Computing with Coins

On randomness and determinism

Polaris Team
Jean-Marc.Vincent@imag.fr

November 2018

COMPUTING WITH COINS

1 A SIMPLE RANDOM GAME : Head or Tail

2 NUMERICAL COMPUTATION : Π

3 DOBBLE : INTERSECTING SUBSETS FAMILIES

4 ZKIP : Sudoku

5 LIKE OR UNLIKE

WHO SHOULD SET THE TABLE ?

Fair decision

WHO SHOULD SET THE TABLE ?

Fair decision

WHO SHOULD SET THE TABLE ?

Fair decision ?

WHO SHOULD SET THE TABLE ?

Fair decision ?

Simulate a *fair coin* with an unfair one

WHO SHOULD SET THE TABLE ?

Fair decision ?

Simulate a *fair coin* with an unfair one

Tail

Head

WHO SHOULD SET THE TABLE ?

Fair decision ?

Simulate a *fair coin* with an unfair one

Tail

Head

Hint : Flip the coin many times

UNFAIR COIN

Flip the coin two times 2

UNFAIR COIN

Flip the coin two times 2

$\Rightarrow$ **Flip again**

UNFAIR COIN

Flip the coin two times 2

⇒ Flip again

⇒ Flip again

UNFAIR COIN

Flip the coin two times 2

⇒ Flip again

⇒ Flip again

⇒ Return Tail

UNFAIR COIN

Flip the coin two times 2

⇒ Flip again

⇒ Flip again

⇒ Return Tail

⇒ Return Head

REFERENCES

Guess Who ?

in testing for either even or odd. To cite a human example, for simplicity, in tossing a coin it is probably easier to make two consecutive tosses independent than to toss heads with probability exactly one-half. If independence of successive tosses is assumed, we can reconstruct a 50–50 chance out of even a badly biased coin by tossing twice. If we get heads-heads or tails-tails, we reject the tosses and try again. If we get heads-tails (or tails-heads), we accept the result as heads (or tails). The resulting process is rigorously unbiased, although the amended process is at most 25 percent as efficient as ordinary coin-tossing.

REFERENCES

Guess Who ?

in testing for either even or odd. To cite a human example, for simplicity, in tossing a coin it is probably easier to make two consecutive tosses independent than to toss heads with probability exactly one-half. If independence of successive tosses is assumed, we can reconstruct a 50–50 chance out of even a badly biased coin by tossing twice. If we get heads-heads or tails-tails, we reject the tosses and try again. If we get heads-tails (or tails-heads), we accept the result as heads (or tails). The resulting process is rigorously unbiased, although the amended process is at most 25 percent as efficient as ordinary coin-tossing.

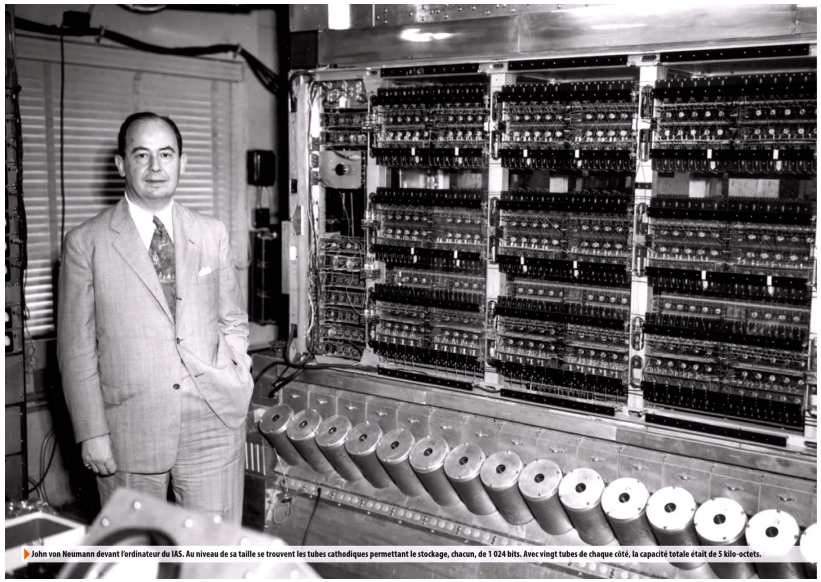
Various Techniques Used in Connection With Random Digits

By John von Neumann

Summary written by George E. Forsythe

J. Res. Nat. Bur. Stand. Appl. Math. Series 3, 36-38 (1951)

Biography



John von Neumann devant l'ordinateur du IAS. Au niveau de sa taille se trouvent les tubes cathodiques permettant le stockage, chacun, de 1 024 bits. Avec vingt tubes de chaque côté, la capacité totale était de 5 kilo-octets.

