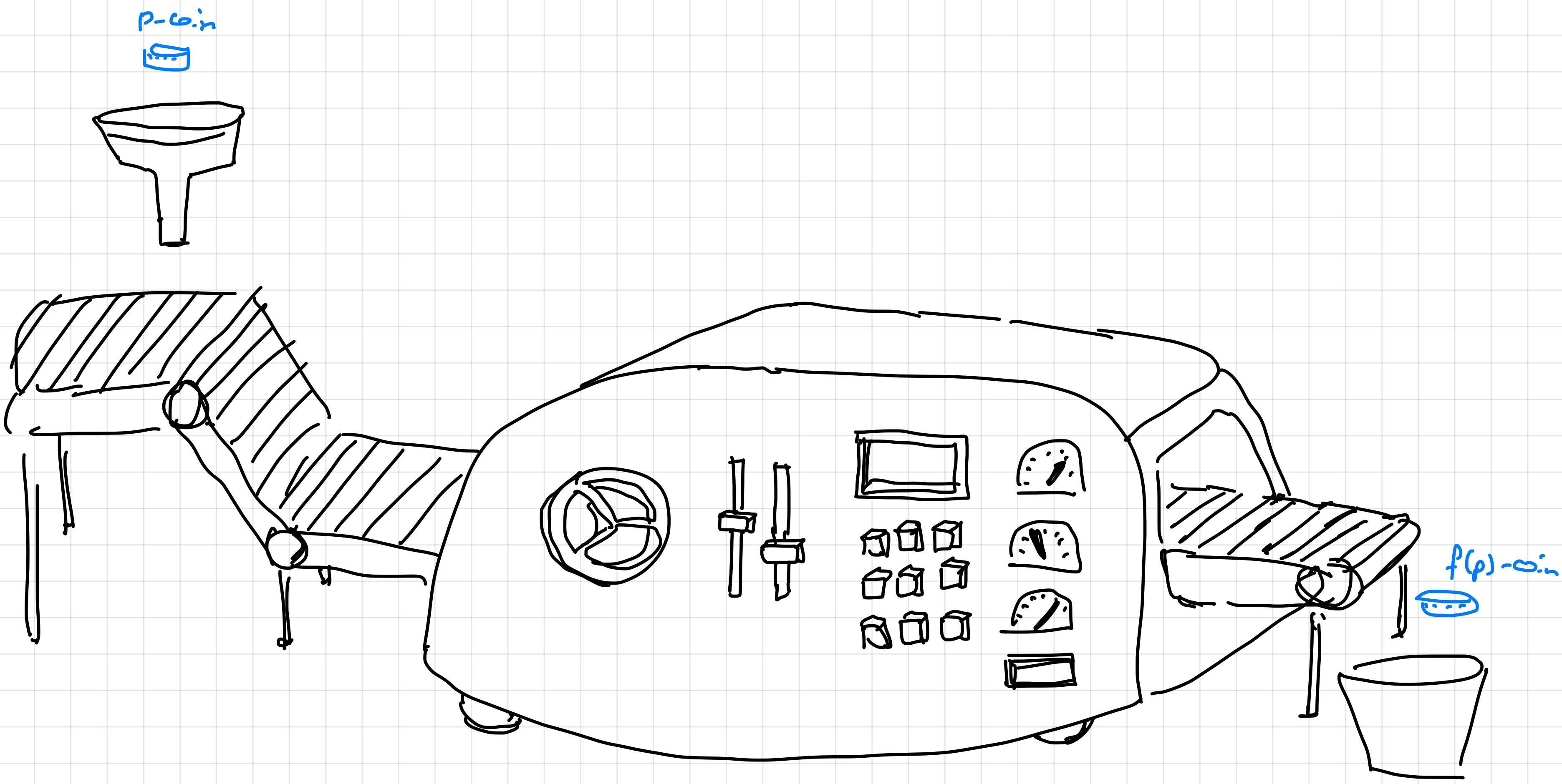
Bernoulli Factories

Renato Paes Leme
(Google Research)

(Bernoulli wearing a factory hat)

Bernoulli Factories



Examples of Simple Factories

1. $f(p) = p^2$

2. $f(p) = p(1-p)$

3. Bernstein monomials:

Single Parameter Bernoulli Factories

Given a function $f : S \subseteq (0,1) \to [0,1]$,

design an algorithm (decision tree)

that samples an $f(p)$-coin from a p-coin

(of unknown bias).

