




Random Permutations in Computational Complexity

John M. Hitchcock   

Department of Electrical Engineering and Computer Science, University of Wyoming, Laramie, WY, USA

Adewale Sekoni   

Department of Mathematics, Computer Science & Physics, Roanoke College, Salem, VA, USA

Hadi Shafei   

Department of Computer Science, University of Huddersfield, UK

Abstract

Classical results of Bennett and Gill (1981) show that with probability 1, $P^A \neq NP^A$ relative to a random oracle A , and with probability 1, $P^\pi \neq NP^\pi \cap coNP^\pi$ relative to a random permutation π . Whether $P^A = NP^A \cap coNP^A$ holds relative to a random oracle A remains open. While the random oracle separation has been extended to specific individually random oracles—such as Martin-Löf random or resource-bounded random oracles—no analogous result is known for individually random permutations.

We introduce a new resource-bounded measure framework for analyzing individually random permutations. We define permutation martingales and permutation betting games that characterize measure-zero sets in the space of permutations, enabling formal definitions of polynomial-time random permutations, polynomial-time betting-game random permutations, and polynomial-space random permutations.

Our main result shows that $P^\pi \neq NP^\pi \cap coNP^\pi$ for every polynomial-time betting-game random permutation π . This is the first separation result relative to individually random permutations, rather than an almost-everywhere separation. We also strengthen a quantum separation of Bennett, Bernstein, Brassard, and Vazirani (1997) by showing that $NP^\pi \cap coNP^\pi \not\subseteq BQP^\pi$ for every polynomial-space random permutation π .

We investigate the relationship between random permutations and random oracles. We prove that random oracles are polynomial-time reducible from random permutations. The converse—whether every random permutation is reducible from a random oracle—remains open. We show that if $NP \cap coNP$ is not a measurable subset of EXP , then $P^A \neq NP^A \cap coNP^A$ holds with probability 1 relative to a random oracle A . Conversely, establishing this random oracle separation with time-bounded measure would imply BPP is a measure 0 subset of EXP .

Our framework builds a foundation for studying permutation-based complexity using resource-bounded measure, in direct analogy to classical work on random oracles. It raises natural questions about the power and limitations of random permutations, their relationship to random oracles, and whether individual randomness can yield new class separations.

2012 ACM Subject Classification Theory of computation \rightarrow Complexity classes; Theory of computation \rightarrow Computational complexity and cryptography; Theory of computation \rightarrow Quantum complexity theory

Keywords and phrases resource-bounded measure, martingales, betting games, random permutations, random oracles

Digital Object Identifier 10.4230/LIPIcs.MFCS.2025.58

Funding John M. Hitchcock: This research was supported in part by NSF grant 2431657.

Acknowledgements We thank Morgan Sinclair and Saint Wesonga for helpful discussions.



© John M. Hitchcock, Adewale Sekoni, and Hadi Shafei;
licensed under Creative Commons License CC-BY 4.0

50th International Symposium on Mathematical Foundations of Computer Science (MFCS 2025).

Editors: Paweł Gawrychowski, Filip Mazowiecki, and Michał Skrzypczak; Article No. 58; pp. 58:1–58:17



Leibniz International Proceedings in Informatics

LIPICs Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

1 Introduction

The seminal work of Bennett and Gill [4] established two foundational separations in computational complexity theory:

1. $P^A \neq NP^A$ relative to a random oracle A with probability 1.
2. $P^\pi \neq NP^\pi \cap \text{coNP}^\pi$ relative to a random permutation π with probability 1.

Subsequent research extended the first separation to hold for specific, individually random oracles, including algorithmically (Martin-Löf) random oracles [5], polynomial-space-bounded random oracles [16], and polynomial-time betting-game random oracles [12]. However, the second separation has not yet been strengthened in an analogous way. Whether $P^A \neq NP^A \cap \text{coNP}^A$ holds relative to a random oracle A remains an open question.

In this paper, we develop a novel framework for resource-bounded permutation measure and randomness, introducing *permutation martingales* and *permutation betting* games. These concepts generalize classical martingales and betting games to the space Π of all length-preserving permutations $\pi : \{0, 1\}^* \rightarrow \{0, 1\}^*$ where $|\pi(x)| = |x|$ for all $x \in \{0, 1\}^*$.

1.1 Background

Bennett and Gill [4] initiated the study of random oracles in computational complexity, proving that $P^A \neq NP^A$ for a random oracle A with probability 1. Subsequent work extended this to individual random oracles. Book, Lutz, and Wagner [5] showed that $P^A \neq NP^A$ for every oracle A that is algorithmically random in the sense of Martin-Löf [17]. Lutz and Schmidt [16] improved this further to show $P^A \neq NP^A$ for every oracle A that is pspace-random in the sense of resource-bounded measure [14]. Hitchcock, Sekoni, and Shafei [12] extended this result to polynomial-time betting-game random oracles [6].

The complexity class $NP \cap \text{coNP}$ is particularly significant because it comprises problems that have both efficiently verifiable proofs of membership and non-membership. This class includes important problems such as integer factorization and discrete logarithm, which are widely believed to be outside P but are not known to be NP -complete. These problems play a central role in cryptography, as the security of widely-used cryptosystems relies on their presumed intractability [22, 7]. Furthermore, under derandomization hypotheses, $NP \cap \text{coNP}$ has been shown to contain problems such as graph isomorphism [13], further underscoring its importance in complexity theory. Thus, understanding the relationship between P and $NP \cap \text{coNP}$ relative to different notions of randomness could shed light on the structure of these classes and the limits of efficient computation.

1.2 Our Approach: Permutation Martingales and Permutation Measure

In this work, we develop a novel framework for resource-bounded permutation measure and randomness. We introduce permutation martingales and permutation betting games, extending classical notions of random permutations. Our theory captures essential properties of random permutations while enabling complexity separations. We prove that random oracles can be computed in polynomial time from a random permutation; however, the converse remains unresolved.

First, we recall the basics of resource-bounded measure. A martingale in Cantor space may be viewed as betting on the membership of strings in a language. The standard enumeration of $\{0, 1\}^*$ is $s_0 = \lambda, s_1 = 0, s_2 = 1, s_3 = 00, s_4 = 01, \dots$. In the i^{th} stage of the game, the martingale has seen the membership of the first i strings and bets on the membership of s_i in the language. The martingale's value is updated based on the outcome of the bet. Formally,

a classical martingale is a function $d : \{0, 1\}^* \rightarrow [0, \infty)$ satisfying the fairness condition

$$d(w) = \frac{d(w0) + d(w1)}{2}$$

for all strings w . Intuitively, $d(w)$ represents the capital that a gambler has after betting on the sequence of bits in w according to a particular strategy. The fairness condition ensures that the expected capital after the next bit is equal to the current capital. A martingale succeeds on a language $A \subseteq \{0, 1\}^*$ if $\limsup_{n \rightarrow \infty} d(A \upharpoonright n) = \infty$, where $A \upharpoonright n$ is the length- n prefix of A 's characteristic sequence. The *success set* of d is $S^\infty[d]$, the set of all sequences that d succeeds on. Ville [25] proved that a set X has Lebesgue measure zero if and only if there is a martingale that succeeds on all elements of X . Lutz [14] defined resource-bounded measure by imposing computability and complexity constraints on the martingales in Ville's theorem.

