# Open Questions on the Bernoulli Factory Problem

Peter Occil

Open Questions on the Bernoulli Factory Problem

This version of the document is dated 2023-07-15.

**Peter Occil**

## 1 Background

Suppose there is a coin that shows heads with an unknown probability, $\lambda$. The goal is to use that coin (and possibly also a fair coin) to build a "new" coin that shows heads with a probability that depends on $\lambda$, call it $f(\lambda)$. This is the *Bernoulli factory problem*, and it can be solved only for certain functions $f$. (For example, flipping the coin twice and taking heads only if exactly one coin shows heads, the probability $2\lambda(1-\lambda)$ can be simulated.)

Specifically, the only functions that can be simulated this way **are continuous and polynomially bounded on their domain, and map** $[0,1]$ **or a subset thereof to** $[0,1]$, as well as $f=0$ and $f=1$. These functions are called *factory functions* in this page. (A function $f(x)$ is *polynomially bounded* if both $f$ and $1-f$ are greater than or equal to $\min(x^n, (1-x)^n)$ for some integer $n$ (Keane and O'Brien 1994)[1]. This implies that $f$ admits no roots on (0, 1) and can't take on the value 0 or 1 except possibly at 0, 1, or both.)

This page contains several questions about the **Bernoulli factory**[2] problem. Answers to them will greatly improve my pages on this site about Bernoulli factories. If you can answer any of them, post an issue in the **GitHub issues page**[3].

> **Note:** The Bernoulli factory problem is a special case of a more general mathematical problem that I call "**The Sampling Problem**[4]".

## 2 Contents


- **Background**
- **Contents**
- **Polynomials that approach a factory function "fast"**
  - **Main Question**
  - **Solving the Bernoulli factory problem with polynomials**
  - **A Matter of Efficiency**
  - **A Conjecture on Polynomial Approximation**
  - **Strategies**
- **Other Questions**


[1] Keane, M. S., and O'Brien, G. L., "A Bernoulli factory", *ACM Transactions on Modeling and Computer Simulation* 4(2), 1994.

[2] https://peteroupc.github.io/bernoulli.html

[3] https://github.com/peteroupc/peteroupc.github.io/issues

[4] https://peteroupc.github.io/sampling.html

- **End Notes**
- **Notes**

# 3 Polynomials that approach a factory function "fast"

This question involves solving the Bernoulli factory problem with polynomials.[5]

In this question, a polynomial $P(x)$ is written in *Bernstein form of degree* $n$ if it is written as—

$$P(x) = \sum_{k=0}^{n} a_k \binom{n}{k} x^k (1-x)^{n-k},$$

where $a_0, ..., a_n$ are the polynomial's *Bernstein coefficients*.

The degree-$n$ *Bernstein polynomial* of an arbitrary function $f(x)$ has Bernstein coefficients $a_k = f(k/n)$. In general, this Bernstein polynomial differs from $f$ even if $f$ is a polynomial.

## 3.1 Main Question

Suppose $f : [0,1] \to [0,1]$ is continuous and belongs to a large class of functions (for example, the $k$-th derivative, $k \geq 0$, is continuous, Lipschitz continuous, concave, strictly increasing, or bounded variation, or $f$ is real analytic).

1. (*Exact Bernoulli factory*): Compute the Bernstein coefficients of a sequence of polynomials $(g_n)$ of degree 2, 4, 8, ..., $2^i$, ... that converge to $f$ from below and satisfy: $(g_{2n} - g_n)$ is a polynomial with non-negative Bernstein coefficients once it's rewritten to a polynomial in Bernstein form of degree exactly $2n$. (**See Note 3 in "End Notes".**) Assume $0 < f(\lambda) < 1$ or $f$ is polynomially bounded.
2. (*Approximate Bernoulli factory*): Given $\epsilon > 0$, compute the Bernstein coefficients of a polynomial or rational function (of some degree $n$) that is within $\epsilon$ of $f$.
3. (*Series expansion of simple functions*): Find a non-negative random variable $X$ and a series $f(\lambda) = \sum_{a \geq 0} \gamma_a(\lambda)$ such that $\gamma_a(\lambda)/\mathbb{P}(X = a)$ (letting $0/0$ equal 0) is a polynomial or rational function with rational Bernstein coefficients lying in $[0,1]$. (**See note 1 in "End Notes".**)

The convergence rate must be $O(1/n^{r/2})$ if the class has only functions with Lipschitz-continuous $(r-1)$-th derivative. The method may not introduce transcendental or trigonometric functions (as with Chebyshev interpolants).