- Middle square generator
- Rejection Method (1947)
-

COMPUTING WITH COINS

1 A SIMPLE RANDOM GAME : Head or Tail

2 NUMERICAL COMPUTATION : Π

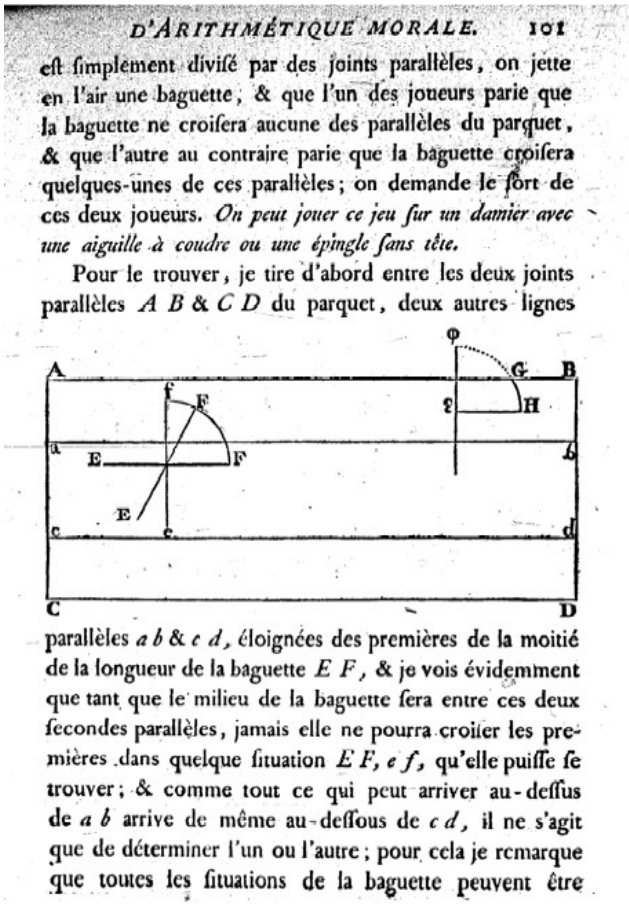
3 DOBBLE : INTERSECTING SUBSETS FAMILIES

4 ZKIP : Sudoku

5 LIKE OR UNLIKE

RANDOMIZED ALGORITHMS

Needle on the floor



D'ARITHMÉTIQUE MORALE. 101

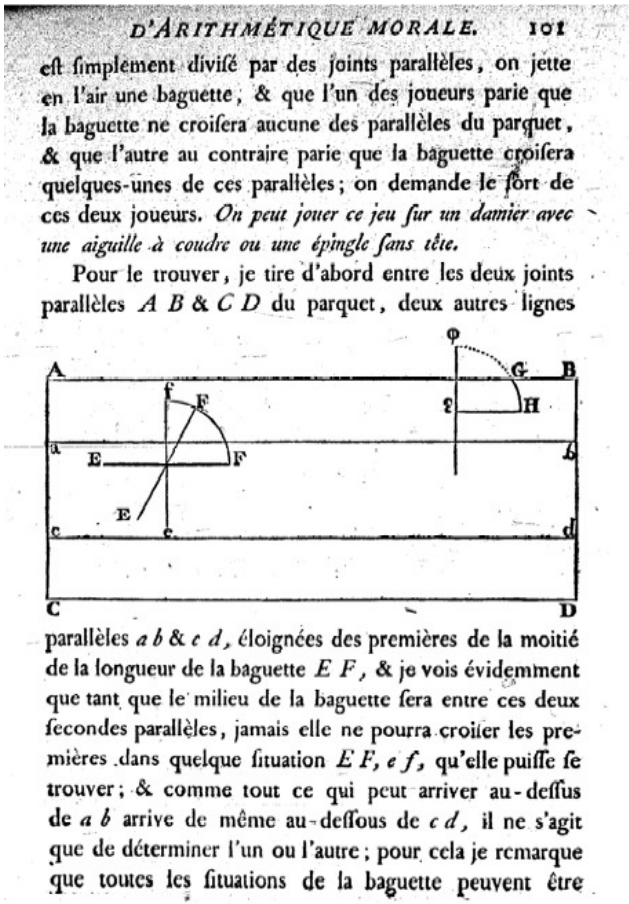
eſt ſimplement diviſé par des joints parallèles, on jette en l'air une baguette, & que l'un des joueurs parie que la baguette ne croiſera aucune des parallèles du parquet, & que l'autre au contraire parie que la baguette croiſera quelques-unes de ces parallèles; on demande le ſort de ces deux joueurs. *On peut jouer ce jeu ſur un damier avec une aiguille à coudre ou une épingle ſans tête.*

Pour le trouver, je tire d'abord entre les deux joints parallèles *A B* & *C D* du parquet, deux autres lignes

parallèles *a b* & *c d*, éloignées des premières de la moitié de la longueur de la baguette *E F*, & je vois évidemment que tant que le milieu de la baguette ſera entre ces deux ſecondes parallèles, jamais elle ne pourra croiſer les premières dans quelque ſituation *E F*, *e f*, qu'elle puiſſe ſe trouver; & comme tout ce qui peut arriver au-deſſus de *a b* arrive de même au-deſſous de *c d*, il ne s'agit que de déterminer l'un ou l'autre; pour cela je remarque que toutes les ſituations de la baguette peuvent être

RANDOMIZED ALGORITHMS

Needle on the floor



D'ARITHMÉTIQUE MORALE. 101

est simplement divisé par des joints parallèles, on jette en l'air une baguette, & que l'un des joueurs parie que la baguette ne croisera aucune des parallèles du parquet, & que l'autre au contraire parie que la baguette croisera quelques-unes de ces parallèles; on demande le sort de ces deux joueurs. *On peut jouer ce jeu sur un damier avec une aiguille à coudre ou une épingle sans tête.*

Pour le trouver, je tire d'abord entre les deux joints parallèles *A B* & *C D* du parquet, deux autres lignes

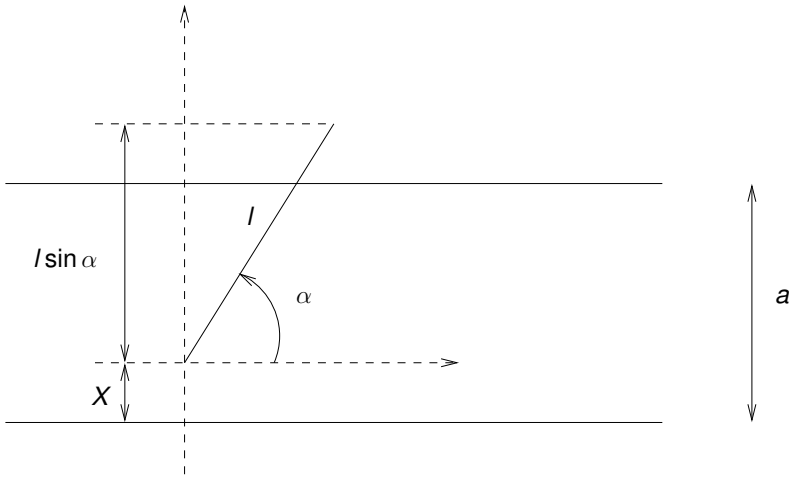
parallèles *a b* & *c d*, éloignées des premières de la moitié de la longueur de la baguette *E F*, & je vois évidemment que tant que le milieu de la baguette sera entre ces deux secondes parallèles, jamais elle ne pourra croiser les premières dans quelque situation *E F*, *e f*, qu'elle puisse se trouver; & comme tout ce qui peut arriver au-dessus de *a b* arrive de même au-dessous de *c d*, il ne s'agit que de déterminer l'un ou l'autre; pour cela je remarque que toutes les situations de la baguette peuvent être

Buffon (1707-1788) - biography

Georges-Louis Leclerc, comte de Buffon (7 septembre 1707 à Montbard - 16 avril 1788 à Paris), est un naturaliste, mathématicien, biologiste, cosmologiste et écrivain français. Ses théories ont influencé deux générations de naturalistes, parmi lesquels notamment Jean-Baptiste de Lamarck et Charles Darwin. La localité éponyme Buffon, dans la Côte-d'Or, fut la seigneurie de la famille Leclerc.
Les premiers travaux de Buffon ont été consacrés aux mathématiques. Il faut surtout signaler le Mémoire sur le jeu de franc carreau, qui présente l'originalité de faire intervenir le calcul infinitésimal dans le calcul des probabilités. Par la suite, Buffon utilisera les mathématiques dans ses recherches sur la résistance du bois et sur le refroidissement des planètes, ainsi que dans son Essai d'arithmétique morale (Supplément, t. IV, 1777), mais ces travaux montrent que, pour lui, les mathématiques ne sont qu'un moyen de préciser l'idée qu'il peut avoir des choses, et non une discipline autonome. Il est ingénieur plus que mathématicien. Par contre, il est philosophe de tempérament. Le tome I de l'Histoire naturelle (1749) s'ouvre par un discours De la manière d'étudier et de traiter l'histoire naturelle, qui est une réflexion sur la valeur de la connaissance humaine. Rompant à la fois avec l'idéalisme rationaliste et l'empirisme sceptique, Buffon affirme la validité d'une science fondée sur les faits, mais sachant en dégager les lois, débarassée de toute téléologie, d'une science qui sans doute ne vaut que pour l'homme, mais qui est la seule que l'homme puisse atteindre. Par la suite, Buffon admettra que l'homme peut découvrir les vraies lois de la nature (De la nature, 1re et 2e vues, Histoire naturelle, t. XII et XIII, 1764-1765). Son tempérament rationaliste l'emporte alors sur sa formation philosophique, d'inspiration sceptique.