We take a similar approach in developing resource-bounded permutation measure. Unlike a classical martingale betting on the bits of a language's characteristic sequence, a permutation martingale bets on the function values of a permutation π . Instead of seeing the characteristic string of a language, a permutation martingale sees a list of permutation function values. More precisely, after $i \geq 0$ rounds of betting, a permutation martingale has seen a *prefix partial permutation*

$$g = [g(s_0), \dots, g(s_{i-1})]$$

where $|g(s_i)| = |s_i|$ for all i . The permutation martingale will bet on the next function value $g(s_i)$. The current *betting length* is $l(g) = |s_i|$, the length of the next string s_i in the standard enumeration. The set of *free strings* available for the next function value is

$$\text{free}(g) = \{x \in \{0, 1\}^{l(g)} \mid x \text{ is not listed in } g\}.$$

For any prefix partial permutation g , a permutation martingale d outputs a value $d(g, x) \geq 0$ for each $x \in \text{free}(g)$. The values satisfy the averaging condition

$$d(g) = \frac{1}{|\text{free}(g)|} \sum_{x \in \text{free}(g)} d(g, x).$$

Here g, x denotes appending the string x as the next function value in prefix partial permutation g .

Prefix partial permutations may be used as cylinders to define a measure in Π that is equivalent to the natural product probability measure. We detail this in Section 3. Briefly, a class $X \subseteq \Pi$ has measure 0 if for every $\epsilon > 0$, there exists a sequence of cylinders $\{\llbracket g_i \rrbracket \mid i \in \mathbb{N}\}$ that has total measure at most ϵ and covers X . This is difficult to work with computationally as the covers may be large and require exponential time to enumerate.

We prove an analogue of Ville's theorem [25], showing that permutation martingales characterize measure 0 sets in the permutation space Π : a class $X \subseteq \Pi$ has measure 0 if and only if there a permutation martingale d with $X \subseteq S^\infty[d]$. This permutation martingale characterization allows us to impose computability and complexity constraints in the same way Lutz did for resource-bounded measure in Cantor space [14]. In the following, let Δ be a resource bound such as \mathbf{p} , \mathbf{p}_2 , \mathbf{pspace} , or $\mathbf{p}_2\mathbf{space}$ (see Section 3.5 for more details).

► **Definition 1.1.** *Let Δ be a resource bound. A class of permutations $X \subseteq \Pi$ has Δ -measure 0 if there is a Δ -computable permutation martingale that succeeds on X .*

Betting games [6, 18] are a generalization of martingales that are allowed to bet on strings in an adaptive order rather than the standard order. We analogously introduce permutation betting games as a generalization of both permutation martingales and classical betting games by allowing the betting strategy to adaptively choose the order in which it bets on the permutation's values. We use these betting games to define resource-bounded permutation betting-game measure.

► **Definition 1.2.** *Let Δ be a resource bound. A class of permutations $X \subseteq \Pi$ has Δ -betting game measure 0 if there is a Δ -computable permutation betting game that succeeds on X .*

We also define *individually* random permutations.

► **Definition 1.3.** *Let $\pi \in \Pi$ be a permutation and let Δ be a resource bound.*

1. π is Δ -random if no Δ -permutation martingale succeeds on π .
2. π is Δ -betting game random if no Δ -permutation betting game succeeds on π .

1.3 Our Results

Our main result strengthens the Bennett–Gill permutation separation by proving that $P \neq NP \cap \text{coNP}$ relative to every polynomial-time betting-game random permutation π . Formally, Theorem 5.1 establishes that

$$P^\pi \neq NP^\pi \cap \text{coNP}^\pi$$

for every p -betting-game random permutation π . In fact, we obtain even stronger separations in terms of bi-immunity [8, 2], a notion formalizing the absence of infinite, easily-decidable subsets (see Section 5 for more details). We show that for a p -betting-game random permutation π , the class $\text{NLIN}^\pi \cap \text{coNLIN}^\pi$ contains languages that are bi-immune to $\text{DTIME}^\pi(2^{kn})$ for all $k \geq 1$, where NLIN denotes nondeterministic linear time. Moreover, relative to a p_2 -betting-game random permutation, we derive that $NP^\pi \cap \text{coNP}^\pi$ contains languages that are bi-immune to $\text{DTIME}^\pi(2^{n^k})$ for every $k \geq 1$.

Bennett et al. [3] showed that $NP^\pi \cap \text{coNP}^\pi \not\subseteq \text{BQTIME}^\pi(o(2^{n/3}))$ relative to a random permutation π with probability 1. We apply our resource-bounded permutation measure framework to improve this to individual space-bounded random oracles. Specifically, we show that relative to a $p_2\text{space}$ -random permutation π ,

$$NP^\pi \cap \text{coNP}^\pi \not\subseteq \text{BQP}^\pi.$$

This illustrates the power of our framework for analyzing the interplay between randomness, classical complexity, and quantum complexity.

1.4 Random Oracles and Measure 0-1 Laws in EXP

Tardos [23] proved that if $\text{AM} \cap \text{coAM} \neq \text{BPP}$, then $P^A \neq NP^A \cap \text{coNP}^A$ with probability 1 for a random oracle A . This is proved using ALMOST complexity classes. For a relativizable complexity class \mathcal{C} , its ALMOST- \mathcal{C} class consists of all languages that are in the class with probability 1 relative to a random oracle: $\text{ALMOST-}\mathcal{C} = \{L \mid \Pr[L \in \mathcal{C}^A] = 1\}$. We have $\text{ALMOST-P} = \text{BPP}$ [4] and $\text{ALMOST-NP} = \text{AM}$ [20]. The condition $\text{AM} \cap \text{coAM} \neq \text{BPP}$ implies that there exist problems in $\text{ALMOST-NP} \cap \text{ALMOST-coNP}$ that are not in ALMOST-P . Since the intersection of measure 1 classes is measure 1, this implies $NP^A \cap \text{coNP}^A \neq P^A$ relative to a random oracle A with probability 1. Recent work of Ghosal et al. [9] shows that if $\text{UP} \not\subseteq \text{RP}$, then $P^A \neq NP^A \cap \text{coNP}^A$ with probability 1 for a random oracle A . In

Section 7 we pivot from permutation randomness to classical random oracles and show that resolving the long-standing question “does $P^R = NP^R \cap coNP^R$ with probability 1?” is tightly linked to quantitative structure inside EXP . Leveraging the conditional oracle separations of Tardos [23] and of Ghosal et al. [9], we prove that if $P^R = NP^R \cap coNP^R$ holds almost surely, then several familiar subclasses of EXP obey strong 0-1 laws: specifically, either $NP \cap coNP$, $UP \cap coUP$, (and, in a weaker form, UP vs. $FewP$) each has p -measure 0 or else fills all of EXP . Consequently, non-measurability of any one of these classes immediately forces $P^R \neq NP^R \cap coNP^R$ with probability 1. We further show that placing the same oracle separation in p_2 measure would collapse BPP below EXP , thereby framing the random-oracle problem in terms of concrete measure-theoretic thresholds inside exponential time.

1.5 Organization

This paper is organized as follows: Section 2 contains preliminaries. Section 3 develops permutation martingales, resource-bounded permutation measure, and random permutations. Elementary properties of p -random permutations are presented in Section 4. In Section 5, we prove our main results on random permutations for P vs. $NP \cap coNP$. Section 6 contains our results on $NP \cap coNP$ versus quantum computation relative to a random permutation. In Section 7 we present our results on random oracles and 0-1 laws. We conclude in Section 8 with some open questions.