## 3.2 Solving the Bernoulli factory problem with polynomials

An **algorithm**[6] (Łatuszyński et al. 2009/2011)[7] simulates a factory function $f(\lambda)$ via two sequences of polynomials that converge from above and below to that function. Roughly speaking, the algorithm works as follows:

[5]See also the following questions on *Mathematics Stack Exchange* and *MathOverflow*: **Converging polynomials**, **Error bounds**, **A conjecture**, **Hypergeometric random variable**, **Lorentz operators**, **Derivatives of moments**, **Series representations**. https://math.stackexchange.com/questions/3904732/what-are-ways-to-compute-polynomials-that-converge-from-above-and-below-to-a-con https://mathoverflow.net/questions/442057/explicit-and-fast-error-bounds-for-approximating-continuous-functions https://mathoverflow.net/questions/427595/a-conjecture-on-consistent-monotone-sequences-of-polynomials-in-bernstein-form https://mathoverflow.net/questions/429037/bounds-on-the-expectation-of-a-function-of-a-hypergeometric-random-variable https://mathoverflow.net/questions/407179/using-the-holtz-method-to-build-polynomials-that-converge-to-a-continuous-functi https://mathoverflow.net/questions/447064/explicit-bounds-on-derivatives-of-moments-related-to-bernstein-polynomials https://mathoverflow.net/questions/409174/concave-functions-series-representation-and-converging-polynomials

[6]https://peteroupc.github.io/bernoulli.html#General_Factory_Functions

[7]Łatuszyński, K., Kosmidis, I., Papaspiliopoulos, O., Roberts, G.O., "**Simulating events of unknown probabilities via reverse time martingales**", arXiv:0907.4018v2 [stat.CO], 2009/2011. https://arxiv.org/abs/0907.4018v2

1. Generate U, a uniform random variate in $[0, 1]$.
2. Flip the input coin (with a probability of heads of $\lambda$), then build an upper and lower bound for $f(\lambda)$, based on the outcomes of the flips so far. In this case, these bounds come from two degree-$n$ polynomials that approach $f$ as $n$ gets large, where $n$ is the number of coin flips so far in the algorithm.
3. If U is less than or equal to the lower bound, return 1. If U is greater than the upper bound, return 0. Otherwise, go to step 2.

The result of the algorithm is 1 with probability *exactly* equal to $f(\lambda)$, or 0 otherwise.

However, the algorithm requires the polynomial sequences to meet certain requirements; among them, the sequences must be of Bernstein-form polynomials that converge from above and below to a factory function. Specifically:

*For $f(\lambda)$ there must be a sequence of polynomials $(g_n)$ in Bernstein form of degree 1, 2, 3, … that converge to $f$ from below and satisfy: $(g_{n+1} - g_n)$ is a polynomial with non-negative Bernstein coefficients once it's rewritten to a polynomial in Bernstein form of degree exactly $n + 1$ (**see Note 3 in "End Notes"**; Nacu and Peres (2005)[8]; Holtz et al. (2011)[9]). For $f(\lambda) = 1 - f(\lambda)$ there must likewise be a sequence of this kind.*

## 3.3 A Matter of Efficiency

However, ordinary Bernstein polynomials converge to a function at the rate $\Omega(1/n)$ in general, a result known since Voronovskaya (1932)[10] and a rate that will lead to an **infinite expected number of coin flips in general**. (See also my **supplemental notes**[11].)

But Lorentz (1966)[12] showed that if the function is positive and has a continuous $k$-th derivative, there are polynomials with nonnegative Bernstein coefficients that converge at the rate $O(1/n^{k/2})$ (and thus can enable a **finite expected number of coin flips** if the function is "smooth" enough).

Thus, people have developed alternatives, including linear combinations and iterated Boolean sums of Bernstein polynomials, to improve the convergence rate. These include Micchelli (1973)[13], Guan (2009)[14], Güntürk and Li (2021a)[15], (2021b)[16], the "Lorentz operator" in Holtz et al. (2011)[17], Draganov (2014), and Tachev (2022)[18].

