part 2 of Theorem 4.21. The current result implies the old statement because if a set T has an $n^{(\log n)^{O(1)}}$-nongappy, P-printable subset, then there exists $k \in \mathbb{N}^+$ such that T has an $n^{(\log n)^k}$-nongappy, P-printable subset, and because $\mathrm{UP}_{\leq O(1) + \frac{1}{3}\log^{[4]}(n)} \subseteq \mathrm{UP}_{\leq O(1) + C\log^{[3]}(n)}$ for any constant $C > 0$. The latter holds because for any C there exists N such that $C \log^{[3]}(n) \geq \frac{1}{3} \log^{[4]}(n)$ for all $n > N$, and so if a machine M witnesses $L \in \mathrm{UP}_{\leq O(1) + \frac{1}{3}\log^{[4]}(n)}$, then the machine M' that, on inputs of length at most N, memorizes whether to accept or reject, and, on inputs of length greater than N, simulates M, witnesses $L \in \mathrm{UP}_{\leq O(1) + C\log^{[3]}(n)}$.

For sufficiently large n, we have $j(n) \leq C\sqrt{\log n}$ for some constant $C \in \mathbb{N}^+$ that depends on d. So we have

$$\begin{aligned} j(n)^{j(n)} &\leq C^{C\sqrt{\log n}} \cdot (\log n)^{C\sqrt{\log n}} \\ &\leq 2^{C \log C \cdot \sqrt{\log n}} \cdot 2^{\log\log n \cdot C\sqrt{\log n}}. \end{aligned}$$

For sufficiently large n, $\log\log n \leq \sqrt{\log n}$, so for large n the second quantity in the multiplication is at most n^C.The first quantity is at most $n^{C \log C}$ since $\sqrt{\log n} \leq \log n$. Letting $C' = C \log C + C$ for convenience, for sufficiently large n, $j(n)^{j(n)} \leq n^{C'}$. Since k is a constant while j tends to infinity with n, for large n, $k^{j(n)} \leq j(n)^{j(n)} \leq n^{C'}$. Finally, since $C' \geq C \geq 1$, for all n, $\sqrt{\log n} \leq n^{C'}$. Plugging everything into Equation (4), we get that for all sufficiently large n,

$$\begin{aligned} F^{[j(n)]}(j(n)\lambda) &\leq n^{2C'} \cdot C\lambda\sqrt{\log n} \cdot [\log(n^{2C'} \cdot C\lambda\sqrt{\log n})]^{C\sqrt{\log n}} \\ &\leq C\lambda n^{3C'} \cdot [\log(C\lambda n^{3C'})]^{C\sqrt{\log n}} \\ &= C\lambda n^{3C'} \cdot 2^{\log\log(C\lambda n^{3C'}) \cdot C\sqrt{\log n}}. \end{aligned}$$

Notice that for large n, $\log\log(C\lambda n^{3C'}) = \log(\log(C\lambda) + 3C' \log n) \leq \log(4C' \log n) = \log(4C') + \log\log n \leq 2\log\log n \leq \sqrt{\log n}$. Thus, we have that for large n,

$$\begin{aligned} F^{[j(n)]}(j(n)\lambda) &\leq C\lambda n^{3C'} \cdot 2^{\sqrt{\log n} \cdot C\sqrt{\log n}} \\ &= C\lambda n^{3C'+C}. \end{aligned}$$

Hence, there exists a β (namely, this constant $3C' + C$) such that $F^{[j(n)]}(j(n)\lambda) = O(n^\beta)$.

Thus, for any function $g : \mathbb{N} \to \mathbb{R}^{\geq 1}$ satisfying $g(n) = O(\sqrt{\log n})$, there exists a function j such that $\mathrm{UP}_{\leq g(n)} \subseteq \mathrm{UP}_{\leq j(n)} \subseteq \mathrm{RC}_T$.