2 Preliminaries

The binary alphabet is $\Sigma = \{0, 1\}$, the set of all binary strings is Σ^* , the set of all binary strings of length n is Σ^n , and the set of all infinite binary sequences is Σ^∞ . The empty string is denoted by λ . We use the standard enumeration of strings, $s_0 = \lambda, s_1 = 0, s_2 = 1, s_3 = 00, s_4 = 01, \dots$. The characteristic sequence of a language A is the sequence $\chi_A \in \Sigma^\infty$, where $\chi_A[n] = 1 \iff s_n \in A$. We refer to $\chi_A[s_n] = \chi_A[n]$ as the characteristic bit of s_n in A . A language A can alternatively be seen as a subset of Σ^* , or as an element of Σ^∞ via identification with its characteristic sequence χ_A . Given strings x, y we denote by $[x, y]$ the set of all strings z such that $x \leq z \leq y$. For any string s_n and natural number k , $s_n + k$ is the string s_{n+k} ; e.g. $\lambda + 4 = 01$. Similarly we denote by $A[x, y]$ the substring of the characteristic sequence χ_A that corresponds to the characteristic bits of the strings in $[x, y]$. We use parentheses for intervals that do not include the endpoints. We write $A \upharpoonright n$ for the length n prefix of A . A statement \mathcal{S}_n holds infinitely often (written i.o.) if it holds for infinitely many n , and it holds almost everywhere (written a.e.) if it holds for all but finitely many n .

3 Permutation Martingales and Permutation Measure

3.1 Permutation Measure Space

Resource-bounded measure is typically defined in the Cantor Space $C = \{0, 1\}^\infty = 2^\mathbb{N}$ of all infinite binary sequences. For measure in C , we use the open balls or cylinders $C_w = w \cdot C$ that have measure $\mu(C_w) = 2^{-|w|}$ for each $w \in \Sigma^*$. Let \mathcal{C} be the σ -algebra generated by $\{C_w \mid w \in \{0, 1\}^*\}$. Resource-bounded measure and algorithmic randomness typically work in the probability space (C, \mathcal{C}, μ) .

We only consider permutations in Π , the set of permutations on $\{0, 1\}^*$ that preserve string lengths. Given a permutation $\pi \in \Pi$, we denote by π_n the permutation π restricted to $\{0, 1\}^n$ i.e., π_n is a permutation on $\{0, 1\}^n$. Similarly, Π_n denotes the set of permutations in

Π restricted to $\{0,1\}^n$. Bennett and Gill [4] considered random permutations by placing the uniform measure on each Π_n and taking the product measure to get a measure on Π . We now define this measure space more formally so we may place martingales on it.

Standard resource-bounded measure identifies a language $A \subseteq \{0,1\}^*$ with its infinite binary characteristic sequence $\chi_A \in \mathbb{C}$. For permutations, we analogously use the value sequence consisting of all function values.

► **Definition 3.1.** *The value sequence of a permutation $f \in \Pi$ is the sequence*

$$\nu_f = [f(s_0), f(s_1), f(s_2), \dots]$$

of function values where s_0, s_1, s_2, \dots is the standard enumeration of $\{0,1\}^$.*

We identify a permutation $f \in \Pi$ with its value sequence ν_f . Initial segments of permutations are called prefix partial permutations.

► **Definition 3.2.** *A prefix partial permutation is a list $g = [g(s_0), \dots, g(s_{N-1})]$ of function values for some $N \geq 0$ where no value is repeated and $|g(s_i)| = |s_i|$ for all $0 \leq i < N$. We let $\text{PP}\Pi$ denote the class of all prefix partial permutations.*

We write each $g \in \text{PP}\Pi$ as a list $g = [g(s_0), \dots, g(s_{N-1})]$. The *length* of g is N , the number of function values assigned, and is denoted $|g|$. We use $[]$ to denote the *empty list*, the list of length 0. We write $f \upharpoonright N$ for the length N prefix partial permutation of $f \in \Pi$.

► **Definition 3.3.** *For each $g = [g(s_0), \dots, g(s_{N-1})] \in \text{PP}\Pi$, the cylinder of all permutations in Π that extend g is*

$$[g] = \{h \in \Pi \mid h(s_0) = g(s_0), \dots, h(s_{N-1}) = g(s_{N-1})\}.$$

For measure in Π , we are taking the uniform distribution on the set of all Π_n of length-preserving permutations for all n . Our basic open sets are $\{[g] \mid g \in \text{PP}\Pi\}$. Suppose $g \in \text{PP}\Pi$ has $|g| = 2^n - 1$ for some $n \geq 0$. Then, following Bennett and Gill [4], the measure

$$\mu([g]) = \prod_{k=0}^{n-1} \frac{1}{(2^k)!}$$

is easy to define because the distribution is uniform over the $(2^k)!$ permutations at each length. If $2^n - 1 \leq |g| < 2^{n+1} - 1$, let $m = |g| - 2^n + 1$ and then

$$\mu([g]) = \left(\prod_{k=0}^{n-1} \frac{1}{(2^k)!} \right) \frac{(2^n - m)!}{(2^n)!} = \left(\prod_{k=0}^{n-1} \frac{1}{(2^k)!} \right) \frac{1}{P(2^n, m)},$$

where $P(n, k) = \frac{n!}{(n-k)!}$ denotes the number of k -permutations on n elements. For convenience, we commonly write $\mu(g) = \mu([g])$.

Let $\mathcal{F}_\Pi = \sigma(\text{PP}\Pi)$ be the σ -algebra generated by the collection of all $[g]$ where $g \in \text{PP}\Pi$. By Carathéodory's extension theorem, μ extends uniquely to \mathcal{F}_Π , yielding the probability space $(\Pi, \mathcal{F}_\Pi, \mu)$. We will work in this probability space. Because μ is outer regular, we have the typical open cover characterization of measure zero:

► **Theorem 3.4.** *A class $X \subseteq \Pi$ has measure 0 if and only if for every $\epsilon > 0$, there is an open covering $G = \{g_0, g_1, \dots\} \subseteq \text{PP}\Pi$ such that*

$$\sum_{i=0}^{\infty} \mu(g_i) < \epsilon \quad \text{and} \quad X \subseteq \bigcup_{i=0}^{\infty} [g_i].$$

3.2 Permutation Martingales

In resource-bounded measure in Cantor Space, a *martingale* is a function $d : \Sigma^* \rightarrow [0, \infty)$ such that for all $w \in \Sigma^*$, we have the following averaging condition:

$$d(w) = \frac{d(w0) + d(w1)}{2}.$$

A martingale in Cantor space may be viewed as betting on the membership of strings in a language. The standard enumeration of $\{0, 1\}^*$ is $s_0 = \lambda, s_1 = 0, s_2 = 1, s_3 = 00, s_4 = 01, \dots$. In the i^{th} stage of the game, the martingale has seen the membership of the first i strings and bets on the membership of s_i in the language. The martingale's value is updated based on the outcome of the bet. For further background on resource-bounded measure, we refer to [14, 15, 1, 6, 10].

A permutation martingale operates similarly, but instead of betting on the membership of a string in a language it bets on the next function value of the permutation. Instead of seeing the characteristic string of a language, a permutation martingale sees a *prefix partial permutation*, which is a list of permutation function values $g = [g(s_0), \dots, g(s_{i-1})]$ satisfying $|g(s_i)| = |s_i|$ for all i . The permutation martingale will bet on the next function value $g(s_i)$. The current *betting length* is the length of the next string $s_{|g|}$ in the standard enumeration: $l(g) = |s_{|g|}|$. The set of *free strings* available for the next function value is

$$\text{free}(g) = \{x \in \{0, 1\}^{l(g)} \mid x \text{ is not in } g\}.$$

For example, $\text{free}([\lambda]) = \{0, 1\}$, $\text{free}([\lambda, 1, 0, 11]) = \{00, 01, 10\}$, and $\text{free}([\lambda, 1, 0, 11, 00, 01]) = \{10\}$.