These alternative polynomials usually include results where the error bound is the desired $O(1/n^{k/2})$, but most of those results (e.g., Theorem 4.4 in Micchelli; Theorem 5 in Güntürk and Li) have hidden constants with no upper bounds given, making them unimplementable (that is, it can't be known beforehand whether a given polynomial will come close to the target function within a user-specified error tolerance).

[8]Nacu, Şerban, and Yuval Peres. "Fast simulation of new coins from old", The Annals of Applied Probability 15, no. 1A (2005): 93-115.

[9]Holtz, O., Nazarov, F., Peres, Y., "**New Coins from Old, Smoothly**", Constructive Approximation 33 (2011). https://link.springer.com/article/10.1007/s00365-010-9108-5

[10]E. Voronovskaya, "Détermination de la forme asymptotique d'approximation des fonctions par les polynômes de M. Bernstein", 1932.

[11]https://peteroupc.github.io/bernsupp.html

[12]G.G. Lorentz, "The degree of approximation by polynomials with positive coefficients", 1966.

[13]Micchelli, Charles. "**The saturation class and iterates of the Bernstein polynomials**", Journal of Approximation Theory 8, no. 1 (1973): 1-18. https://www.sciencedirect.com/science/article/pii/0021904573900282

[14]Guan, Zhong. "**Iterated Bernstein polynomial approximations**." arXiv preprint arXiv:0909.0684 (2009). https://arxiv.org/pdf/0909.0684

[15]Güntürk, C. Sinan, and Weilin Li. "**Approximation with one-bit polynomials in Bernstein form**", arXiv:2112.09183 (2021); Constructive Approximation, pp.1-30 (2022). https://arxiv.org/pdf/2112.09183

[16]Güntürk, C. Sinan, and Weilin Li. "**Approximation of functions with one-bit neural networks**", arXiv:2112.09181 (2021). https://arxiv.org/abs/2112.09181

[17]Holtz, O., Nazarov, F., Peres, Y., "**New Coins from Old, Smoothly**", Constructive Approximation 33 (2011). https://link.springer.com/article/10.1007/s00365-010-9108-5

[18]Tachev, Gancho. "**Linear combinations of two Bernstein polynomials**", *Mathematical Foundations of Computing*, 2022. https://doi.org/10.3934/mfc.2022061

## 3.4 A Conjecture on Polynomial Approximation

The following is a **conjecture**[19] that could help reduce this problem to the problem of finding explicit error bounds when approximating a function by polynomials.

Let $f(\lambda) : [0,1] \to (0,1)$ have $r \geq 1$ continuous derivatives, let $M$ be the maximum of the absolute value of $f$ and its derivatives up to the $r$-th derivative, and denote the Bernstein polynomial of degree $n$ of a function $g$ as $B_n(g)$. Let $W_{2^0}(\lambda), W_{2^1}(\lambda), ..., W_{2^i}(\lambda), ...$ be a sequence of functions on [0, 1] that converge uniformly to $f$.

For each integer $n \geq 1$ that's a power of 2, suppose that there is $D > 0$ such that—

$$|f(\lambda) - B_n(W_n(\lambda))| \leq DM/n^{r/2},$$

whenever $0 \leq \lambda \leq 1$. Then there is $C_0 \geq D$ such that for every $C \geq C_0$, the polynomials $(g_n)$ in Bernstein form of degree 2, 4, 8, ..., $2^i$, ..., defined as $g_n = B_n(W_n(\lambda) - CM/n^{r/2})$, converge from below to $f$ and satisfy: $(g_{2n} - g_n)$ is a polynomial with non-negative Bernstein coefficients once it's rewritten to a polynomial in Bernstein form of degree exactly $2n$. (**See Note 3 in "End Notes".**)

Equivalently (see also Nacu and Peres (2005)[20]), there is $C_1 > 0$ such that the inequality $(PB)$ (see below) holds true for each integer $n \geq 1$ that's a power of 2 (see "Strategies", below).

My goal is to see not just whether this conjecture is true, but also which value of $C_0$ (or $C_1$) suffices for the conjecture, especially for any combination of the special cases mentioned at the end of "**Main Question**", above.