[Keane O'Brien 1994]

Von Neumann's Procedure

Sample an unbiased coin from a biased one

4 $f(p) = \frac{1}{2}$ for $p \in (0,1)$

Von Neumann's Procedure

Sample a coin of bias x from a biased one

(5) $f(p) = x$ for some fixed $x \in [0, 1)$

Bernstein Polynomials

(6) Bernstein polynomials $f(p) = \cdots$

(7) $f(p) = \dfrac{p}{2-p}$

Other Examples

(f) Moment Generating Functions, e.g. $f(p) = e^{p-1}$

Complete Characterization

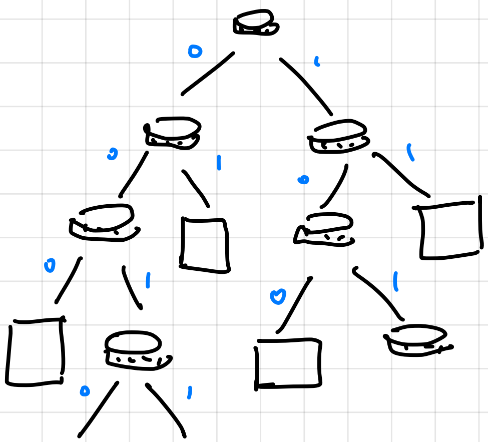
Which functions $f : S \subseteq (0,1) \longrightarrow [0,1]$

admit Bernoulli factories?

① What is a general factory?

② Examples of functions that don't admit factories

Generic Factory



Factory = Decision Tree

Nodes:

- p (p-coin)
- c (helper coin)
- $\boxed{0}$ $\boxed{1}$ (output)

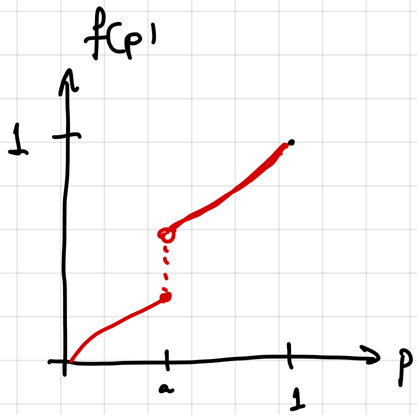
- Finite vs Infinite:

- Termination:

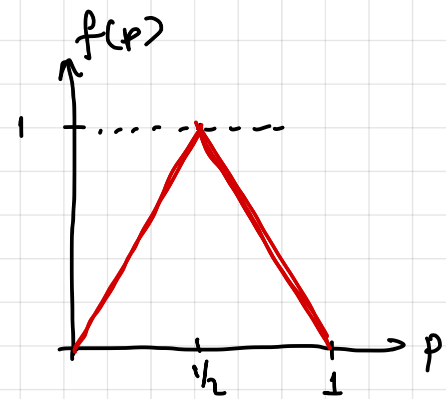
- $\mathbb{P}[\mathcal{F}(p)=1] =$

Functions Without Factories

(A)



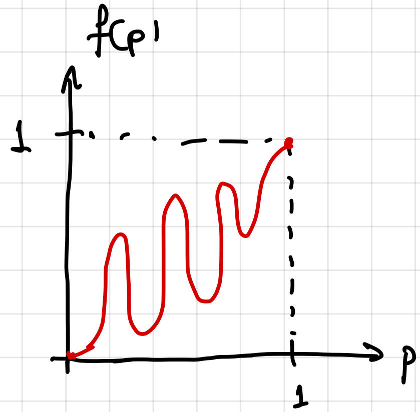
(B)



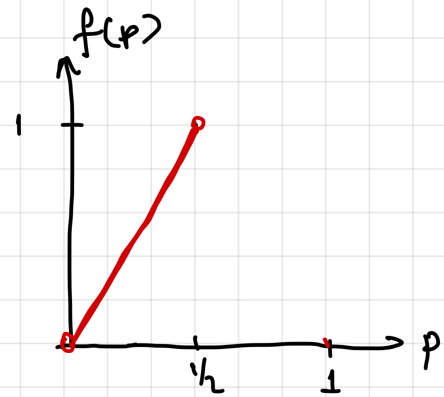
Functions Without Factories

Test Your Intuition. Which of these functions has a factory?