We now introduce our main conceptual contribution, permutation martingales.

► **Definition 3.5.** A *permutation martingale* is a function $d : \text{PP}\Pi \rightarrow [0, \infty)$ such that for every prefix partial permutation $g \in \text{PP}\Pi$,

$$d(g) = \frac{1}{|\text{free}(g)|} \sum_{x \in \text{free}(g)} d(g, x),$$

where (g, x) is the result of appending x to g .

Success is defined for permutation martingales analogously to success for classical martingales.

► **Definition 3.6.** Let d be a permutation martingale. We say d *succeeds on* $f \in \Pi$ if

$$\limsup_{N \rightarrow \infty} d(f \upharpoonright N) = \infty.$$

The *success set* of d is

$$S^\infty[d] = \{f \in \Pi \mid d \text{ succeeds on } f\}$$

and the *unitary success set* of d is the set

$$S^1[d] = \{f \in \Pi \mid (\exists n) d(f \upharpoonright n) \geq 1\}.$$

We establish the analogue of Ville's theorem [25] for measure in Π and permutation martingales:

► **Theorem 3.7.** The following statements are equivalent for every $X \subseteq \Pi$:

1. X has measure 0.
2. For every $\epsilon > 0$, there is a permutation martingale d with $d(\lambda) < \epsilon$ and $X \subseteq S^1[d]$.
3. There is a permutation martingale d with $X \subseteq S^\infty[d]$.

3.3 A Permutation Martingale Example

We construct a permutation martingale d that succeeds on any length-preserving permutation whose restriction to length n is a cycle permutation for all but finitely many n . We partition the initial capital into infinitely many shares $a_i = 1/i^2$. For each i , the share a_i is used to bet on the event that, for all $n \geq i$, the length- n restriction of the permutation is a cycle permutation.

The betting strategy is simple: when moving from length $n - 1$ to n , the martingale wagers all relevant capital on the image of the n -bit string $1^{n-1}0$. In the final step of forming a cycle of length 2^n , there are exactly two choices for the image of $1^{n-1}0$. One choice yields a cycle of length 2^n ; the other does not. Since it is a binary choice, the martingale places its entire stake a_i (for all $i \leq n$) on the cycle outcome, thereby doubling its capital whenever the cycle is formed.

Hence, on any permutation whose restriction to length n is a cycle permutation for all but finitely many n , infinitely many of these bets succeed. Consequently, each of those corresponding shares a_i grows without bound, and so the overall martingale d succeeds on all such permutations.

3.4 Permutation Martingales as Random Variables

Hitchcock and Lutz [11] showed how the martingales used in computational complexity are a special case of martingales used in probability theory. We explain how this extends to permutation martingales. Given a martingale $d : \{0,1\}^* \rightarrow [0, \infty)$, Hitchcock and Lutz define the random variable $\xi_{d,n} : \mathbb{C} \rightarrow [0, \infty)$ by $\xi_{d,n}(S) = d(S \upharpoonright n)$ for each $n \geq 0$. Let $\mathcal{M}_n = \sigma(\{C_w \mid w \in \{0,1\}^n\})$ be the σ -algebra generated by the cylinders of length n . Then the sequence $(\xi_{d,n} \mid n \geq 0)$ is a martingale in the probability theory sense with respect to the filtration $(\mathcal{M}_n \mid n \geq 0)$: for all $n \geq 0$, $E[\xi_{d,n+1} \mid \mathcal{M}_n] = \xi_{d,n}$.

Similarly, given a permutation martingale $d : \text{PP}\Pi \rightarrow [0, \infty)$, for each N we can define the random variable $X_{d,N} : \Pi \rightarrow [0, \infty)$ by $X_{d,N}(f) = d(f \upharpoonright N)$ for each $N \geq 0$. Let

$$\mathcal{G}_N = \sigma(\{[g] \mid g \in \text{PP}\Pi \text{ and } |g| = N\})$$

be the σ -algebra generated by the cylinders in $\text{PP}\Pi$ of length N . Then $(X_{d,N} \mid N \geq 0)$ is a martingale in the probability theory sense with respect to the filtration $(\mathcal{G}_N \mid N \geq 0)$: for all $N \geq 0$, $E[X_{d,N+1} \mid \mathcal{G}_N] = X_{d,N}$.

3.5 Resource-Bounded Permutation Measure

We follow the standard notion of computability for real-valued functions [14] to define resource-bounded permutation martingales.

► **Definition 3.8.** Let $d : \text{PP}\Pi \rightarrow [0, \infty)$ be a permutation martingale.

1. d is computable in time $t(n)$ if there is an exactly computable $\hat{d} : \text{PP}\Pi \times \mathbb{N} \rightarrow \mathbb{Q}$ such that for all $f \in \text{PP}\Pi$ and $r \in \mathbb{N}$, $|d(f) - \hat{d}(f, r)| \leq 2^{-r}$ and $\hat{d}(f, r)$ is computable in time $t(|f| + r)$.
2. d is computable in space $s(n)$ if there is an exactly computable $\hat{d} : \text{PP}\Pi \times \mathbb{N} \rightarrow \mathbb{Q}$ such that for all $f \in \text{PP}\Pi$ and $r \in \mathbb{N}$, $|d(f) - \hat{d}(f, r)| \leq 2^{-r}$ and $\hat{d}(f, r)$ is computable in space $s(|f| + r)$.
3. If d is computable in polynomial time, then d is a **p**-permutation martingale.
4. If d is computable in quasipolynomial time, then d is a **p₂**-permutation martingale.
5. If d is computable in polynomial space, then d is a **pspace**-permutation martingale.
6. If d is computable in quasipolynomial space, then d is a **p₂space**-permutation martingale.

We are now ready to define resource-bounded permutation measure.

► **Definition 3.9.** Let $\Delta \in \{p, p_2, \text{pspace}, p_2\text{space}\}$. Let $X \subseteq \Pi$ and $X^c = \Pi - X$ be the complement of X within Π .

1. X has Δ -measure 0, written $\mu_\Delta(X) = 0$, if there is a Δ -computable permutation martingale d with $X \subseteq S^\infty[d]$.
2. X has Δ -measure 1, written $\mu_\Delta(X) = 1$, if $\mu_\Delta(X^c) = 0$

► **Definition 3.10.** Let $\Delta \in \{p, p_2, \text{pspace}, p_2\text{space}\}$. A permutation $\pi \in \Pi$ is Δ -random if π is not contained in any Δ -measure 0 set.

Equivalently, π is Δ -random if no Δ -martingale succeeds on π .

3.6 Permutation Betting Games

Originated in the field of algorithmic information theory, betting games are a generalization of martingales [19, 18], which were introduced to computational complexity by Buhrman et al. [6]. Similar to martingales, betting games can be thought of as strategies for betting on a binary sequence, except that with betting games we have the additional capability of selecting which position in a sequence to bet on next. In other words, a betting game is permitted to select strings in a nonmonotone order, with the important restriction that it may not bet on the same string more than once (see Buhrman et al. [6] for more details).

A permutation betting game is a generalization of a permutation martingale, implemented by an oracle Turing machine, where it is allowed to select strings in nonmonotone order. Prefixes of permutation betting games can be represented as *ordered partial permutations* defined below.