## 3.5 Strategies

The following are some strategies for answering these questions:

- For iterated Boolean sums (linear combinations of iterates) of Bernstein polynomials ($U_{n,k}$ in **Micchelli 1973**[21]; see also **Güntürk and Li**[22]), verify my **proofs of these bounds in Propositions B10C and B10D**[23].
- For linear combinations of Bernstein polynomials (Butzer (1953)[24], **Tachev 2022**[25]), verify my proof of those error bounds in **my Proposition B10**[26].
- For the "**Lorentz operator**[27]" (Holtz et al. 2011)[28], find explicit bounds, with no hidden constants, on the approximation error for the operator $Q_{n,r}(f)$ and for the polynomials $(f_n)$ and $(g_n)$ formed with it, and find the hidden constants $\theta_\alpha$, $s$, and $D$ as well as those in Lemmas 15, 17 to 22, 24, and 25 in the paper. Or verify my proof of the order-2 operator's error bounds in **my Proposition B10A**[29]. The bounds should have the form $C \cdot \max((\lambda(1-\lambda)/n)^{1/2}, 1/n)^r$, where $C$ is an explicitly given constant depending only on $f$ and $r$.
- Let $f : [-1,1] \to [0,1]$ be continuous. Find explicit bounds, with no hidden constants, on the error in approximating $f$ with the following polynomials: The polynomials are similar to Chebyshev interpolants, but evaluate $f$ at *rational* values of $\lambda$ that converge to Chebyshev or Legendre points (e.g.,

[19] https://peteroupc.github.io/bernsupp.html#A_Conjecture_on_Polynomial_Approximation

[20] Nacu, Şerban, and Yuval Peres. "Fast simulation of new coins from old", The Annals of Applied Probability 15, no. 1A (2005): 93-115.

[21] https://www.sciencedirect.com/science/article/pii/0021904573900282

[22] https://arxiv.org/abs/2112.09181

[23] https://peteroupc.github.io/bernapprox.html#Results_Used_in_Approximations_by_Polynomials

[24] Butzer, P.L., "Linear combinations of Bernstein polynomials", Canadian Journal of Mathematics 15 (1953).

[25] https://doi.org/10.3934/mfc.2022061

[26] https://peteroupc.github.io/bernapprox.html#Results_Used_in_Approximations_by_Polynomials

[27] https://link.springer.com/article/10.1007/s00365-010-9108-5

[28] Holtz, O., Nazarov, F., Peres, Y., "**New Coins from Old, Smoothly**", Constructive Approximation 33 (2011). https://link.springer.com/article/10.1007/s00365-010-9108-5

[29] https://peteroupc.github.io/bernapprox.html#Results_Used_in_Approximations_by_Polynomials

converging to $\cos(j\pi/n)$ with increasing $n$). The error bounds must be close to those of Chebyshev interpolants (see, e.g., chapters 7, 8, and 12 of Trefethen, ***Approximation Theory and Approximation Practice***[30], 2013).

- Find other polynomial operators meeting the requirements of the main question (see "Main Question", above) and having explicit error bounds, with no hidden constants, especially operators that preserve polynomials of a higher degree than linear functions.
- Find a sequence of functions $(W_n(f))$ and an explicit and tight upper bound on $C_1 > 0$ such that, for each integer $n \geq 1$ that's a power of 2—

$$\left|\left(\sum_{i=0}^{k} W_n\left(\frac{i}{n}\right)\sigma_{n,k,i}\right) - W_{2n}\left(\frac{k}{2n}\right)\right| = |\mathbb{E}[W_n(X_k/n)] - W_{2n}(\mathbb{E}[X_k/n])| \leq \frac{C_1 M}{n^{r/2}}, \tag{PB}$$

whenever $0 \leq k \leq 2n$, where $M = \max(L, \max|f^{(0)}|, ..., \max|f^{(r-1)}|)$, $L$ is $\max|f^{(r)}|$ or the Lipschitz constant of $f^{(r-1)}$, $X_k$ is a hypergeometric($2n$, $k$, $n$) random variable, and $\sigma_{n,k,i} = \binom{n}{i}\binom{n}{k-i}/\binom{2n}{k} = \mathbb{P}(X_k = i)$ is the probability that $X_k$ equals $i$. (**See notes 3 and 4 in "End Notes" as well as "Proofs for Polynomial-Building Schemes**[31]**".**)