(C)



(D)



$f : (0, 1/2) \to (0, 1)$

Theorem (Keane, O'Brien)

Function $f: S \subseteq (0,1) \to (0,1)$ admits a factory if:

(1) it is continuous

(2) f is constant or poly-bounded

$\exists n$ s.t. $\min\left[f(p), 1-f(p)\right] \geq \min\left(p^n, (1-p)^n\right)$

Proof: Necessity:

Theorem (Keane, O'Brien)

Function $f: S \subseteq (0,1) \to (0,1)$ admits a factory if:

(1) it is continuous

(2) f is constant or poly-bounded

$\exists n$ s.t. $\min[f(p), 1-f(p)] \geq \min(p^n, 1-p^n)$

Lemma: Given f as in Thm, there is a function g implementable by a finite factory s.t.

$$0 \leq f(p) - \frac{1}{4} g(p) \leq \frac{3}{4}$$

s.t. $\frac{4}{3}\left(f(p) - \frac{1}{4} g(p)\right)$ is poly-bounded.

Lemma $\Rightarrow$ Thm

Theorem (Keane, O'Brien)

Function $f: S \subseteq (0,1) \to (0,1)$ admits a factory if:

(1) it is continuous

(2) f is constant or poly-bounded

$\exists n$ s.t. $\min\left[f(p), 1 - f(p)\right] \geq \min(p^n, 1-p^n)$

<u>Lemma</u>: Given f as in Thm, there is a function g implementable by a finite factory s.t.

$$0 \leq f(p) - \frac{1}{4} g(p) \leq \frac{3}{4}$$

s.t. $\frac{4}{3}\left(f(p) - \frac{1}{4} g(p)\right)$ is poly-bounded.

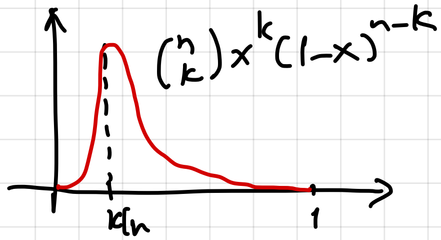
Lemma (Proof by picture)

Alternative Proof (Nacu-Peres)

① Bernstein approximation: given continuous function $f:[0,1]\to\mathbb{R}$

define $Q_n[f](x) = \sum_{k=0}^{n} f\left(\frac{k}{n}\right)\binom{n}{k} x^k (1-x)^{n-k}$

then: $Q_n[f](x) \to f(x)$ uniformly.



② Polya's Thm: If $q(x,y)$ is a real homogeneous polynomial such that $q(x,y)>0$ $\forall x,y>0$ then $\exists n$ s.t. all coefficients of $(x+y)^n q(x,y)$ are non-negative.

Idea: If $f:(0,1)\to[\varepsilon,1-\varepsilon]$ use ① to construct approximators and ② to stitch the functions together in a series.

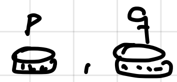
Fast Simulation

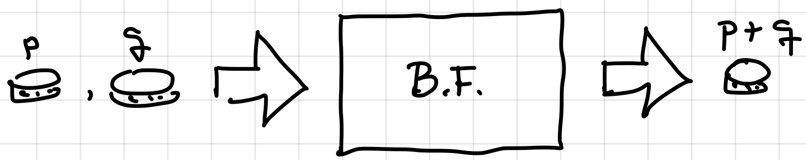
(Mossel-Peres 2002)
(Nacu-Peres 2005)

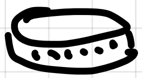
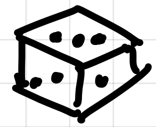
N = # coins tossed until output (random variable)

Property of f		Property of N	
continuous	$\Leftrightarrow$	$N < \infty$ a.s.	(i.e. it terminates)
real-analytic	$\Leftrightarrow$	$\mathbb{P}(N \leq n) \leq O(\rho^n)$	exponential tail. $\rho = \rho(p) < 1$.
Lipschitz	$\Leftarrow$	$\mathbb{E}[N] < \infty$	
rational	$\Leftrightarrow$	N via finite automata	

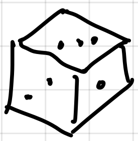
Problem: Sum of Two Coins

Given two coins  with the promise that $p+q \le 1-\varepsilon$, sample from a $(p+q)$-biased coin.



Coins  to Dice 

(Mossel - Peres 2002)
(Dughmi et al 2017)
(Morina et al 2020)

 $\longrightarrow$ 

p_1 , p_2 , ... p_n

$$X = \begin{cases} 1 & \text{w.p. } p_1 \\ 2 & \text{w.p. } p_2 \\ \dots & \\ n & \text{w.p. } p_n \end{cases}$$

(Bernoulli Race).

Rational Functions

Factory for $f(p) = \dfrac{\sum_{i=0}^{k} a_i p^i}{\sum_{i=0}^{k} b_i p^i}$ $\quad f: (0,1) \to (0,1).$

① Bernoulli race between two coins  and 

Rational Functions

Factory for $f(p) = \dfrac{\sum_{i=0}^{k} a_i p^i}{\sum_{i=0}^{k} b_i p^i}$ $f: (0,1) \to (0,1)$.