► **Definition 3.11.** An ordered partial permutation is a list $g = [(x_1, y_1), \dots, (x_n, y_n)]$ of pairs of strings for some $n \geq 0$ where for all $1 \leq i < j \leq n$, $x_i \neq x_j$ and $y_i \neq y_j$, and $|x_i| = |y_i|$ for all $1 \leq i \leq n$. We let $\text{OP}\Pi$ denote the class of all ordered partial permutations.

For a permutation betting game, the averaging condition takes into consideration the length of the next string to be queried as follows. Let $w \in \text{OP}\Pi$ be the list of queried strings paired with their images, and $a \in \{0, 1\}^n$ be the next string the betting game will query. Define $\text{free}(w, n)$ to be the set of length- n strings that are available for the next function value, i.e., length- n strings that are not the function value of any of the queried strings. Then the following averaging condition over free strings of length n must hold for the permutation betting game $d : \text{OP}\Pi \rightarrow [0, \infty)$

$$d(w) = \sum_{b \in \text{free}(w, n)} \frac{d(w[a, b])}{|\text{free}(w, n)|}$$

where $w[a, b]$ is the list w appended with the pair (a, b) .

► **Definition 3.12.** A betting game is a $t(n)$ -time betting game if for all n , all strings of length n have been queried by time $t(2^n)$.

We define betting game measure 0 and betting game randomness analogously.

► **Definition 3.13.** Let $\Delta \in \{p, p_2, \text{pspace}, p_2\text{space}\}$.

1. A class $X \subseteq \Pi$ has Δ -betting-game measure 0 if there is a Δ -computable permutation betting game d with $X \subseteq S^\infty[d]$.
2. A permutation $\pi \in \Pi$ is Δ -betting game random if no Δ -betting game succeeds on π .

3.7 Measure Conservation

Lutz's Measure Conservation Theorem implies that resource-bounded measure gives nontrivial notions of measure within exponential-time complexity classes: $\mu_p(E) \neq 0$ and $\mu_{p_2}(\text{EXP}) \neq 0$. Let PermE be the class of length-preserving permutations that can be computed in $2^{O(n)}$ time and PermEXP be the class of length-preserving permutations that can be computed in $2^{n^{O(1)}}$ time. We show that our notions of permutation measure have conservation theorems within these classes of exponential-time computable permutations.

► **Lemma 3.14.** *For any $t(2^n)$ -time permutation martingale D , we can construct a permutation in time $O(2^{2n}t(2^n))$ that is not covered by D .*

The following theorem follows from Lemma 3.14.

► **Theorem 3.15.**

1. PermE does not have p -permutation measure 0.
2. PermEXP does not have p_2 -permutation measure 0.

Proving similar results for betting games turns out to be more challenging, given that they are allowed to bet on strings in an adaptive order. To address this, we define the following class of *honest* betting games.

► **Definition 3.16.** *A $\log(t(2^n))$ -honest $t(n)$ -permutation betting game is a $t(n)$ -time permutation betting game such that for all languages A , for all n , all non-zero bets by time $t(2^n)$ are for strings of length at most $\log(t(2^n))$.*

We use this definition in the following Lemma:

► **Lemma 3.17.** *For any $\log(t(2^n))$ -honest $t(2^n)$ -permutation betting game G , we can construct a permutation in $O(2^{2n}t(2^n)^2)$ time that is not covered by G .*

► **Theorem 3.18.**

1. PermE does not have $O(n)$ -honest p -permutation betting game measure 0.
2. PermEXP does not have $O(n^k)$ -honest p_2 -permutation betting game measure 0.

Since pspace -permutation martingales can simulate $O(n)$ -honest p -betting-games, and $p_2\text{space}$ -permutation martingales can simulate $O(n^k)$ -honest p_2 -betting-games, we have the following:

► **Proposition 3.19.** *Let π be a permutation.*

1. *If π is a pspace -random permutation, then π is $O(n)$ -honest p -betting game random.*
2. *If π is a $p_2\text{space}$ -random permutation, then π is $O(n^k)$ -honest p_2 -betting game random.*

4 Elementary Properties of Random Permutations

In this section, we explore fundamental properties of random permutations that provide insights into how permutation martingales and betting games operate. Understanding these properties is crucial for applying permutation randomness in computational complexity. We show that random permutations are computationally difficult to compute and to invert. We then investigate the relationship between random permutations and random oracles, showing how random permutations can generate random oracles.

4.1 Intractability of Random Permutations

► **Definition 4.1.** A permutation $\pi \in \Pi$ is noticeably polynomial time if there are polynomials p, q and TM M such that for infinitely many n , M computes π on at least $2^n/p(n)$ strings of length n in $q(n)$ time for each string.

► **Theorem 4.2.** The set $X = \{\pi \in \Pi \mid \pi_n \text{ is noticeably polynomial time}\}$ has \mathbf{p} -permutation measure 0.

The proof uses a simple averaging argument: we partition the set of length- n strings into $2^n/n^{\lg n}$ subintervals, each of size $n^{\lg n}$. By the noticeably-polynomial-time property of the permutations in X , at least one subinterval contains superpolynomially many strings whose images are computable. The martingale then identifies a sufficiently small subset of these strings and makes correct predictions often enough to succeed.

► **Corollary 4.3.** If $\pi \in \Pi$ is \mathbf{p} -random, then any polynomial-time TM will be able to compute π on at most a $1/\text{poly}$ fraction for all sufficiently large n .

Similarly, we can show that random permutations are hard to invert on a noticeable subset infinitely often. The main difference is that we search for TMs inverting the permutation rather than TMs that compute the permutation.

► **Definition 4.4.** A permutation $\pi \in \Pi$ is noticeably invertible if there is a polynomial-time TM M and a polynomial p such that for infinitely many n , $|\{x \in \{0, 1\}^n \mid M(\pi(x)) = x\}| \geq 2^n/p(n)$.

► **Theorem 4.5.** The set $X = \{\pi \in \Pi \mid \pi_n \text{ is noticeably invertible}\}$ has \mathbf{p} -permutation measure 0.

4.2 Random Permutations versus Random Oracles

Bennett and Gill used random permutations, rather than random languages, to separate \mathbf{P} from $\mathbf{NP} \cap \mathbf{coNP}$. It is still unknown whether random oracles separate \mathbf{P} from $\mathbf{NP} \cap \mathbf{coNP}$. In this section, we examine how random permutations yield random languages. We show that a \mathbf{p} -random permutation can be used to generate a \mathbf{p} -random language. All of the results in this section are stated for \mathbf{p} -randomness. They also hold for \mathbf{p}_2 -randomness.

Given a permutation $\pi \in \Pi$, we define the language

$$L_\pi = \{x \mid \text{the first bit of } \pi(0^{2|x}|x) \text{ is } 1\}.$$

For a set of permutations $X \subseteq \Pi$, we define the set of languages

$$L_X = \{L_\pi \mid \pi \in X\}.$$

► **Lemma 4.6.** For any set of permutations $X \subseteq \Pi$, if a \mathbf{p} -computable martingale d succeeds on the set of languages $L_X = \{L_\pi \mid \pi \in X\}$, then there is a \mathbf{p} -computable permutation martingale that succeeds on X .

► **Corollary 4.7.** If π is a \mathbf{p} -random permutation, then L_π is a \mathbf{p} -random language.

We now extend the previous lemma to honest \mathbf{p} -permutation betting games. By Lemma 3.17, honest \mathbf{p} -permutation betting games do not cover \mathbf{PermE} and honest \mathbf{p}_2 -permutation betting games do not cover $\mathbf{PermEXP}$.