MODELIZATION

Notations



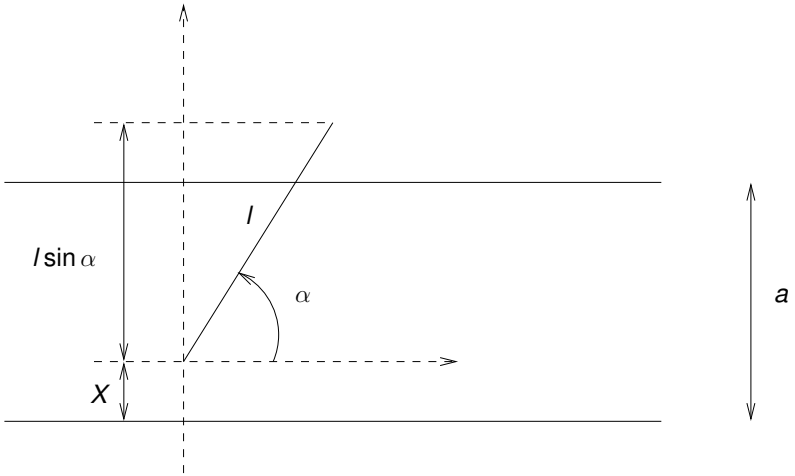
X uniformly distributed on $[0, a]$

α uniformly distributed on $[0, \pi]$

Compute $\mathbb{P}(X + l \sin \alpha \geqslant a)$

MODELIZATION

Notations

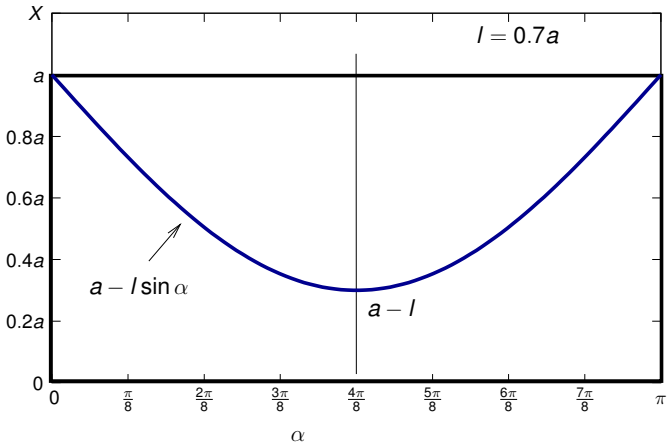


X uniformly distributed on $[0, a]$

α uniformly distributed on $[0, \pi]$

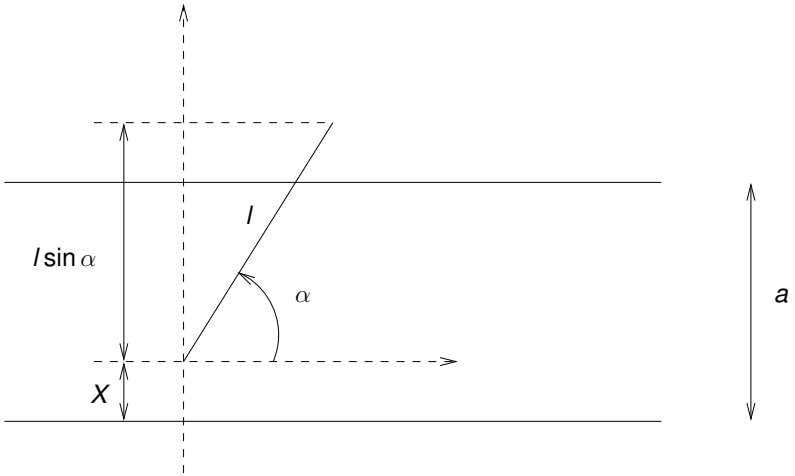
Compute $\mathbb{P}(X + l \sin\alpha \geqslant a)$

Area representation



MODELIZATION

Notations

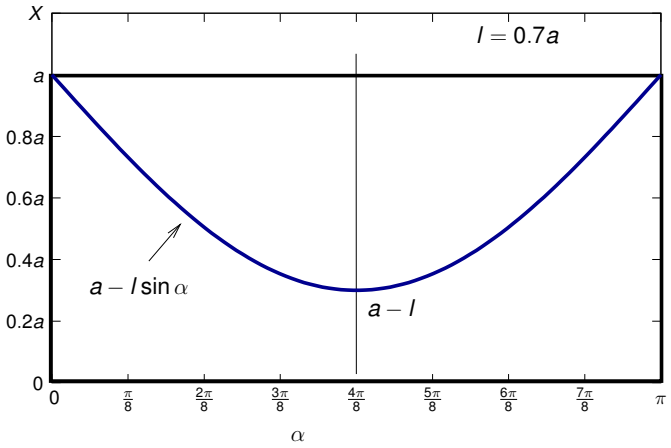


X uniformly distributed on $[0, a]$

α uniformly distributed on $[0, \pi]$

Compute $\mathbb{P}(X + l \sin\alpha \geqslant a)$

Area representation

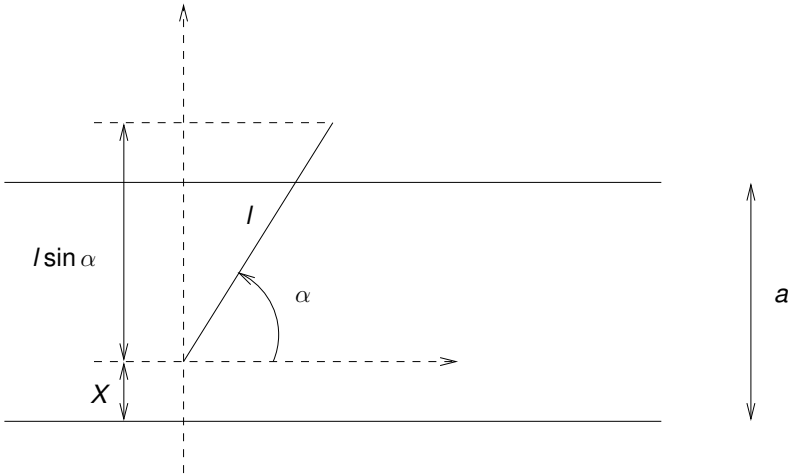


Computation

$$
\begin{aligned}
\mathbb{P}(X + l\sin\alpha \geqslant a) &= 1 - \mathbb{P}(X + l\sin\alpha \leqslant a);\\
&= 1 - \mathbb{P}(X \leqslant a - l\sin\alpha);\\
&= 1 - \frac{\text{Surface under the blue curve}}{\text{Surface of the rectangle}};\\
&= 1 - \frac{1}{\pi a}\int_0^{\pi} (a - l\sin\alpha)d\alpha;\\
&= 1 - \frac{1}{\pi a}\left[a.\alpha + l\cos\alpha\right]_0^{\pi} = \frac{2l}{\pi a}.
\end{aligned}
$$

MODELIZATION

Notations

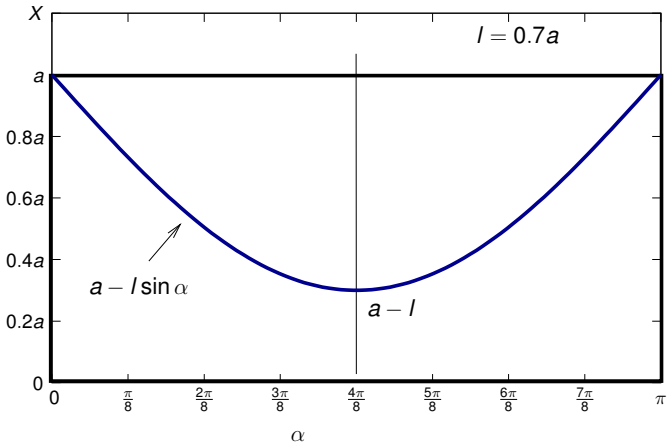


X uniformly distributed on $[0, a]$

α uniformly distributed on $[0, \pi]$

Compute $\mathbb{P}(X + l \sin\alpha \geqslant a)$

Area representation



Computation

$$\begin{aligned}
\mathbb{P}(X + l\sin\alpha \geqslant a) &= 1 - \mathbb{P}(X + l\sin\alpha \leqslant a);\\
&= 1 - \mathbb{P}(X \leqslant a - l\sin\alpha);\\
&= 1 - \frac{\text{Surface under the blue curve}}{\text{Surface of the rectangle}};\\
&= 1 - \frac{1}{\pi a}\int_0^{\pi}(a - l\sin\alpha)d\alpha;\\
&= 1 - \frac{1}{\pi a}[a.\alpha + l\cos\alpha]_0^{\pi} = \frac{2l}{\pi a}.
\end{aligned}$$