② Polya's Thm: If $q(x,y)$ is a real homogeneous polynomial such that $q(x,y) > 0 \;\; \forall x,y > 0$ then $\exists n$ s.t all coefficients of $(x+y)^n q(x,y)$ are non-negative.

$a(x) = \sum_i a_i x^i$ $A(x,y) =$

$b(x) = \sum_i b_i x^i$ $B(x,y) =$

Rational Functions

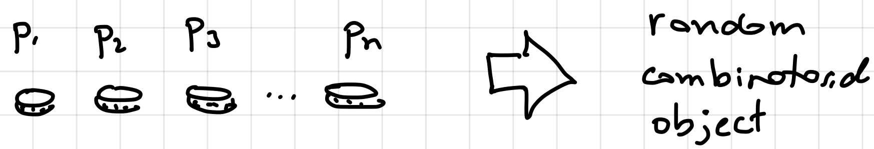
rational.

$$\mathbb{P}(X = i) = \frac{f_i(x_1 \ldots x_n)}{g_i(x_1 \ldots x_n)}$$

Polya's Thm: If $g(x_1 \ldots x_m)$ is a real homogeneous polynomial such that $g(x_1 \ldots x_m) > 0$ for $x_i > 0 \ \forall i$ then $\exists n$ s.t. all coefficients of $(x_1 + \cdots + x_m)^n g(x_1 \ldots x_m)$ are positive.

Part II: Combinatorial Factories

(Niazadeh, PL, Schneider 2021)



Random Combinatorial Objects

(1) k- Subset

(2) Matchings

Random Combinatorial Objects

(3) spanning-trees

(4) s-t-flows

Random Combinatorial Objects

(*) Vertices of a polytope

Polytope P contained in $[0,1]^n$

V = vertices of P

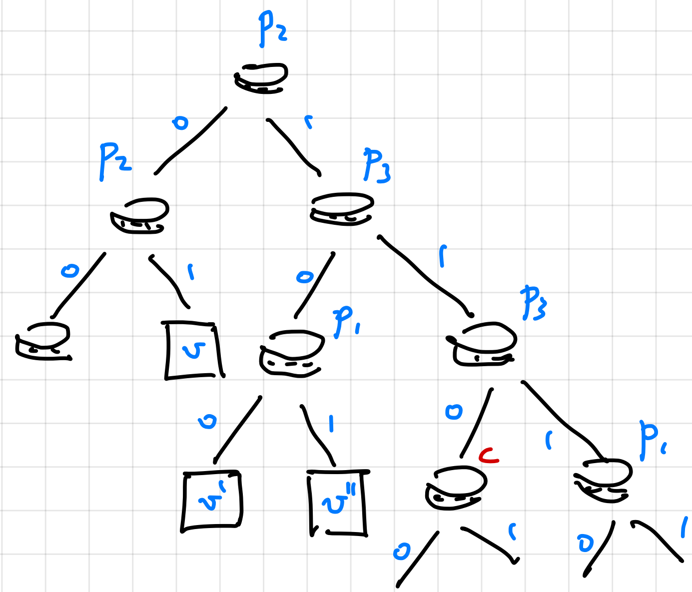
Given coins $p_1 \dots p_n$ s.t. $p = (p_1 \cdots p_n) \in P \cap (0,1)^n$

output a vertex $v \in V$ s.t. $\mathbb{E}[v] = p$.

General Bernoulli Factory

Output set : V

Input coins: p_1 p_2 ... p_3



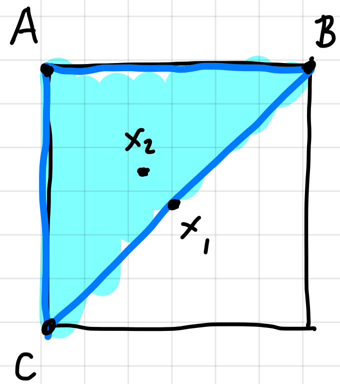
Nodes:

p_i - coin p_i

helper coin c (constant c)

output node $\boxed{v}$ ($v \in V$)

Necessary Conditions

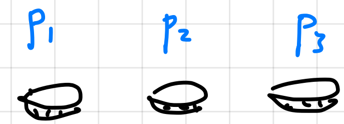


Output at x_1 :

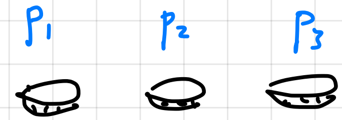
Output at x_2 :