► **Lemma 4.8.** *For any set of permutations $X \subseteq \Pi$, if an honest \mathbf{p} -betting game g succeeds on the set of languages $L_X = \{L_\pi \mid \pi \in X\}$, then there is an honest \mathbf{p} -permutation betting game that succeeds on X .*

► **Definition 4.9.** *Give a language L , we define Π_L to be set of permutations*

$$\Pi_L = \left\{ \pi \in \Pi \mid \begin{array}{l} \text{for all } n > 0 \text{ and } x \in \{0, 1\}^n, \\ \pi(0^{2n}x) = by \text{ for some } y \in \{0, 1\}^{3n-1} \\ \text{if and only if } L[x] = b \end{array} \right\}.$$

Given a set of languages X , we define Π_X as the set of permutations $\Pi_X = \bigcup_{L \in X} \Pi_L$.

► **Lemma 4.10.** *For any set of languages $X \subseteq \{0, 1\}^\infty$, if a \mathbf{p} -computable permutation martingale d succeeds on the set of permutations Π_X , then there is a \mathbf{p} -computable martingale that succeeds on X .*

► **Corollary 4.11.** *If π is a \mathbf{p} -betting game random permutation, then L_π is a \mathbf{p} -betting game random language.*

5 Random Permutations for $\mathbf{NP} \cap \mathbf{coNP}$

Bennett and Gill [4] studied the power of random oracles in separating complexity classes. In particular, they showed that $\mathbf{P}^A \neq \mathbf{NP}^A$ relative to a random oracle with probability 1. However, they were not able to separate \mathbf{P} from $\mathbf{NP} \cap \mathbf{coNP}$ relative to a random oracle. They also made the observation that if $\mathbf{P}^A = \mathbf{NP}^A \cap \mathbf{coNP}^A$ for a random oracle A , then \mathbf{P}^A must include seemingly computationally hard problems such as factorization. They also proved that any non-oracle-dependent language that belongs to \mathbf{P}^A with probability 1, also belongs to \mathbf{BPP} . As a result, if $\mathbf{P}^A = \mathbf{NP}^A \cap \mathbf{coNP}^A$ for a random oracle A with probability 1, then these difficult problems in $\mathbf{NP} \cap \mathbf{coNP}$ would be solvable in probabilistic polynomial time (\mathbf{BPP}). To achieve a separation between \mathbf{P}^A and $\mathbf{NP}^A \cap \mathbf{coNP}^A$, they considered length-preserving permutations on $\{0, 1\}^*$ and showed that $\mathbf{P}^\pi \neq \mathbf{NP}^\pi \cap \mathbf{coNP}^\pi$ for every random permutation π .

Using resource-bounded permutation betting games on the set of all length preserving permutations of $\{0, 1\}^*$, we strengthen the Bennett-Gill permutation separation, proving that $\mathbf{P}^\pi \neq \mathbf{NP}^\pi \cap \mathbf{coNP}^\pi$ for any \mathbf{p} -betting-game random permutations π . More generally, we show that the set of permutations π such that, \mathbf{NP}^π is not $\mathbf{DTIME}^\pi(2^{kn})$ -bi-immune has \mathbf{p} -permutation-betting-game measure 0. Recall that a language L is bi-immune to a complexity class C if no infinite subset of L or its complement is decidable in C [8, 2].

The following is our main theorem where its first part states that relative to a \mathbf{p} -betting-game random permutation π , there is a language L in $\mathbf{NLIN}^\pi \cap \mathbf{coNLIN}^\pi$ such that no infinite subset of L or its complement is $\mathbf{DTIME}^\pi(2^{kn})$ -decidable.

► **Theorem 5.1.**

1. *If π is a \mathbf{p} -betting-game random permutation, then $\mathbf{NLIN}^\pi \cap \mathbf{coNLIN}^\pi$ contains a $\mathbf{DTIME}^\pi(2^{kn})$ -bi-immune language for all $k \geq 1$.*
2. *If π is a \mathbf{p}_2 -betting-game random permutation, then $\mathbf{NP}^\pi \cap \mathbf{coNP}^\pi$ contains a $\mathbf{DTIME}^\pi(2^{n^k})$ -bi-immune language for all $k \geq 1$.*

Our headline result is a corollary of Theorem 5.1.

► **Corollary 5.2.** *If π is a \mathbf{p} -betting-game random permutation, then $\mathbf{P}^\pi \neq \mathbf{NP}^\pi \cap \mathbf{coNP}^\pi$.*

To prove Theorem 5.1, we first define the following test languages. For each $k \geq 1$, define the “half range” test languages

$$\begin{aligned} \text{HRNG}_k^\pi &= \{x \mid \exists y \in \{0,1\}^{k|x|-1}, \pi(0y) = x^k\} \\ &= \{x \mid \forall y \in \{0,1\}^{k|x|-1}, \pi(1y) \neq x^k\}, \end{aligned}$$

and

$$\begin{aligned} \text{POLYHRNG}_k^\pi &= \{x \mid \exists y \in \{0,1\}^{|x|^{k-1}-1}, \pi(0y) = x^{|x|^{k-1}}\} \\ &= \{x \mid \forall y \in \{0,1\}^{|x|^{k-1}-1}, \pi(1y) \neq x^{|x|^{k-1}}\}. \end{aligned}$$

A string $x \in \{0,1\}^n$ belongs to HRNG_k^π if the preimage of x^k (k copies of x) in $\{0,1\}^{kn}$ begins with 0. If x does not belong to HRNG_k^π , then the preimage of x^k begins with 1. In either case, the preimage serves as a witness for x . The language POLYHRNG_k^π is similar, but we are looking for a preimage in $\{0,1\}^{n^k}$ of $x^{n^{k-1}}$ (n^{k-1} copies of x). It follows that

$$\text{HRNG}_k^\pi \in \text{NLIN}^\pi \cap \text{coNLIN}^\pi$$

and

$$\text{HRNG}_k^\pi \in \text{NTIME}^\pi(n^k) \cap \text{coNTIME}^\pi(n^k)$$

for all $k \geq 1$.

The following lemma implies Theorem 5.1.

► **Lemma 5.3.** *Let $k \geq 0$.*

1. *The set $X = \{\pi \in \Pi \mid \text{HRNG}_{k+3}^\pi \text{ is not } \text{DTIME}(2^{kn})^\pi\text{-immune}\}$ has $O(n)$ -honest \mathfrak{p} -permutation-betting-game measure 0.*
2. *The set $X = \{\pi \in \Pi \mid \text{POLYHRNG}_{k+1}^\pi \text{ is not } \text{DTIME}(2^{n^k})^\pi\text{-immune}\}$ has $O(n^k)$ -honest \mathfrak{p}_2 -permutation-betting-game measure 0.*

By symmetry of $\text{NLIN}^\pi \cap \text{coNLIN}^\pi$ and $\text{NTIME}^\pi(n^k) \cap \text{coNTIME}^\pi(n^k)$, Lemma 5.3 also applies to the complement of HRNG_{k+3}^π and $\text{POLYHRNG}_{k+1}^\pi$. Therefore, both languages are bi-immune and Theorem 5.1 follows.

Combining Lemma 5.3 with Proposition 3.19 also gives the following corollary. In the next section we will prove more results about \mathfrak{p} space-random permutations.