# 4 Other Questions

- Let $f(\lambda) : [0,1] \to [0,1]$ be writable as $f(\lambda) = \sum_{n\geq 0} a_n\lambda^n$, where $a_n \geq 0$ is rational, $a_n$ is nonzero infinitely often, and $f(1)$ is irrational. Then what are simple criteria to determine whether there is $0 < p < 1$ such that $0 \leq a_n \leq p(1-p)^n$ and, if so, to find such $p$? Obviously, if $(a_n)$ is nowhere increasing then $1 > p \geq a_0$.
- For each $r > 0$, characterize the functions $f(\lambda)$ that admit a Bernoulli factory where the expected number of coin flips, raised to the power of $r$, is finite.
- **Multiple-output Bernoulli factories**[32]**: Let $f(\lambda) : [a,b] \to (0,1)$ be continuous, where $0 < a$, $a < b$, $b < 1$.** Define the entropy bound as $h(f(\lambda))/h(\lambda)$, where $h(x) = -x\ln(x) - (1-x)\ln(1-x)$ is related to the Shannon entropy function. Then there is an algorithm that tosses heads with probability $f(\lambda)$ given a coin that shows heads with probability $\lambda$ and no other source of randomness (Keane and O'Brien 1994)[33].

  But, **is there an algorithm for $f$ that produces *multiple* outputs rather than one and has an expected number of coin flips per output that is arbitrarily close to the entropy bound, uniformly for every $\lambda$ in $f$'s domain**? Call such an algorithm an *optimal factory*. (See Nacu and Peres (2005, Question 1)[34].) And, does the answer change if the algorithm has access to a fair coin in addition to the biased coin?

  So far, constants as well as $\lambda$ and $1-\lambda$ do admit an optimal factory (see same work), and, as Yuval Peres (Jun. 24, 2021) told me, there is an efficient multiple-output algorithm for $f(\lambda) = \lambda/2$. But are there others? See an **appendix in one of my articles**[35] for more information on my progress on the problem.
- **Pushdown automata and algebraic functions**[36]: A *pushdown automaton* is a finite state machine with an unbounded stack, driven by a biased coin with an unknown probability of heads, $\lambda$. Its stack

[30] https://www.chebfun.org/ATAP/

[31] https://peteroupc.github.io/bernsupp.html#Proofs_for_Polynomial_Building_Schemes

[32] https://mathoverflow.net/questions/412772/from-biased-coins-to-biased-coins-as-efficiently-as-possible

[33] Keane, M. S., and O'Brien, G. L., "A Bernoulli factory", *ACM Transactions on Modeling and Computer Simulation* 4(2), 1994.

[34] Nacu, Şerban, and Yuval Peres. "Fast simulation of new coins from old", The Annals of Applied Probability 15, no. 1A (2005): 93-115.

[35] https://peteroupc.github.io/bernsupp.html#Multiple_Output_Bernoulli_Factory

[36] https://cstheory.stackexchange.com/questions/50853/from-coin-flips-to-algebraic-functions-via-pushdown-automata

starts with a single symbol. On each step, the machine flips the coin, then, based on the coin flip, the current state, and the top stack symbol, it moves to a new state (or keeps it unchanged) and replaces the top stack symbol with zero or more symbols. When the stack is empty, the machine stops and returns either 0 or 1 depending on the state it ends up at.

Let $f(\lambda)$ be continuous and map the open interval (0, 1) to itself. Mossel and Peres (2005)[37] showed that a pushdown automaton can output 1 with probability $f(\lambda)$ only if $f$ is *algebraic over the rational numbers* (there is a nonzero polynomial $P(x, y)$ in two variables and whose coefficients are rational numbers, such that $P(x, f(x)) = 0$ for every $x$ in the domain of $f$). See an **appendix in one of my articles**[38] for more information on my progress on the problem.