(Part 2) Fix $k \in \mathbb{N}^+$. Suppose $T \subseteq \mathbb{N}^+$ has an $n^{(\log n)^k}$-nongappy, P-printable subset. Set $F : \mathbb{R}^+ \to \mathbb{R}^+$ to be $F(t) = t^{(\log t)^k}$. The conditions from Theorem 4.10 are satisfied by F as for all $t \geq 4$, $F(t) \geq t + 2$ and $(\forall c \in \mathbb{R}^{\geq 1})[cF(t) = ct^{(\log t)^k} \leq (ct)^{(\log(ct))^k} = F(ct)]$, and F is nondecreasing on $\{t \in \mathbb{R}^+ \mid t \geq 4\}$. Let $\lambda = 4 + |s|$, where s is the smallest element of the $n^{(\log n)^k}$-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 $n^{(\log n)^k}$-nongappy, P-printable such that $|s| \geq 4$. For every function $g : \mathbb{N} \to \mathbb{R}^{\geq 1}$ satisfying $g(n) = O(1) + \frac{1}{\lceil \log(k+1)+1 \rceil} \log\log\log n$, there exists $d \in \mathbb{N}^+$ such that $g(n) \leq d + \frac{1}{\lceil \log(k+1)+1 \rceil} \log\log\log n$ and hence $\mathrm{UP}_{\leq g(n)} \subseteq \mathrm{UP}_{\leq d + \frac{1}{\lceil \log(k+1)+1 \rceil} \log\log\log n} = \mathrm{UP}_{\leq \lfloor d + \frac{1}{\lceil \log(k+1)+1 \rceil} \log\log\log n \rfloor}$. The function $j(n) = \lfloor d + \frac{1}{\lceil \log(k+1)+1 \rceil} \log\log\log n \rfloor$ can be computed in time polynomial in the value n since $\lfloor \frac{\log\log\log n}{\lceil \log(k+1)+1 \rceil} \rfloor$ can be computed by doing a linear search for the largest natural number i such that $2^{2^{2^{\lceil \log(k+1)+1 \rceil i}}} \leq n$ (the ceiling can be hardcoded since k is a constant). Additionally, $j(n)$ has value at most polynomial in the value n. So $j(n)$ satisfies the conditions of Theorem 4.10. Applying Theorem 4.10, to prove that $\mathrm{UP}_{\leq j(n)} \subseteq \mathrm{RC}_T$ it suffices to show that for some $\beta \in \mathbb{N}$, $F^{[j(n)]}(j(n)\lambda) = O(n^\beta)$.

We first show that for all $\ell \in \mathbb{N}^+$ and $t \in \mathbb{R}^+$, $F^{[\ell]}(t) = t^{(\log t)^{(k+1)^\ell - 1}}$. We do so by induction on ℓ. Notice that for all $t \in \mathbb{R}^+$, $F^{[1]}(t) = t^{(\log t)^k} = t^{(\log t)^{(k+1)^1 - 1}}$, so the claim holds for $\ell = 1$. Assume for induction that the identity holds for some $\ell \geq 1$. Fix some $t \in \mathbb{R}^+$, and let $t' = t^{(\log t)^{(k+1)^\ell - 1}}$. Using the inductive hypothesis, $F^{[\ell+1]}(t) = F(F^{[\ell]}(t)) = F(t') = t'^{(\log t')^k}$. We have

$(\log t')^k = ((\log t)^{(k+1)^\ell - 1} \log t)^k = (\log t)^{k(k+1)^\ell}$, and thus

$$F^{[\ell+1]}(t) = (t^{(\log t)^{(k+1)^\ell - 1}})^{(\log t)^{k(k+1)^\ell}} = t^{(\log t)^{k(k+1)^\ell + (k+1)^\ell - 1}}. \tag{5}$$

Using the binomial theorem,

$$\begin{aligned}
k(k+1)^\ell + (k+1)^\ell - 1 &= -1 + \sum_{0 \le i \le \ell} \binom{\ell}{i} k^{i+1} + \sum_{0 \le i \le \ell} \binom{\ell}{i} k^i \\
&= -1 + \sum_{1 \le i \le \ell+1} \binom{\ell}{i-1} k^i + \sum_{0 \le i \le \ell} \binom{\ell}{i} k^i && \text{(by reindexing)} \\
&= -1 + k^{\ell+1} + 1 + \sum_{1 \le i \le \ell} \left[\binom{\ell}{i-1} + \binom{\ell}{i} \right] k^i \\
&= k^{\ell+1} + \sum_{1 \le i \le \ell} \binom{\ell+1}{i} k^i \\
&= (k+1)^{\ell+1} - 1,
\end{aligned}$$

which, when substituted back into Equation (5), gives us $F^{[\ell+1]}(t) = t^{(\log t)^{(k+1)^{\ell+1} - 1}}$, completing the induction.