► **Corollary 5.4.**

1. *If π is a \mathfrak{p} space-random permutation, then $\text{NLIN}^\pi \cap \text{coNLIN}^\pi$ contains a $\text{DTIME}^\pi(2^{kn})$ -bi-immune language for all $k \geq 1$.*
2. *If π is a \mathfrak{p}_2 space-random permutation, then $\text{NP}^\pi \cap \text{coNP}^\pi$ contains a $\text{DTIME}^\pi(2^{n^k})$ -bi-immune language for all $k \geq 1$.*

6 Random Permutations for $\text{NP} \cap \text{coNP}$ versus Quantum Computation

Bennett, Bernstein, Brassard, and Vazirani [3] showed that $\text{NP}^\pi \cap \text{coNP}^\pi \not\subseteq \text{BQTIME}^\pi(o(2^{n/3}))$ relative to a random permutation π with probability 1. In this section we investigate how much of their result holds relative to individual random oracles at the space-bounded level.

We begin with a general lemma about test languages and QTM. We write $\text{PP}_{\leq n} = \{g \in \text{PP} \mid |g| \leq 2^{n+1} - 1\}$ for all prefix partial permutations defined on strings in $\{0,1\}^{\leq n}$. For a string s_i in the standard enumeration, we write $g \upharpoonright s_i$ for the length i prefix of g . In other words, $g \upharpoonright s_i = [g(s_0), \dots, g(s_{i-1})]$.

► **Lemma 6.1.** *Let π be a permutation with an associated test language L_π and let $p(n)$ and $q(n)$ be polynomials. If for some oracle QTM M and some function $l(n)$ the following conditions hold, then π is not a pspace -random permutation.*

1. *The membership of 0^n in L_π depends on the membership of the strings of length at most $p(n)$.*
2. *M^π decides L_π with error probability δ , for some constant $0 < \delta < 1$, and queries only strings of length at most $l(n)$.*
3. *For any partial prefix permutation $\rho \in \text{PP}\Pi_{\leq l(n)}$, the conditional probability*

$$\Pr_{|\psi|=l(n)} [M^\psi(0^n) = L_\psi(0^n) \mid \rho \sqsubseteq \psi]$$

is computable in $(|\rho| + 2^n)^{O(1)}$ space.

4. *For some constant $1 > \epsilon > \delta$ and for all but finitely many n ,*

$$\Pr_{|\psi|=l(n)} [M^\psi(0^n) = L_\psi(0^n) \mid \pi \upharpoonright 0^n \sqsubseteq \psi] < 1 - \epsilon.$$

In the following Theorem, we use Lemma 6.1 to extend the result by Bennett, Bernstein, Brassard, and Vazirani [3] to pspace -random permutations.

► **Theorem 6.2.** *If π is a pspace -random permutation, then $\text{NLIN}^\pi \cap \text{coNLIN}^\pi$ is not contained in BQP^π .*

We now refine the previous result by considering more restricted quantum machines that only query strings of $O(n)$ length. This restriction allows us to extend the result to machines with running time $o(2^{n/3})$, analogous to the result of Bennett et al. [3]. Whether this extension holds without the restriction on query length remains an open problem.

► **Theorem 6.3.** *If π is a pspace -random permutation and $T(n) = o(2^{n/3})$, then $\text{NLIN}^\pi \cap \text{coNLIN}^\pi$ is not contained $\text{BQTIME}^{\pi, O(n)\text{-honest}}(T(n))$.*

Together, these theorems extend the classical separation of Bennett et al. [3] to individual pspace -random permutations, both in the general and the honest-query setting.

7 Random Oracles for $\text{NP} \cap \text{coNP}$ and 0-1 Laws for Measure in EXP

Tardos [23] used the characterizations

$$\text{BPP} = \text{ALMOST-P} = \{A \mid \Pr_R [A \in \text{P}^R] = 1\} \quad [4]$$

and

$$\text{AM} = \text{ALMOST-NP} = \{A \mid \Pr_R [A \in \text{NP}^R] = 1\} \quad [20]$$

to prove the following conditional theorem separating P from $\text{NP} \cap \text{coNP}$ relative to a random oracle.

► **Theorem 7.1** (Tardos [23]). *If $\text{AM} \cap \text{coAM} \neq \text{BPP}$, then $\text{P}^R \neq \text{NP}^R \cap \text{coNP}^R$ for a random oracle R with probability 1.*

Recently, Ghosal et al. [9] used non-interactive zero-knowledge (NIZK) proofs to prove a similar conditional theorem.

► **Theorem 7.2** (Ghosal et al. [9]). *If $UP \not\subseteq RP$, then $P^R \neq NP^R \cap coNP^R$ for a random oracle R with probability 1.*

In this section we use Theorems 7.1 and 7.2 to connect the open problem of P versus $NP \cap coNP$ relative to a random oracle to open questions about the resource-bounded measure of complexity classes within EXP . In particular, we relate the problem to measure 0-1 laws and measurability in EXP . First, we need the following derandomization lemma. The first two parts follow from previous work, while the third part of the lemma is a new observation as far as we know, though its proof uses the techniques from the proofs of the first two parts.

► **Lemma 7.3.**

1. *If $\mu_p(NP) \neq 0$, then $BPP \subseteq NP \cap coNP = AM \cap coAM$.*
2. *If $\mu_p(UP \cap coUP) \neq 0$, then $BPP \subseteq UP \cap coUP$.*
3. *If $\mu_p(FewP) \neq 0$, then $BPP \subseteq FewP \cap coFewP$.*

In the following theorem, we have three hypotheses where a complexity class X is assumed to be not equal to EXP and the p -measure of a subclass of X is concluded to be 0.

► **Theorem 7.4.** *Suppose that $P^R = NP^R \cap coNP^R$ for a random oracle R with probability 1. Then all of the following hold:*

1. $NP \neq EXP \Rightarrow \mu_p(NP \cap coNP) = 0$.
2. $UP \neq EXP \Rightarrow \mu_p(UP \cap coUP) = 0$.
3. $FewP \neq EXP \Rightarrow \mu_p(UP) = 0$.

Theorem 7.4 has the following corollary about measure 0-1 laws in EXP . We recall the definitions $\mu(X \mid EXP) = 0$ if $\mu_{p_2}(X \cap EXP) = 0$ and $\mu(X \mid EXP) = 1$ if $\mu_{p_2}(X^c \mid EXP) = 0$ [14].

► **Corollary 7.5.** *Suppose that $P^R = NP^R \cap coNP^R$ for a random oracle R with probability 1. Then all of the following hold:*

1. $\mu(NP \cap coNP \mid EXP) \in \{0, 1\}$.
2. $\mu(UP \cap coUP \mid EXP) \in \{0, 1\}$.
3. $\mu(UP \mid EXP) = 0$ or $\mu(FewP \mid EXP) = 1$.

In the third case of Corollary 7.5, we almost have a 0-1 law for UP . Can a full 0-1 law be obtained?

The contrapositives of the implications in Corollary 7.5 show that the random oracle question for P versus $NP \cap coNP$ is resolved under nonmeasurability hypotheses. A complexity class X is defined to be *not measurable* in EXP if $\mu(X \mid EXP) \neq 0$ and $\mu(X \mid EXP) \neq 1$ [15, 21].

► **Corollary 7.6.**

1. *If $NP \cap coNP$ is not measurable in EXP , then $P^R \neq NP^R \cap coNP^R$ for a random oracle R with probability 1.*
2. *If $UP \cap coUP$ is not measurable in EXP , then $P^R \neq NP^R \cap coNP^R$ for a random oracle R with probability 1.*
3. *If UP and $FewP$ are both not measurable in EXP , then $P^R \neq NP^R \cap coNP^R$ for a random oracle R with probability 1.*

On the other hand, if the consequence of Corollary 7.6 can be proved with measure in EXP , then we would have $BPP \neq EXP$, which implies $\mu(BPP \mid EXP) = 0$ by the 0-1 law for BPP [24].