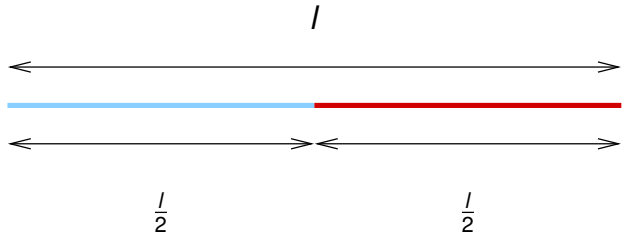
Result

The hitting probability :

$$\mathbb{P}(X + l\sin\alpha \geqslant a) = \frac{2l}{\pi a}.$$

PROBABILISTIC THINKING

- Change the problem : compute N the number of intersections between the needle and the lines ; we will compute $\mathbb{E}N$.
- Consider a needle, paint one half in **b**lue the other half in **r**ed. Then $N = N_b + N_r$ and



$$\begin{aligned} f(l) &= \mathbb{E}N = \mathbb{E}N_b + \mathbb{E}N_r \text{ linearity of expectation} \\ &= f\left(\frac{l}{2}\right) + f\left(\frac{l}{2}\right) \\ &\quad \text{because } \mathbb{E}N_r \text{ corresponds to throwing a needle of size } \frac{l}{2} \text{ (forget the blue part)} \\ &= 2f\left(\frac{l}{2}\right) \end{aligned}$$

- Generalize to any rational $\frac{p}{q}$

$$f\left(\frac{p}{q}\right) = \frac{p}{q} f(1)$$

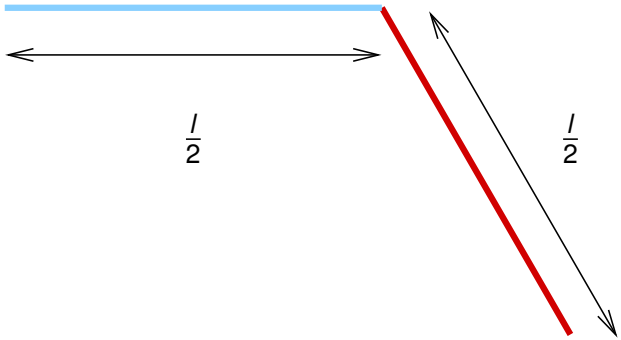
- use a continuity argument to conclude that

  $f(x) = xf(1)$

  and f is linear, its coefficient is $f(1)$

PROBABILISTIC THINKING (2)

- Change the problem : consider a twisted needle and compute N the number of intersections between the needle and the lines.



- Compute $\mathbb{E}N$

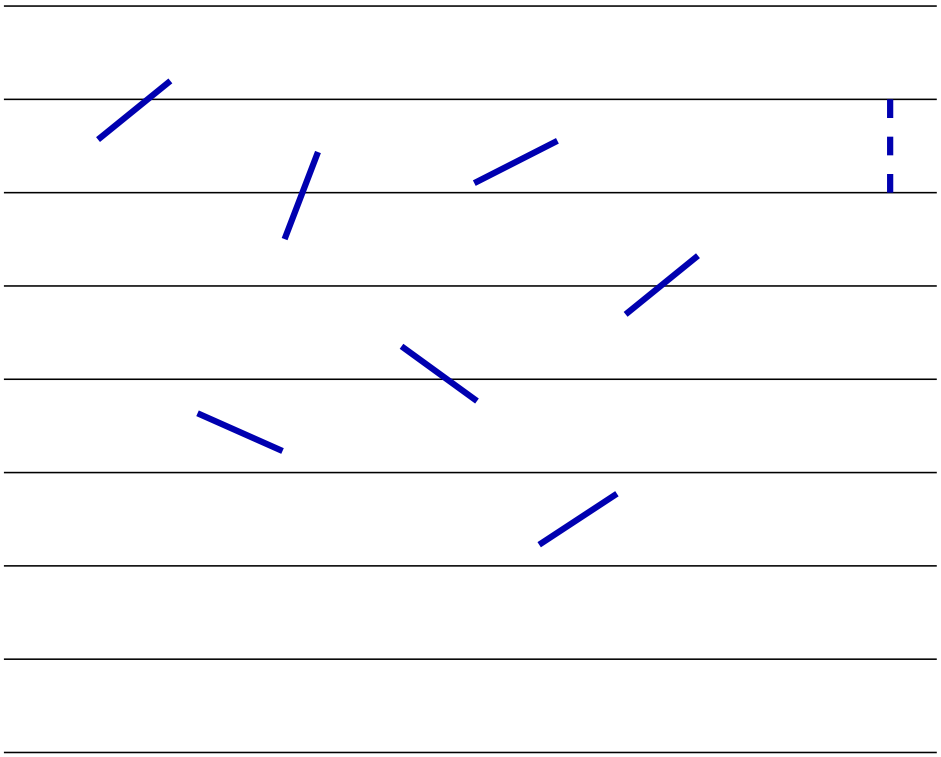
$$\begin{aligned}\mathbb{E}N &= \mathbb{E}N_b + \mathbb{E}N_r \text{ linearity of expectation} \\ &= f\left(\frac{l}{2}\right) + f\left(\frac{l}{2}\right) \\ &= 2f\left(\frac{l}{2}\right)\end{aligned}$$

- Use the same argument as before to have the same relation for any sequence of segments, then for any curve that could be approximated by segments (rectifiable)

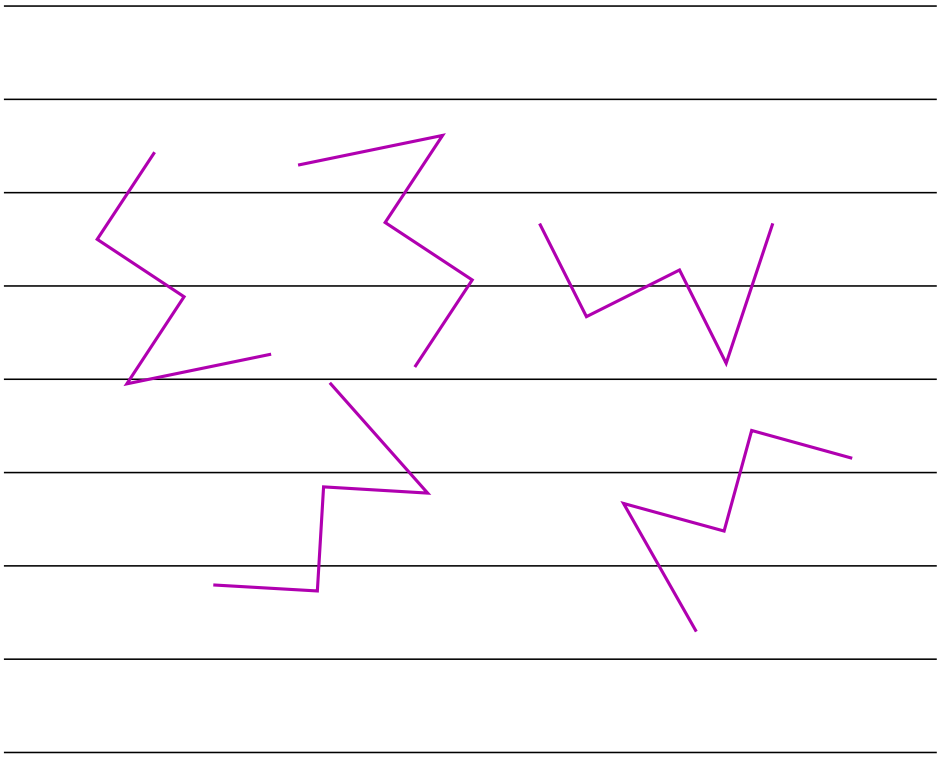
  The expected number of intersection points of the curve with the lines is linear in the length of the curve