We now use this identity to prove that there exists β such that $F^{[j(n)]}(j(n)\lambda) = O(n^\beta)$. For convenience, let $t_n = j(n)\lambda$. Notice that since for all n, $j(n)\lambda > 0$ and $j(n) \in \mathbb{N}^+$, we can apply the identity we just proved to get $F^{[j(n)]}(t_n) = t_n^{(\log t_n)^{(k+1)^{j(n)} - 1}}$. To complete the proof, it suffices to show that there is a constant β such that for sufficiently large n, the expression on the right-hand side is at most n^β. Taking the log of both sides twice, it suffices to show that there exists a constant β such that for large enough n, $(k+1)^{j(n)} \log\log(t_n) \le \log\log n + \log\beta$. Plugging in the definitions of j and t_n,

$$\begin{aligned}
(k+1)^{j(n)} \log\log(t_n) &\le (k+1)^{d + \frac{1}{\lceil \log(k+1)+1 \rceil} \log^{[3]}(n)} \cdot \log\log\left(d\lambda + \frac{d}{\lceil \log(k+1)+1 \rceil} \log^{[3]}(n) \right) \\
&= (k+1)^d \cdot 2^{\frac{\log(k+1)}{\lceil \log(k+1)+1 \rceil} \log^{[3]}(n)} \cdot \log\log\left(d\lambda + \frac{d}{\lceil \log(k+1)+1 \rceil} \log^{[3]}(n) \right).
\end{aligned}$$

It is easy to see that for large enough n, $\log\log(d\lambda + \frac{d}{\lceil \log(k+2)+1 \rceil} \log^{[3]}(n)) \le 2\log^{[5]}(n)$ (asymptotically, the leading-order term is $\log^{[5]}(n)$ on the left and $2\log^{[5]}(n)$ on the right). For convenience, let $\epsilon = 1 - \frac{\log(k+1)}{\lceil \log(k+1)+1 \rceil}$. We have that for sufficiently large n,

$$\begin{aligned}
(k+1)^{j(n)} \log\log(t_n) &\le (k+1)^d \cdot (\log\log n)^{\frac{\log(k+1)}{\lceil \log(k+1)+1 \rceil}} \cdot 2\log^{[5]}(n), \\
&= 2(k+1)^d \cdot (\log\log n)^{1-\epsilon} \cdot \log^{[5]}(n).
\end{aligned}$$

For large n, $\log^{[5]}(n) \le (\log\log n)^{\epsilon/2}$, and so the preceding expression is bounded above by $C(\log\log n)^{1-\epsilon/2}$ where C is a constant that depends on k and d. For all $\beta \ge 1$ and for sufficiently large n, this quantity is at most $\log\log n + \log\beta$. Thus, there exists a β (namely, any $\beta \ge 1$) such that $F^{[j(n)]}(j(n)\lambda) = O(n^\beta)$.

Putting everything together, we have showed that for every $g : \mathbb{N} \to \mathbb{R}^{\ge 1}$ satisfying $g(n) = O(1) + \frac{1}{\lceil \log(k+1)+1 \rceil} \log\log\log n$, there exists a function j such that $\mathrm{UP}_{\le g(n)} \subseteq \mathrm{UP}_{\le j(n)} \subseteq \mathrm{RC}_T$.

(Part 3) Suppose $T \subseteq \mathbb{N}^+$ has a 2^n-nongappy, P-printable subset S. Set $F : \mathbb{R}^+ \to \mathbb{R}^+$ to be $F(t) = 2^t$. The conditions from Theorem 4.10 are satisfied by $F(t)$ as for all $t \ge 2$, $F(t) \ge t + 2$ and $(\forall c \in \mathbb{R}^{\ge 1})$ $[cF(t) = c \cdot 2^t \le 2^{ct} = F(ct)]$, and F is nondecreasing on $\{t \in \mathbb{R}^+ \mid t \ge 2\}$.