► **Theorem 7.7.** *If $\{A \mid P^A = NP^A \cap \text{coNP}^A\}$ has measure 0 in EXP, then $\mu(\text{BPP} \mid \text{EXP}) = 0$.*

These results suggest that resolving whether $P^R = NP^R \cap \text{coNP}^R$ relative to a random oracle requires a deeper understanding of the resource-bounded measurability within EXP of fundamental subclasses such as BPP, NP, UP, and FewP.

8 Conclusion

We have introduced resource-bounded random permutations and shown that $P^\pi \neq NP^\pi \cap \text{coNP}^\pi$ for all p-betting-game random permutations. We remark that all of the results in Sections 5 and 6 about $\text{NLIN} \cap \text{coNLIN}$ and $NP \cap \text{coNP}$ hold for their unambiguous versions $\text{ULIN} \cap \text{coULIN}$ and $\text{UP} \cap \text{coUP}$, respectively. An interesting open problem is whether our main theorem can be improved from betting-game random permutations to random permutations.

► **Question 8.1.** *Does $P^\pi \neq NP^\pi \cap \text{coNP}^\pi$ for a p-random permutation π ?*

More generally, the relative power of permutation martingales versus betting games should be investigated.

► **Question 8.2.** *Are polynomial-time permutation martingales and permutation betting games equivalent?*

We proved two restricted versions of the Bennett et al. [3] random permutation separation. Does the full version hold relative to individual random permutations?

► **Question 8.3.** *If π is a pspace-random permutation and $T(n) = o(2^{n/3})$, is $\text{NLIN}^\pi \cap \text{coNLIN}^\pi$ not contained in $\text{BQTIME}^\pi(T(n))$?*

References

- 1 K. Ambos-Spies and E. Mayordomo. Resource-bounded measure and randomness. In A. Sorbi, editor, *Complexity, Logic and Recursion Theory*, Lecture Notes in Pure and Applied Mathematics, pages 1–47. Marcel Dekker, New York, N.Y., 1997. doi:10.1201/9780429187490-1.
- 2 J. L. Balcázar and U. Schöning. Bi-immune sets for complexity classes. *Mathematical Systems Theory*, 18:1–10, 1985. doi:10.1007/bf01699457.
- 3 C. H. Bennett, E. Bernstein, G. Brassard, and U. V. Vazirani. Strengths and weaknesses of quantum computing. *SIAM Journal on Computing*, 26(5):1510–1523, 1997. doi:10.1137/S0097539796300933.
- 4 C. H. Bennett and J. Gill. Relative to a random oracle A , $P^A \neq NP^A \neq \text{co-NP}^A$ with probability 1. *SIAM Journal on Computing*, 10:96–113, 1981. doi:10.1137/0210008.
- 5 R. V. Book, J. H. Lutz, and K. W. Wagner. An observation on probability versus randomness with applications to complexity classes. *Mathematical Systems Theory*, 27:201–209, 1994. doi:10.1007/bf01578842.
- 6 H. Buhrman, D. van Melkebeek, K. W. Regan, D. Sivakumar, and M. Strauss. A generalization of resource-bounded measure, with application to the BPP vs. EXP problem. *SIAM Journal on Computing*, 30(2):576–601, 2001. doi:10.1137/S0097539798343891.
- 7 W. Diffie and M. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, 1976. doi:10.1109/TIT.1976.1055638.
- 8 P. Flajolet and J. Steyaert. On sets having only hard subsets. In *Proc. 2nd Colloq. on Automata, Languages, and Programming, Lecture Notes in Computer Science*, volume 14, pages 446–457. Springer-Verlag, Berlin, 1974. doi:10.1007/978-3-662-21545-6_34.

- 9 Riddhi Ghosal, Yuval Ishai, Alexis Korb, Eyal Kushilevitz, Paul Lou, and Amit Sahai. Hard languages in $\text{NP} \cap \text{coNP}$ and NIZK proofs from unstructured hardness. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing, STOC 2023*, pages 1243–1256, New York, NY, USA, 2023. Association for Computing Machinery. doi:10.1145/3564246.3585119.
- 10 R. C. Harkins and J. M. Hitchcock. Exact learning algorithms, betting games, and circuit lower bounds. *ACM Transactions on Computation Theory*, 5(4):article 18, 2013. doi:10.1145/2539126.2539130.
- 11 J. M. Hitchcock and J. H. Lutz. Why computational complexity requires stricter martingales. *Theory of Computing Systems*, 39(2):277–296, 2006. doi:10.1007/s00224-005-1135-4.
- 12 J. M. Hitchcock, A. Sekoni, and H. Shafei. Polynomial-time random oracles and separating complexity classes. *ACM Transactions on Computation Theory*, 13(1), 2021. doi:10.1145/3434389.
- 13 A. Klivans and D. van Melkebeek. Graph nonisomorphism has subexponential size proofs unless the polynomial-time hierarchy collapses. *SIAM Journal on Computing*, 31(5):1501–1526, 2002. doi:10.1137/s0097539700389652.
- 14 J. H. Lutz. Almost everywhere high nonuniform complexity. *Journal of Computer and System Sciences*, 44(2):220–258, 1992. doi:10.1016/0022-0000(92)90020-j.
- 15 J. H. Lutz. The quantitative structure of exponential time. In L. A. Hemaspaandra and A. L. Selman, editors, *Complexity Theory Retrospective II*, pages 225–254. Springer-Verlag, 1997. doi:10.1007/978-1-4612-1872-2_10.
- 16 J. H. Lutz and W. J. Schmidt. Circuit size relative to pseudorandom oracles. *Theoretical Computer Science*, 107(1):95–120, March 1993. doi:10.1016/0304-3975(93)90256-s.
- 17 P. Martin-Löf. The definition of random sequences. *Information and Control*, 9:602–619, 1966. doi:10.1016/s0019-9958(66)80018-9.
- 18 W. Merkle, J. S. Miller, A. Nies, J. Reimann, and F. Stephan. Kolmogorov-Loveland randomness and stochasticity. *Annals of Pure and Applied Logic*, 138(1–3):183–210, 2006. doi:10.1016/j.apal.2005.06.011.
- 19 A. A. Muchnik, A. L. Semenov, and V. A. Uspensky. Mathematical metaphysics of randomness. *Theoretical Computer Science*, 207(2):263–317, 1998. doi:10.1016/S0304-3975(98)00069-3.
- 20 N. Nisan and A. Wigderson. Hardness vs randomness. *Journal of Computer and System Sciences*, 49(2):149–167, 1994. doi:10.1016/s0022-0000(05)80043-1.
- 21 K. W. Regan, D. Sivakumar, and J. Cai. Pseudorandom generators, measure theory, and natural proofs. In *Proceedings of the 36th Symposium on Foundations of Computer Science*, pages 26–35. IEEE Computer Society, 1995. doi:10.1109/SFCS.1995.492459.
- 22 R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, February 1978. doi:10.1145/359340.359342.
- 23 G. Tardos. Query complexity, or why is it difficult to separate $\text{NP}^A \cap \text{coNP}^A$ from P^A by random oracles A ? *Combinatorica*, 9(4):385–392, 1989. doi:10.1007/BF02125350.
- 24 D. van Melkebeek. The zero-one law holds for BPP. *Theoretical Computer Science*, 244(1–2):283–288, 2000. doi:10.1016/s0304-3975(00)00191-2.
- 25 J. Ville. *Étude Critique de la Notion de Collectif*. Gauthier-Villars, Paris, 1939.