PROBABILISTIC THINKING (3)

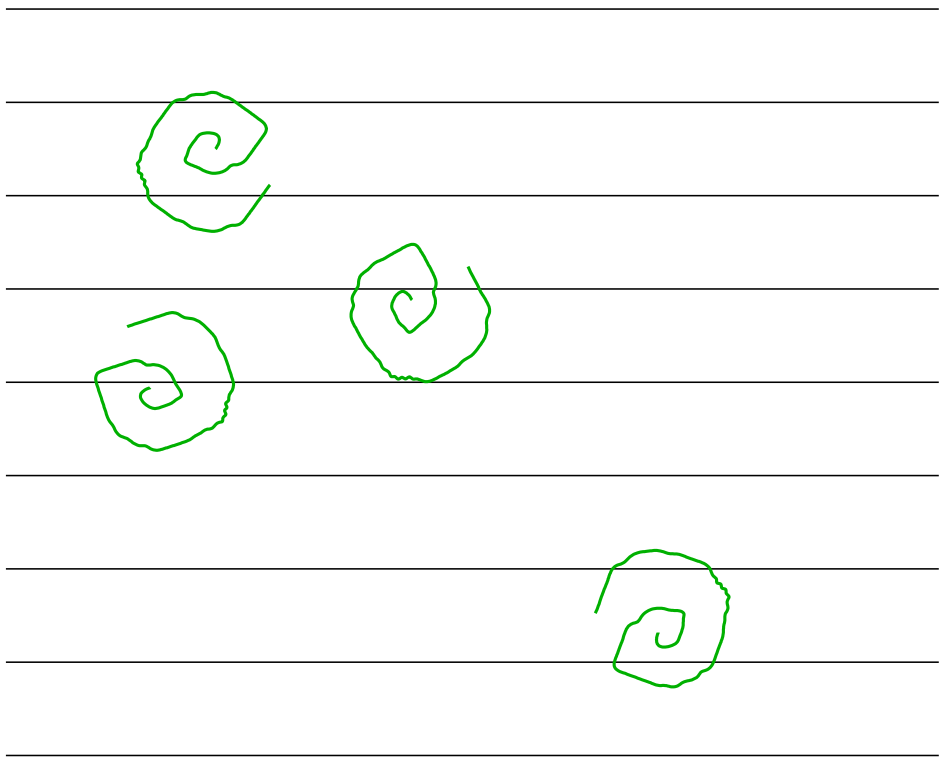
PROBABILISTIC THINKING (3)



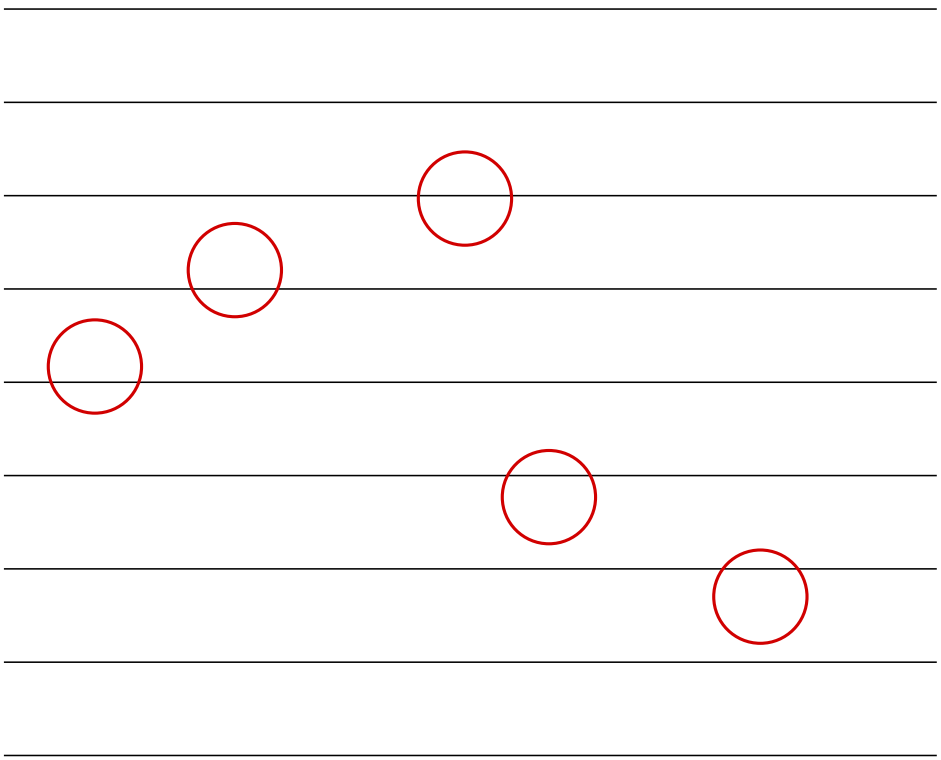
PROBABILISTIC THINKING (3)



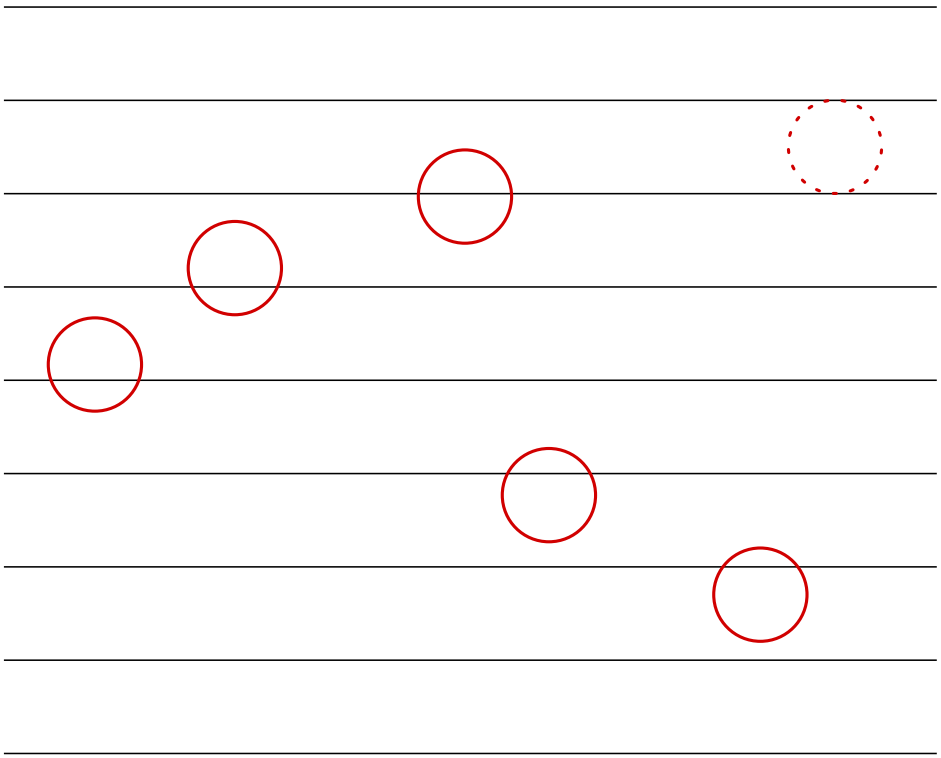
PROBABILISTIC THINKING (3)