Let λ be as defined in the theorem statement—that is, $\lambda = 4 + \min_{s \in S, |s| \geq 2}(|s|)$. Notice that this is equal to $4 + |s|$, where s is the smallest element of S where the conditions on F hold, and so λ is as in Theorem 4.10. Let $j : \mathbb{N} \to \mathbb{N}^+$ be $j(n) = \max(1, \lfloor \lambda^{-1} \log^{\circledast}(n) \rfloor)$. Since $\log^{\circledast}$ can be computed in polynomial time, the function $j(n)$ can be computed in time at most polynomial in the value n and also will have value at most polynomial in the value n. Applying Theorem 4.10, to show that $\mathrm{UP}_{\leq \max(1, \lfloor \frac{\log^{\circledast} n}{\lambda} \rfloor)} \subseteq \mathrm{RC}_T$ it is enough to show that $F^{[j(n)]}(j(n)\lambda) = O(n)$. It suffices to show that for all sufficiently large n, $F^{[j(n)]}(j(n)\lambda) \leq n$. Since $\log^{\circledast}(n) \to \infty$ as $n \to \infty$, for large enough n we have $\lambda^{-1} \log^{\circledast}(n) \geq 1$ and hence $j(n) = \lfloor \lambda^{-1} \log^{\circledast}(n) \rfloor$. Thus, for sufficiently large n,

$$F^{[j(n)]}(j(n)\lambda) \leq \underbrace{2^{2^{\cdot^{\cdot^{\cdot^{2}}}}}}_{j(n)}{}^{\log^{\circledast}(n)} \leq \underbrace{2^{2^{\cdot^{\cdot^{\cdot^{2}}}}}}_{j(n)}{}^{\log[\log^{\circledast}(n)](n)} \leq \underbrace{2^{2^{\cdot^{\cdot^{\cdot^{2}}}}}}_{\log^{\circledast}(n)}{}^{\log[\log^{\circledast}(n)](n)} = n,$$

which finishes the proof. ❑

5 Conclusion and Open Problems

This work applied and adapted the iterative constant-setting technique used by Cai and Hemachandra [16] and Borchert et al. [9] to a more general setting. In particular, we generalized Borchert et al.'s notion of "nongappiness," 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. We also noted the apparent tradeoff between the nongappiness of the targets used in iterative constant-setting and the nondeterministic ambiguity of the classes one can capture using those targets. For example, beyond the containments we explicitly derived with Theorems 4.6 and 4.10, those two metatheorems themselves seem to reflect a tradeoff 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 tradeoff between gaps and ambiguity. Another open problem is to capture the relationship between $\log^{\circledast}$ and $\log^{*}$ more tightly than Theorems 4.15 and 4.18 do.

One last related open research direction is to further study nongappy, P-printable subsets of the primes. We noted two sufficient conditions for showing the existence of P-printable subsets of primes, namely the hypothesis about the probabilistic complexity class RP by Allender [2, Corollary 32 and the comment following it] and the Lenstra–Pomerance–Wagstaff Conjecture [43, 49]. Furthermore, we proved that the Lenstra–Pomerance–Wagstaff Conjecture in fact implies that for all $\epsilon > 0$, the primes have an $n^{1+\epsilon}$-nongappy, P-printable subset. While finding a P-printable subset of the primes would itself be interesting, we have shown how it would also be a useful step toward understanding the restricted counting class defined by the primes, namely if one could find a suitably nongappy such set.

Appendix

A Deferred Proof of Theorem 4.3

We now briefly give the simple proof of Theorem 4.3. We assume that the reader has already read the less simple proof of Theorem 4.6 and thus has seen that proof's use of iterative constant-setting.

Proof of Theorem 4.3. Let L be a language in $\mathrm{UP}_{\leq k}$, witnessed by a machine $\hat{N}$. To show $L \in \mathrm{RC}_T$, we give a description of a NPTM N that on every input x has $\#\mathrm{acc}_N(x) \in T$ if $x \in L$ and $\#\mathrm{acc}_N(x) = 0$ if $x \notin L$.

On input x, N nondeterministically guesses an integer $i \in \{1, 2, \ldots, k\}$, then 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, where the constants c_i are as defined in the following. Note that unlike the proof of Theorem 4.6, these constants $c_1, \ldots, c_k$ do not have to be computed on the fly by N but rather are hard-coded into N, so we do not need T to be P-printable.

Set c_1 to be the least element of T. Iteratively set, in this order, c_2, c_3, …, c_k, as follows. Given $c_1, \ldots, c_{i-1}$, set $b_i = \sum_{1 \le \ell \le i-1} c_\ell \binom{i}{\ell}$. Then let a_i be the least element of T such that $a_i \ge b_i$, and set $c_i = a_i - b_i$. Our description of machine N is complete.