Prove or disprove:

1. If $f$ is algebraic over rational numbers it can be simulated by a pushdown automaton.
2. $\min(\lambda, 1-\lambda)$ and $\lambda^{1/p}$, for every prime $p \geq 3$, can be simulated by a pushdown automaton.
3. Given that $f$ is algebraic over rational numbers, it can be simulated by a pushdown automaton if and only if its "critical exponent" is a dyadic number greater than $-1$ or has the form $-1-1/2^k$ for some integer $k \geq 1$. (**See note 2 in "End Notes".**)

- **Coin-flipping degree**[39]: Let $p(\lambda)$ be a polynomial that maps the closed unit interval to itself and satisfies $0 < p(\lambda) < 1$ whenever $0 < \lambda < 1$. Then its *coin-flipping degree* (Wästlund 1999)[40] is the smallest value of $n$ such that $p$'s *Bernstein* coefficients of degree $n$ lie in the closed unit interval. Given that a polynomial's degree is $m$ and its "standard" coefficients are integers, what are upper bounds (or even exact maximums) on its coin flipping degree?

- **Simple simulation algorithms**[41]: References are sought to papers and books that describe irrational constants or Bernoulli factory functions (continuous functions mapping (0,1) to itself) in any of the following ways. Ideally they should involve only rational numbers and should not compute $p$-adic digit expansions.
  - Simulation experiments that succeed with an irrational probability.
  - Simple **continued fraction**[42] expansions of irrational constants.
  - Functions written as infinite power series with rational coefficients (see "**Certain Power Series**[43]").
  - Irrational numbers written as series expansions with rational coefficients (see "**Certain Converging Series**[44]").
  - Functions whose integral is an irrational number.
  - Closed shapes inside the unit square whose area is an irrational number. (Includes algorithms that tell whether a box lies inside, outside, or partly inside or outside the shape.) **Example.**[45]
  - Generate a uniform ($x$, $y$) point inside a closed shape, then return 1 with probability $x$. For what shapes is the expected value of $x$ an irrational number? **Example.**[46].

- Given integer $m \geq 0$, rational number $0 < k \leq \exp(1)$, and unknown heads probability $0 \leq \lambda \leq 1$, find

[37] Mossel, Elchanan, and Yuval Peres. New coins from old: computing with unknown bias. Combinatorica, 25(6), pp.707-724, 2005.

[38] https://peteroupc.github.io/bernsupp.html#Pushdown__Automata__and__Algebraic__Functions

[39] https://mathoverflow.net/questions/448538/bounds-on-the-coin-flipping-degree

[40] Wästlund, J., "**Functions arising by coin flipping**", 1999.

[41] https://stats.stackexchange.com/questions/541402/what-are-relatively-simple-simulations-that-succeed-with-an-irrational-probabili

[42] https://peteroupc.github.io/bernoulli.html#Continued__Fractions

[43] https://peteroupc.github.io/bernoulli.html#Certain__Power__Series

[44] https://peteroupc.github.io/bernoulli.html#Certain__Converging__Series

[45] https://peteroupc.github.io/bernoulli.html#pi____4

[46] https://peteroupc.github.io/bernsupp.html#4__3____pi

a **Bernoulli factory**[47] for—

$$f(\lambda) = \exp(-(\exp(m+\lambda) - (k(m+\lambda)))) = \frac{\exp(-\exp(m+\lambda))}{\exp(-(k(m+\lambda)))}, \tag{PD}$$

that, as much as possible, avoids calculating $h(\lambda) = \exp(m+\lambda) - k(m+\lambda)$; in this sense, the more implicitly the Bernoulli factory works with irrational or transcendental functions, the better. A solution is sought especially when $k$ is 1 or 2. Note that the right-hand side of (PD) can be implemented by **ExpMinus**[48] and division Bernoulli factories, but is inefficient and heavyweight due to the need to calculate $\epsilon$ for the division factory. In addition there is a Bernoulli factory that first calculates $h(\lambda)$ and $floor(h(\lambda))$ using constructive reals and then runs **ExpMinus**, but this is likewise far from lightweight. (Calculating exp(.) with floating-point operations is not acceptable for this question.)