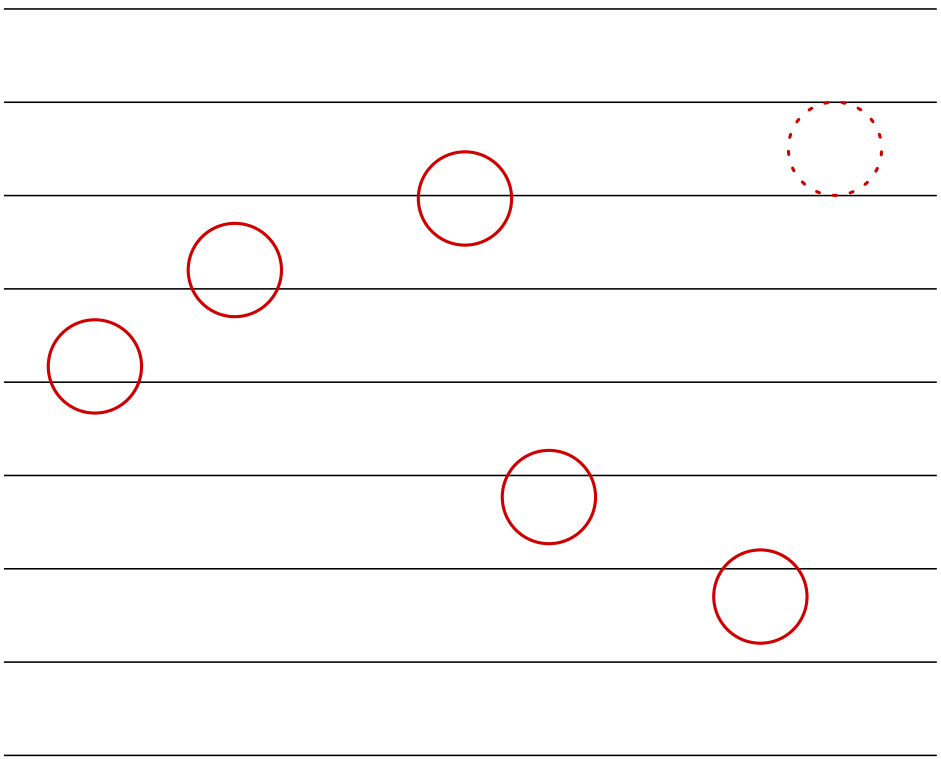
PROBABILISTIC THINKING (3)



PROBABILISTIC THINKING (3)



PROBABILISTIC THINKING (3)



For a circle with diameter a, length is πa

$$\mathbb{E}N = 2 \text{ and } f(1) = \frac{2}{\pi a}$$

Finally for the needle with length l on interspaced lines a : $\mathbb{E}N = \mathbb{P}(\text{ Hit }) = \frac{2l}{\pi a}$.

COMPUTING WITH COINS

1 A SIMPLE RANDOM GAME : Head or Tail

2 NUMERICAL COMPUTATION : Π

3 DOBBLE : INTERSECTING SUBSETS FAMILIES

4 ZKIP : Sudoku

5 LIKE OR UNLIKE

THE DOBBLE GAME

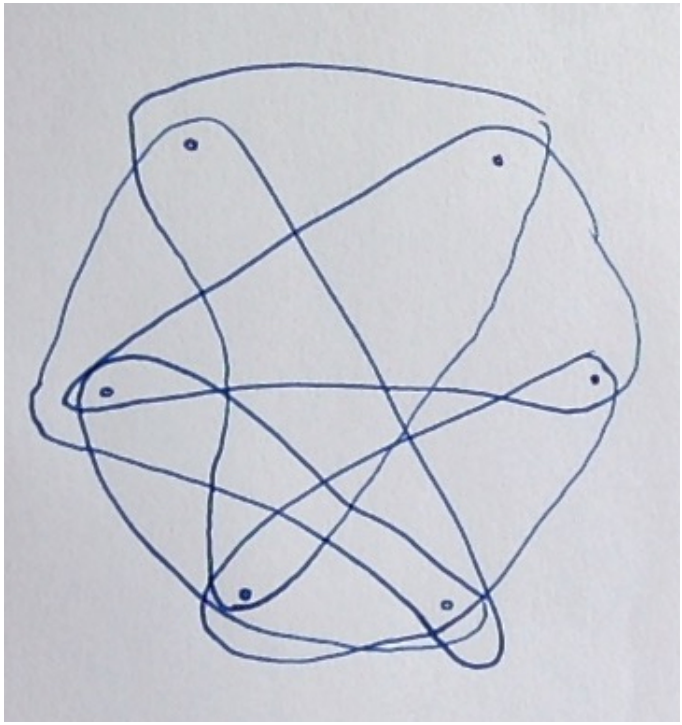
Only one symbol in common between two cards.

INTERSECTING SUBSETS

Let $\mathcal{F}$ be a family of intersecting subsets of $\{0, 1, 2, \cdots, n-1\}$ of size k with $k \leqslant \frac{n}{2}$

$$A, B \in \mathcal{F} \Rightarrow A \cap B \neq \emptyset$$

with $n = 6$ and $k = 3$



a trivial lower bound $\geqslant \binom{n-1}{k-1}$

INTERSECTING SUBSETS

Let $\mathcal{F}$ be a family of intersecting subsets of $\{0, 1, 2, \cdots, n-1\}$ of size k with $k \leqslant \frac{n}{2}$

$A, B \in \mathcal{F} \Rightarrow A \cap B \neq \emptyset$ **What could be the maximal size of $\mathcal{F}$?**

INTERSECTING SUBSETS

Let $\mathcal{F}$ be a family of intersecting subsets of $\{0, 1, 2, \cdots, n-1\}$ of size k with $k \leqslant \frac{n}{2}$

$A, B \in \mathcal{F} \Rightarrow A \cap B \neq \emptyset$ **What could be the maximal size of $\mathcal{F}$?**

Erdös-Ko-Rado Theorem (1938)

$$|\mathcal{F}| \leqslant \binom{n-1}{k-1}$$

INTERSECTING SUBSETS

Let $\mathcal{F}$ be a family of intersecting subsets of $\{0, 1, 2, \cdots, n-1\}$ of size k with $k \leqslant \frac{n}{2}$

$A, B \in \mathcal{F} \Rightarrow A \cap B \neq \emptyset$ **What could be the maximal size of $\mathcal{F}$?**

Erdös-Ko-Rado Theorem (1938)

$$|\mathcal{F}| \leqslant \binom{n-1}{k-1}$$

Idea : preliminary lemma

For $0 \leqslant s \leqslant n-1$,
$A_s = \{s, s+1, \cdots, s+k-1\} \pmod{n}$,

then $\mathcal{F}$ can contain at most k of the sets A_s.

INTERSECTING SUBSETS

Let $\mathcal{F}$ be a family of intersecting subsets of $\{0, 1, 2, \cdots, n-1\}$ of size k with $k \leqslant \frac{n}{2}$

$A, B \in \mathcal{F} \Rightarrow A \cap B \neq \emptyset$ **What could be the maximal size of $\mathcal{F}$?**

Erdös-Ko-Rado Theorem (1938)

$$|\mathcal{F}| \leqslant \binom{n-1}{k-1}$$

Idea : preliminary lemma

For $0 \leqslant s \leqslant n-1$,
$A_s = \{s, s+1, \cdots, s+k-1\} \pmod{n}$,

then $\mathcal{F}$ can contain at most k of the sets A_s.