Similarly to the proof of Theorem 4.6, we have set c_i to ensure that $\#\mathrm{acc}_N(x) \in T$ if $\hat{N}(x)$ accepts and $\#\mathrm{acc}_N(x) = 0$ if $\hat{N}(x)$ rejects. It is clear from the construction—keeping in mind that $\hat{N}$ runs in nondeterministic polynomial time and the c_i each will be fixed constants—that N is an NPTM. ❑

Acknowledgments

An anonymous ACM TOCT referee found, and in many cases suggested corrections for, flaws in a number of our proofs, and that referee also gave us proposed argument lines and suggested strengthenings that we have followed—for example, part 2 of Theorem 4.21 in its current form is stronger than in previous versions of the article. We are deeply grateful to the anonymous ACM TOCT and MFCS referees, and to Eric Allender, Benjamin Carleton, Kenneth Regan, and Henry Welles, for helpful comments, corrections, information, and improvements.

References

[1] Manindra Agrawal, Neeraj Kayal, and Nitin Saxena. 2004. PRIMES is in P. *Annals of Mathematics* 160, 2 (2004), 781–793. https://doi.org/10.4007/annals.2004.160.781

[2] Eric W. Allender. 1989. Some consequences of the existence of pseudorandom generators. *Journal of Computer and System Sciences* 39, 1 (1989), 101–124. https://doi.org/10.1016/0022-0000(89)90021-4

[3] Eric W. Allender and Roy S. Rubinstein. 1988. P-Printable sets. *SIAM Journal on Computing* 17, 6 (1988), 1193–1202. https://doi.org/10.1137/0217075

[4] Antonis Antonopoulos, Eleni Bakali, Aggeliki Chalki, Aris Pagourtzis, Petros Pantavos, and Stathis Zachos. 2022. Completeness, approximability, and exponential time results for counting problems with easy decision version. *Theoretical Computer Science* 915 (2022), 55–73. https://doi.org/10.1016/j.tcs.2022.02.030

[5] Richard Beigel. 1989. On the relativized power of additional accepting paths. In *Proceedings of the 4th Structure in Complexity Theory Conference*. IEEE, 216–224.

[6] Richard Beigel, John Gill, and Ulrich Hertrampf. 1990. Counting Classes: Thresholds, parity, mods, and fewness. In *Proceedings of the 7th Annual Symposium on Theoretical Aspects of Computer Science*. Lecture Notes in Computer Science, Vol. 415, Springer-Verlag, 49–57.

[7] Charles H. Bennett and John Gill. 1981. Relative to a random oracle A, $\mathrm{P}^A \neq \mathrm{NP}^A \neq \mathrm{coNP}^A$ with probability 1. *SIAM Journal on Computing* 10, 1 (1981), 96–113. https://doi.org/10.1137/0210008

[8] Leonard C. Berman. 1977. *Polynomial Reducibilities and Complete Sets*. Ph. D. Dissertation. Cornell University, Ithaca, NY.

[9] Bernd Borchert, Lane A. Hemaspaandra, and Jörg Rothe. 2000. Restrictive acceptance suffices for equivalence problems. *London Mathematical Society Journal of Computation and Mathematics* 3 (2000), 86–95. https://doi.org/10.1112/S146115700000022X

[10] Bernd Borchert and Frank Stephan. 2000. Looking for an analogue of Rice's theorem in circuit complexity theory. *Mathematical Logic Quarterly* 46, 4 (2000), 489–504. https://doi.org/10.1002/1521-3870(200010)46:4%3C489::AID-MALQ489%3E3.0.CO;2-F

[11] Daniel P. Bovet, Pierluigi Crescenzi, and Riccardo Silvestri. 1995. Complexity classes and sparse oracles. *Journal of Computer and System Sciences* 50, 3 (1995), 382–390. https://doi.org/10.1006/jcss.1995.1030

[12] Gilles Brassard. 1985. Crusade for a better notation. *ACM SIGACT News* 17, 1 (1985), 60–64. https://doi.org/10.1145/382250.382808

[13] Gilles Brassard and Paul Bratley. 1988. *Algorithmics: Theory & Practice*. Prentice Hall.

[14] Jin-Yi Cai and Xi Chen. 2017. *Complexity Dichotomies for Counting Problems: Volume 1, Boolean Domain*. Cambridge University Press.