Factory for k-Subset

Natural Algorithms:



Factory for k-Subset



Sampford Sampling

$$\mathbb{P}[\text{sample } S] = \prod_{i \in S} p_i \prod_{i \notin S} (1-p_i) \cdot$$

<u>Algorithm</u>

Flip each coin X_i

$S = \{i ; X_i = 1\}$

if $|S| \neq k$ restart

output S

A Guess

For every polytope $P = \{x \in [0,1]^n ;\ Ax = b\}$ we can find polynomials $f_v(p_1 \cdots p_n)$ such that:

(1) $\sum_{v \in V} f_v(p_1 \cdots p_n) \cdot (p - v) = 0 \quad \forall p \in P.$

(2) $f_v(p_1 \cdots p_n)$ are implementable by a Bernoulli factory

$$f_v(p) =$$

Solve a Program

$$f_v(p) =$$

$$\sum_v f_v(p) \cdot (p - v) = 0 \quad \forall p ; Ap = b$$

sage

(Manipulate polynomials)

SciPy

(Solve linear programs)

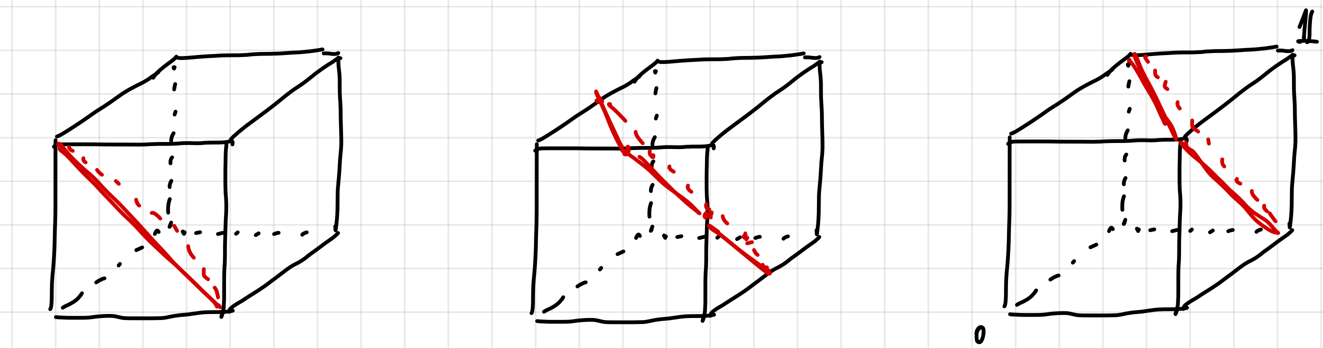
Next Simplest Example

Towards co-dimension 1: $P = \{ x \in [0,1]^n ; \; a^T x = b \}$.

Simplest case we didn't understand: $\sum_i x_i = \alpha \qquad \alpha \notin \mathbb{Z}$.

Example: $n = 3 \qquad \alpha = 1.5$

What are the vertices?



$\alpha = 1$	$\alpha = 1.5$	$\alpha = 2$
$\lvert V \rvert = 3$	$\lvert V \rvert = 6$	$\lvert V \rvert = 3$
permutations of $(1,0,0)$	permutations of $(1, \frac{1}{2}, 0)$	permutations of $(1,1,0)$

Next Simplest Example

Towards co-dimension 1: $\quad P = \{ x \in [0,1]^n ; \; a^T x = b \}$.

Simplest case we didn't understand: $\sum_i x_i = \alpha \qquad \alpha \notin \mathbb{Z}$.

In general: $\quad n \,, \quad \alpha = k - \varepsilon \qquad 0 < \varepsilon < 1$

$$V = \text{permutations of } (\underbrace{1, 1, \dots, 1}_{k-1}, 1-\varepsilon, \underbrace{0, \dots, 0}_{n-k})$$

Start with $n = 3 \quad k = 1 + \varepsilon$ (simplest unknown example).

If polynomials exist we should be able to find it. After staring at the solutions for very long:

$$f_v(P) =$$

Co-dimension One

$P = \{x \in [0,1]^n ;\ a^T x = b\}.$

Generic hyperplane $\Longrightarrow$ Each vertex has one special index.
avoiding $\{0,1\}^n$

$v_i \in (0,1)$ $\qquad f_v(p) = |a_i| \cdot p_i (1-p_i) \prod_{j : v_j = 1} p_j \prod_{j : v_j = 0} (1-p_j)$

Non-generic hyperplanes:

Any dimension

Factory for Matching

Application to Mechanism Design

Some Open Problems