Proof If $A_s \in \mathcal{F}$ intersecting sets with A_s can be partitioned into $k-1$ disjoints pairs (A_{s-i}, A_{s+k-i}) and $\mathcal{F}$ can contain at most one member of each pair.

INTERSECTING SUBSETS

Let $\mathcal{F}$ be a family of intersecting subsets of $\{0, 1, 2, \cdots, n-1\}$ of size k with $k \leqslant \frac{n}{2}$

$A, B \in \mathcal{F} \Rightarrow A \cap B \neq \emptyset$ **What could be the maximal size of $\mathcal{F}$?**

Erdös-Ko-Rado Theorem (1938)

$$|\mathcal{F}| \leqslant \binom{n-1}{k-1}$$

Idea : preliminary lemma

For $0 \leqslant s \leqslant n-1$,
$A_s = \{s, s+1, \cdots, s+k-1\} \pmod{n}$,

then $\mathcal{F}$ can contain at most k of the sets A

Proof If $A_s \in \mathcal{F}$ intersecting sets with A_s can be partitioned into $k-1$ disjoints pairs (A_{s-i}, A_{s+k-i}) and $\mathcal{F}$ can contain at most one member of each pair.

Probabilistic Thinking

Consider a uniformly generated random permutation σ and an index i uniformly generated on $\{0, 1, \cdots, n-1\}$

$$A = \{\sigma(i), \sigma(i+1), \sigma(i+k-1)\}$$

conditioned by σ at most k elements of this form belong to $\mathcal{F}$ then

$$\mathbb{P}(A \in \mathcal{F}|\sigma) \leqslant \frac{k}{n} \text{ and } \mathbb{P}(A \in \mathcal{F}) \leqslant \frac{k}{n}.$$

But A is uniformly generated on the k-sets then

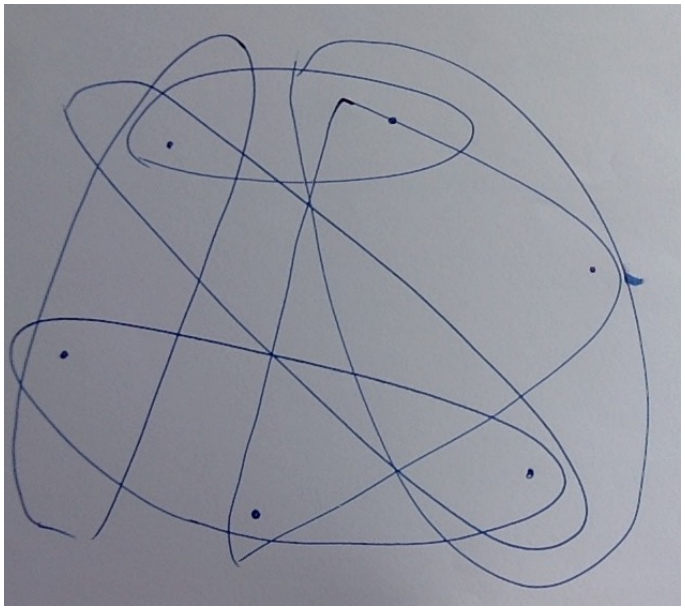
$$\mathbb{P}(A \in \mathcal{F}) = \frac{|\mathcal{F}|}{\binom{n}{k}} \; ; \; |\mathcal{F}| \leqslant \frac{k}{n}.\binom{n}{k} = \binom{n-1}{k-1}$$

[The Probabilistic Method *N. Alon and J.H. Spencer* Wiley 2016]

SPERNER'S FAMILY

A family $\mathcal{S}$ of subsets of $\{1, \cdots, n\}$ is a Sperner's family iff

$$A, B \in \mathcal{S} \Rightarrow A \not\subset B \text{ and } B \not\subset A$$



maximal size of a Sperner's family lower bounded by

$$\binom{n}{\lfloor \frac{n}{2} \rfloor}$$

SPERNER'S FAMILY (2)

A family $\mathcal{S}$ of subsets of $\{1, \cdots, n\}$ is a Sperner's family iff

$$A, B \in \mathcal{S} \Rightarrow A \not\subset B \text{ and } B \not\subset A$$

Theorem

$$\sum_{A \in \mathcal{S}} \frac{1}{\binom{n}{|A|}} \leqslant 1$$

$$|\mathcal{S}| \leqslant \binom{n}{\left[\frac{n}{2}\right]} \text{ Sperner's Theorem (1928)}$$

Idea : chains of subsets

Consider a uniformly generated random permutation σ and an index i uniformly generated on $\{1, \cdots, n\}$

$$C_\sigma = \{\{\sigma(j) : 1 \leqslant j \leqslant i\} : 0 \leqslant i \leqslant n\}$$

Example $\sigma = (3, 2, 5, 1, 4)$

$$C_\sigma = \{\emptyset, \{3\}, \{3, 2\}, \{3, 2, 5\}, \{3, 2, 5, 1\}, \{3, 2, 5, 1, 4\}\}.$$

SPERNER'S FAMILY (2)

A family $\mathcal{S}$ of subsets of $\{1, \cdots, n\}$ is a Sperner's family iff

$$A, B \in \mathcal{S} \Rightarrow A \not\subset B \text{ and } B \not\subset A$$

Theorem

$$\sum_{A \in \mathcal{S}} \frac{1}{\binom{n}{|A|}} \leqslant 1$$

$$|\mathcal{S}| \leqslant \binom{n}{\left[\frac{n}{2}\right]} \text{ Sperner's Theorem (1928)}$$

Idea : chains of subsets

Consider a uniformly generated random permutation σ and an index i uniformly generated on $\{1, \cdots, n\}$

$$C_\sigma = \{\{\sigma(j) : 1 \leqslant j \leqslant i\} : 0 \leqslant i \leqslant n\}$$

Example $\sigma = (3, 2, 5, 1, 4)$

$$C_\sigma = \{\emptyset, \{3\}, \{3, 2\}, \{3, 2, 5\}, \{3, 2, 5, 1\}, \{3, 2, 5, 1$$

Probabilistic Thinking

$$X = |\mathcal{S} \cap C_\sigma| = \sum_{A \in \mathcal{S}} \mathbb{1}_{A \in C_\sigma}$$

$$\mathbb{E}\mathbb{1}_{A \in C_\sigma} = \mathbb{P}(A \in C_\sigma) = \frac{1}{\binom{n}{|A|}}$$

by linearity of expectation

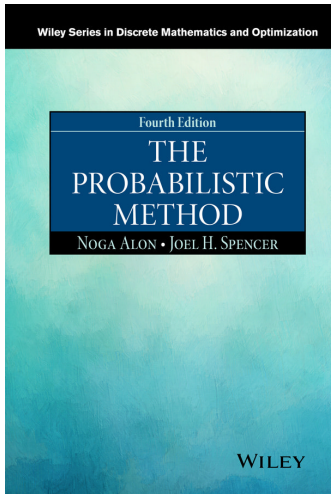
$$1 \geqslant \mathbb{E}X = \sum_{A \in \mathcal{S}} \frac{1}{\binom{n}{|A|}}.$$

but $\binom{n}{|A|} \leqslant \binom{n}{\left[\frac{n}{2}\right]}$ consequently

$$1 \geqslant \sum_{A \in \mathcal{S}} \frac{1}{\binom{n}{|A|}} \geqslant \frac{|\mathcal{S}|}{\binom{n}{\left[\frac{n}{2}\right]}}.$$

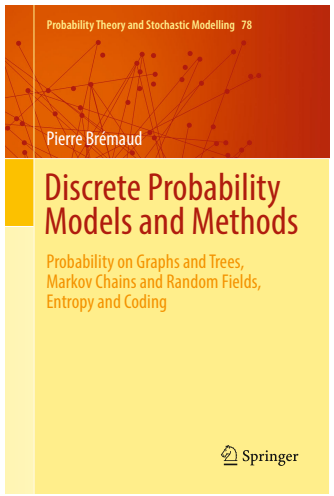
REFERENCES

The reference



Fourth edition, July 2015

A Reference for Probability (discrete)



Edition, 2017

COMPUTING WITH COINS

1 A SIMPLE RANDOM GAME : Head or Tail

2 NUMERICAL COMPUTATION : Π

3 DOBBLE : INTERSECTING SUBSETS FAMILIES

4 **ZKIP : Sudoku**

5 LIKE OR UNLIKE

	2						9	
3		1	9		6	5		2
			8		4			
	9						5	
5			2		3			6
	7						2	
			4		7			
8		2	5		1	7		3
	5						8	

	2						9	
3		1	9		6	5		2
			8		4			
	9						5	
5			2		3			6
	7						2	
			4		7			
8		2	5		1	7		3
	5						8	

Bob : This Sudoko has no solution ! I spent hours on it, that's impossible !