Prove or disprove:

- Given that $f : [0,1] \to (0,1]$ is convex, the polynomials $(g_n) = (B_n(f) - \max_{0\le\lambda\le1} |B_n(f)(\lambda) - f(\lambda)|)$ (where $n \ge 1$ is an integer power of 2) are in Bernstein form of degree $n$, converge to $f$ from below, and satisfy: $(g_{2n} - g_n)$ is a polynomial with non-negative Bernstein coefficients once it's rewritten to a polynomial in Bernstein form of degree exactly $2n$. The same is true for the polynomials $(g_n) = (B_n(f) - |B_n(f)(1/2) - f(1/2)|)$, if $f$ is also symmetric about 1/2.
- Let $f : (D \subseteq [0,1]) \to [0,1]$. Given a coin that shows heads with probability $\lambda$ (which can be 0 or 1), it is possible to toss heads with probability $f(\lambda)$ using the coin and no other sources of randomness (and, thus, $f$ is ***strongly simulable***[49]) **if and only if**—
  - $f$ is constant on its domain, or is continuous and polynomially bounded on its domain (*polynomially bounded* means, both $f$ and $1-f$ are bounded below by $\min(x^n, (1-x)^n)$ for some integer $n$ (Keane and O'Brien 1994)[50]), and
  - $f(0)$ is 0 or 1 if 0 is in $f$'s domain and $f(1)$ is 0 or 1 whenever 1 is in $f$'s domain, and
  - if $f(0) = 0$ or $f(1) = 0$ or both, then there is a polynomial $g(x) : [0,1] \to [0,1]$ with computable coefficients, such that $g(0) = f(0)$ and $g(1) = f(1)$ whenever 0 or 1, respectively, is in the domain of f, and such that $g(x) > f(x)$ for every $x$ in the domain of $f$, except at 0 and 1, and
  - if $f(0) = 1$ or $f(1) = 1$ or both, then there is a polynomial $h(x) : [0,1] \to [0,1]$ with computable coefficients, such that $h(0) = f(0)$ and $h(1) = f(1)$ whenever 0 or 1, respectively, is in the domain of $f$, and such that $g(x) < f(x)$ for every $x$ in the domain of f, except at 0 and 1.

  A condition such as "0 is not in the domain of $f$, or $f$ can be extended to a Lipschitz continuous function on $[0,\epsilon)$ for some $\epsilon > 0$" does not work. A counterexample is $f(x) = (\sin(1/x)/4 + 1/2) \cdot (1-(1-x)^n)$ for $n \ge 1$ ($f(0) = 0$), which is strongly simulable at 0 despite not being Lipschitz at 0. ($(1-x)^n$ is the probability of the biased coin showing zero $n$ times in a row.) Keane and O'Brien already showed strong simulability when $D$ contains neither 0 nor 1.

# 5 End Notes

**Note 1**: An example of $X$ is $\mathbb{P}(X = a) = p(1-p)^a$ where $0 < p < 1$ is a known rational. This question's requirements imply that $\sum_{a\ge0} \max_\lambda |\gamma_a(\lambda)| \le 1$. The proof of Keane and O'Brien (1994)[51] produces a convex combination of polynomials with 0 and 1 as Bernstein coefficients, but the combination is difficult to construct (it requires finding maximums, for example) and so this proof does not appropriately answer this question.

[47] https://peteroupc.github.io/bernoulli.html

[48] https://peteroupc.github.io/bernoulli.html#ExpMinus_exp_minus___z

[49] https://mathoverflow.net/questions/404961/from-biased-coins-and-nothing-else-to-biased-coins

[50] Keane, M. S., and O'Brien, G. L., "A Bernoulli factory", *ACM Transactions on Modeling and Computer Simulation* 4(2), 1994.

[51] Keane, M. S., and O'Brien, G. L., "A Bernoulli factory", *ACM Transactions on Modeling and Computer Simulation* 4(2), 1994.

**Note 2**: On pushdown automata: Etessami and Yannakakis (2009)[52] showed that pushdown automata with rational probabilities are equivalent to recursive Markov chains (with rational transition probabilities), and that for every recursive Markov chain, the system of polynomial equations has nonnegative coefficients. But this paper doesn't deal with the case of recursive Markov chains where the transition probabilities cannot just be rational, but can also be $\lambda$ and $1-\lambda$ where $\lambda$ is an unknown rational or irrational probability of heads. Also, Banderier and Drmota (2014)[53] showed the asymptotic behavior of power series solutions $f(\lambda)$ of a polynomial system, where both the series and the system have nonnegative real coefficients. Notably, functions of the form $\lambda^{1/p}$ where $p \geq 3$ is not a power of 2, are not possible solutions, because their so-called "critical exponent" is not dyadic. But the result seems not to apply to *piecewise* power series such as $\min(\lambda, 1-\lambda)$, which are likewise algebraic functions.