[15] Jin-Yi Cai, Thomas Gundermann, Juris Hartmanis, Lane A. Hemachandra, Vivian Sewelson, Klaus Wagner, and Gerd Wechsung. 1989. The Boolean hierarchy II: Applications. *SIAM Journal on Computing* 18, 1 (1989), 95–111. https://doi.org/10.1137/0218007

[16] Jin-Yi Cai and Lane A. Hemachandra. 1990. On the power of parity polynomial time. *Mathematical Systems Theory* 23, 2 (1990), 95–106. https://doi.org/10.1007/BF02090768

[17] Chris Caldwell. 2021. Heuristics model for the distribution of Mersennes. *PrimePages*. Retrieved March 6, 2024 from https://t5k.org/mersenne/heuristic.html

[18] Aggeliki Chalki. 2022. *On Structural and Descriptive Complexity of Hard Counting Problems the Decision Version of Which Is Easy*. Ph. D. Dissertation. National Technical University of Athens.

[19] Pafnuty Chebyshev. 1852. Mémoire sur les nombres premiers. *Journal de Mathématiques Pures et Appliquées: Série 1* 17 (1852), 366–390.

[20] James L. Cox and Tayfun Pay. 2018. *An Overview of Some Semantic and Syntactic Complexity Classes*. Technical Report. Computing Research Repository. arXiv:1806.03501 [cs.CC]

[21] Stephen Fenner, Lance Fortnow, and Lide Li. 1996. Gap-definability as a closure property. *Information and Computation* 130, 1 (1996), 1–17. https://doi.org/10.1006/inco.1996.0080

[22] Stephen A. Fenner, Lance J. Fortnow, and Stuart A. Kurtz. 1994. Gap-definable counting classes. *Journal of Computer and System Sciences* 48, 1 (1994), 116–148. https://doi.org/10.1016/S0022-0000(05)80024-8

[23] Kevin Ford, Ben Green, Sergei Konyagin, James Maynard, and Terence Tao. 2018. Long gaps between primes. *Journal of the American Mathematical Society* 31, 1 (2018), 65–105. https://doi.org/10.1090/jams/876

[24] Kevin Ford, Ben Green, Sergei Konyagin, and Terence Tao. 2016. Large gaps between consecutive prime numbers. *Annals of Mathematics: Second Series* 183, 3 (2016), 935–974. https://doi.org/10.4007/annals.2016.183.3.4

[25] John Gill. 1977. Computational complexity of probabilistic turing machines. *SIAM Journal on Computing* 6, 4 (1977), 675–695. https://doi.org/10.1137/0206049

[26] Donald B. Gillies. 1964. Three new Mersenne primes and a statistical theory. *Mathematics of Computation* 18, 85 (1964), 93–97. Corrigendum 31, 140 (1977), 1051. https://doi.org/10.1090/S0025-5718-1964-0159774-6

[27] Leslie M. Goldschlager and Ian Parberry. 1986. On the construction of parallel computers from various bases of Boolean functions. *Theoretical Computer Science* 43, 1 (1986), 43–58. https://doi.org/10.1016/0304-3975(86)90165-9

[28] Reuben L. Goodstein. 1947. Transfinite ordinals in recursive number theory. *Journal of Symbolic Logic* 12, 4 (1947), 123–129. https://doi.org/10.2307/2266486

[29] Joachim Grollmann and Alan L. Selman. 1988. Complexity measures for public-key cryptosystems. *SIAM Journal on Computing* 17, 2 (1988), 309–335. https://doi.org/10.1137/0217018

[30] Juris Hartmanis and Yaacov Yesha. 1984. Computation times of NP sets of different densities. *Theoretical Computer Science* 34, 1–2 (1984), 17–32. https://doi.org/10.1016/0304-3975(84)90111-7

[31] Lane A. Hemaspaandra, Mandar Juvekar, Arian Nadjimzadah, and Patrick A. Phillips. 2021. *Gaps, Ambiguity, and Establishing Complexity-Class Containments via Iterative Constant-Setting*. Technical Report. Computing Research Repository. Revised, June 2022. arXiv:2109.147648 [cs.CC]

[32] Lane A. Hemaspaandra, Mandar Juvekar, Arian Nadjimzadah, and Patrick A. Phillips. 2022. Gaps, ambiguity, and establishing complexity-class containments via iterative constant-setting. In *47th International Symposium on Mathematical Foundations of Computer Science (MFCS 2022)*, Stefan Szeider, Robert Ganian, and Alexandra Silva (Eds.). Leibniz International Proceedings in Informatics, Vol. 241. Schloss Dagstuhl–Leibniz-Zentrum fur Informatik, Daghstuhl, Germany, Article 57, 15 pages.

[33] Lane A. Hemaspaandra and Mitsunori Ogihara. 2002. *The Complexity Theory Companion*. Springer-Verlag.

[34] Lane A. Hemaspaandra and Jörg Rothe. 2000. A second step towards complexity-theoretic analogs of Rice's theorem. *Theoretical Computer Science* 244, 1-2 (2000), 205–217. https://doi.org/10.1016/S0304-3975(98)00344-2

[35] Lane A. Hemaspaandra and Marius Zimand. 1993. *Strong Forms of Balanced Immunity*. Technical Report TR-480. Department of Computer Science, University of Rochester, Rochester, NY. Revised, May 1994.

[36] Lane A. Hemaspaandra and Marius Zimand. 1996. Strong self-reducibility precludes strong immunity. *Mathematical Systems Theory* 29, 5 (1996), 535–548. https://doi.org/10.1007/BF01184814

[37] Ker-I. Ko. 1985. On some natural complete operators. *Theoretical Computer Science* 37, 1 (1985), 1–30. https://doi.org/10.1016/0304-3975(85)90085-4

[38] Johannes Köbler, Uwe Schöning, Seinosuke Toda, and Jacobo Torán. 1992. Turing machines with few accepting computations and low sets for PP. *Journal of Computer and System Sciences* 44, 2 (1992), 272–286. https://doi.org/10.1016/0022-0000(92)90022-B

[39] Klaus-Jörn Lange and Peter Rossmanith. 1994. Unambiguous polynomial hierarchies and exponential size. In *Proceedings of the 9th Structure in Complexity Theory Conference*. IEEE, 106–115.

[40] James Maynard. 2016. Large gaps between primes. *Annals of Mathematics: Second Series* 183, 3 (2016), 915–933.

[41] Mark Neyrinck. 2012. An Investigation of Arithmetic Operations (Unpublished, Undated Manuscript). Retrieved March 6, 2024 from http://skysrv.pha.jhu.edu/~neyrinck/extessay.pdf

[42] Christos H. Papadimitriou and Stathis K. Zachos. 1983. Two remarks on the power of counting. In *Proceedings of the 6th GI Conference on Theoretical Computer Science*. Lecture Notes in Computer Science, Vol. 145, Springer-Verlag, 269–276.

[43] Carl Pomerance. 1981. Recent developments in primality testing. *Mathematical Intelligencer* 3, 3 (1981), 97–105. https://doi.org/10.1007/BF03022861

[44] Constantin A. Rubtsov and Giovanni F. Romerio. 2004. Ackermann's Function and New Arithmetical Operations (Unpublished Manuscript). Retrieved March 6, 2024 from https://www.rotarysaluzzo.it/Z_Vecchio_Sito/filePDF/Iperoperazioni%20(1).pdf

[45] Rudy Rucker. 1982. *Infinity and the Mind*. Birkhäuser.

[46] Nikolai Tchudakoff. 1936. On the difference between two neighbouring prime numbers. *Reccueil Mathematique Moscou: New Series* 1 (1936), 799–813.

[47] Leslie G. Valiant. 1976. The relative complexity of checking and evaluating. *Information Processing Letters* 5, 1 (1976), 20–23. https://doi.org/10.1016/0020-0190(76)90097-1

[48] Leslie G. Valiant. 1979. The complexity of computing the permanent. *Theoretical Computer Science* 8, 2 (1979), 189–201. https://doi.org/10.1016/0304-3975(79)90044-6

[49] Samuel S. Wagstaff, Jr. 1983. Divisors of Mersenne numbers. *Mathematics of Computation* 40, 161 (1983), 385–397. https://doi.org/10.1090/S0025-5718-1983-0679454-X

[50] Osamu Watanabe. 1988. On hardness of one-way functions. *Information Processing Letters* 27, 3 (1988), 151–157. https://doi.org/10.1016/0020-0190(88)90071-3

[51] Wikipedia. 2021. Gillies' Conjecture. Retrieved March 6, 2024 from https://en.wikipedia.org/wiki/Gillies%27_conjecture

Received 4 October 2022; revised 11 March 2024; accepted 12 March 2024