**Note 3**: This condition is also known as a "consistency requirement"; it ensures that not only the polynomials "increase" to $f(\lambda)$, but also their Bernstein coefficients do as well. This condition is equivalent in practice to the following statement (Nacu & Peres 2005)[54]. For every integer $n \geq 1$ that's a power of 2, $a(2n,k) \geq \mathbb{E}[a(n, X_{n,k})] = \left(\sum_{i=0}^{k} a(n,i)\binom{n}{i}\binom{n}{k-i}/\binom{2n}{k}\right)$, where $a(n,k)$ is the degree-$n$ polynomial's $k$-th Bernstein coefficient, where $0 \leq k \leq 2n$ is an integer, and where $X_{n,k}$ is a hypergeometric($2n$, $k$, $n$) random variable. A hypergeometric($2n$, $k$, $n$) random variable is the number of "good" balls out of $n$ balls taken uniformly at random, all at once, from a bag containing $2n$ balls, $k$ of which are "good". See also my **MathOverflow question**[55] on finding bounds for hypergeometric variables.

**Note 4**: If $W_n(0) = f(0)$ and $W_n(1) = f(1)$ for every $n$, then the inequality $(PB)$ is automatically true when $k = 0$ and $k = 2n$, so that the statement has to be checked only for $0 < k < 2n$. If, in addition, $W_n$ is symmetric about 1/2, so that $W_n(\lambda) = W_n(1-\lambda)$ whenever $0 \leq \lambda \leq 1$, then the statement has to be checked only for $0 < k \leq n$ (since the values $\sigma_{n,k,i} = \binom{n}{i}\binom{n}{k-i}/\binom{2n}{k}$ are symmetric in that they satisfy $\sigma_{n,k,i} = \sigma_{n,k,k-i}$).This question is a problem of finding the *Jensen gap* of $W_n$ for certain kinds of hypergeometric random variables (**see Note 3**). Lee et al. (2021)[56] deal with a problem very similar to this one and find results that take advantage of $f$'s (here, $W_n$'s) smoothness, but unfortunately assume the variable is supported on an *open* interval, rather than a *closed* one (namely $[0,1]$) as in this question.Special cases for this question are if $W_n = 2f - B_n(f)$ and $r$ is 3 or 4, or $W_n = B_n(B_n(f)) + 3(f - B_n(f))$ and $r$ is 5 or 6.

Particularly for the case $W_n = 2f - B_n(f)$, the right-hand side of $(PB)$ is believed to be $O(1/n^{3/2})$ when $f$ has a Lipschitz continuous second derivative on $[0,1]$, but I have been unable to find a bound better than $O(1/n)$, especially because in one form or another my attempts at the bound seem to require an estimate of $|B_{2n}(f) - B_n(f)|$, which in general is no better than $O(1/n)$. Thus, a proof or counterexample of a bound of $O(1/n^{3/2})$ in this case would be appreciated.

# 6 Notes

[52]Etessami, K. And Yannakakis, M., "Recursive Markov chains, stochastic grammars, and monotone systems of nonlinear equations", Journal of the ACM 56(1), pp.1-66, 2009.

[53]Banderier, C. And Drmota, M., 2015. Formulae and asymptotics for coefficients of algebraic functions. Combinatorics, Probability and Computing, 24(1), pp.1-53.

[54]Nacu, Şerban, and Yuval Peres. "Fast simulation of new coins from old", The Annals of Applied Probability 15, no. 1A (2005): 93-115.

[55]https://mathoverflow.net/questions/429037/bounds-on-the-expectation-of-a-function-of-a-hypergeometric-random-variable

[56]Lee, Sang Kyu, Jae Ho Chang, and Hyoung-Moon Kim. "Further sharpening of Jensen's inequality." Statistics 55, no. 5 (2021): 1154-1168.