Alice : You're a stupid donkey ! I got the solution since 2 days !

Bob : I can't believe it ! You're cheating me !

Bob : Show me !

Alice : And you get the solution, I'm not so naive !

Alice and Bob : Let's think ...

Alice : I have an idea, I'll show you that *I have the solution* without giving you any information about the solution itself.

	2						9	
3		1	9		6	5		2
			8		4			
	9						5	
5			2		3			6
	7						2	
			4		7			
8		2	5		1	7		3
	5						8	

Bob : This Sudoko has no solution ! I spent hours on it, that's impossible !

Alice : You're a stupid donkey ! I got the solution since 2 days !

Bob : I can't believe it ! You're cheating me !

Bob : Show me !

Alice : And you get the solution, I'm not so naive !

Alice and Bob : Let's think ...

Alice : I have an idea, I'll show you that *I have the solution* without giving you any information about the solution itself.

Alice : Probabilistic Thinking !

	2						9	
3		1	9		6	5		2
			8		4			
	9						5	
5			2		3			6
	7						2	
			4		7			
8		2	5		1	7		3
	5						8	

Bob : This Sudoko has no solution ! I spent hours on it, that's impossible !

Alice : You're a stupid donkey ! I got the solution since 2 days !

Bob : I can't believe it ! You're cheating me !

Bob : Show me !

Alice : And you get the solution, I'm not so naive !

Alice and Bob : Let's think ...

Alice : I have an idea, I'll show you that *I have the solution* without giving you any information about the solution itself.

Alice : Probabilistic Thinking !

Property : if we shuffle the figures in a sudoku we still have a sudoku
Protocol : agree on a random (uniform) shuffling algorithm

1. Alice generates a uniform random shuffling (Bob ignores the seed)
2. Bob either
   - Choose a row, a column or a square (27 choices)
   - Check for the problem shuffle
3. Alice reveals the corresponding part of the sudoku, that is checked by Bob

Alice computes a random (uniform) permutation σ

$$\sigma(1) = 4\ \sigma(2) = 3\ \sigma(3) = 7\ \sigma(4) = 2\ \sigma(5) = 1\ \sigma(6) = 8\ \sigma(7) = 9\ \sigma(8) = 6\ \sigma(9) = 5$$

The problem

	2						9	
3		1	9		6	5		2
			8		4			
	9						5	
5			2		3			6
	7						2	
			4		7			
8		2	5		1	7		3
	5						8	

The shuffled problem

	3						5	
7		4	5		8	1		3
			6		2			
	5						1	
1			3		7			8
	9						3	
			2		9			
6		3	1		4	9		7
	1						6	

Alice computes a random (uniform) permutation σ

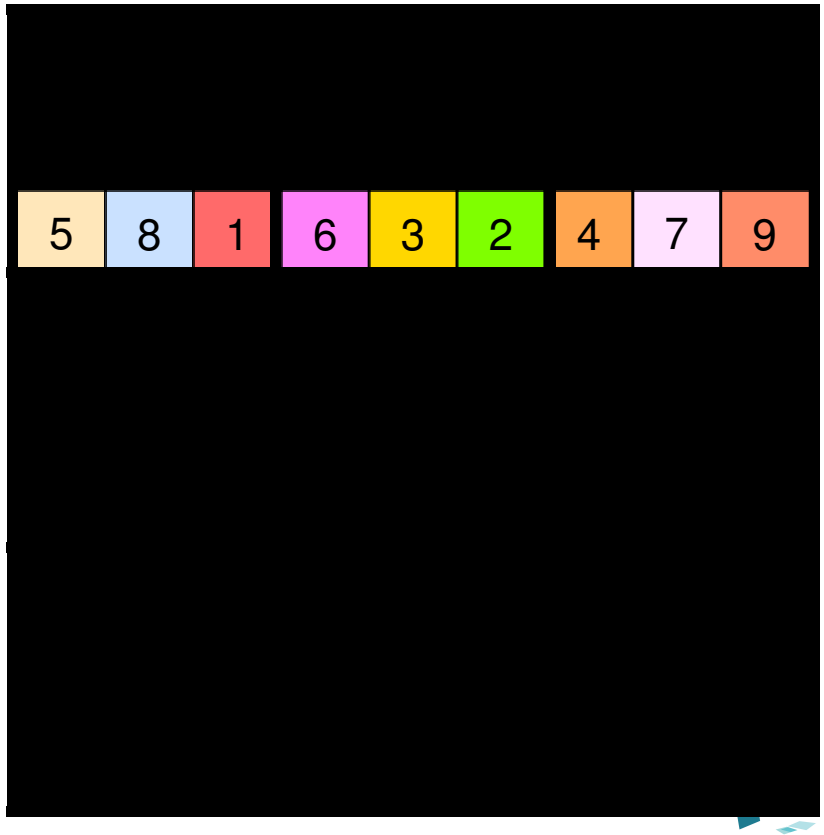
$$\sigma(1) = 4\ \sigma(2) = 3\ \sigma(3) = 7\ \sigma(4) = 2\ \sigma(5) = 1\ \sigma(6) = 8\ \sigma(7) = 9\ \sigma(8) = 6\ \sigma(9) = 5$$

Bob chooses Line 3 and Alice reveals Line 3

The shuffled solution (hidden)

9	3	2	4	7	1	8	5	6
7	6	4	5	9	8	1	2	3
5	8	1	6	3	2	4	7	9
3	5	8	9	4	6	7	1	2
1	4	6	3	2	7	5	9	8
2	9	7	8	1	5	6	3	4
8	7	5	2	6	9	3	4	1
6	2	3	1	5	4	9	8	7
4	1	9	7	8	3	2	6	5

The partially revealed solution



Alice computes another random (uniform) permutation σ

$$\sigma(1) = 5\ \sigma(2) = 1\ \sigma(3) = 6\ \sigma(4) = 2\ \sigma(5) = 3\ \sigma(6) = 9\ \sigma(7) = 7\ \sigma(8) = 8\ \sigma(9) = 4$$

Bob chooses the central square

The shuffled solution (hidden)

7	1	2	5	6	3	9	4	8
6	8	5	4	7	9	3	2	1
4	9	3	8	1	2	5	6	7
1	4	9	7	5	8	6	3	2
3	5	8	1	2	6	4	7	9
2	7	6	9	3	4	8	1	5
9	6	4	2	8	7	1	5	3
8	2	1	3	4	5	7	9	6
5	3	7	6	9	1	2	8	4

Ok thats good, lets try again

The partially revealed solution

7	5	8
1	2	6
9	3	4

Alice computes another random (uniform) permutation σ

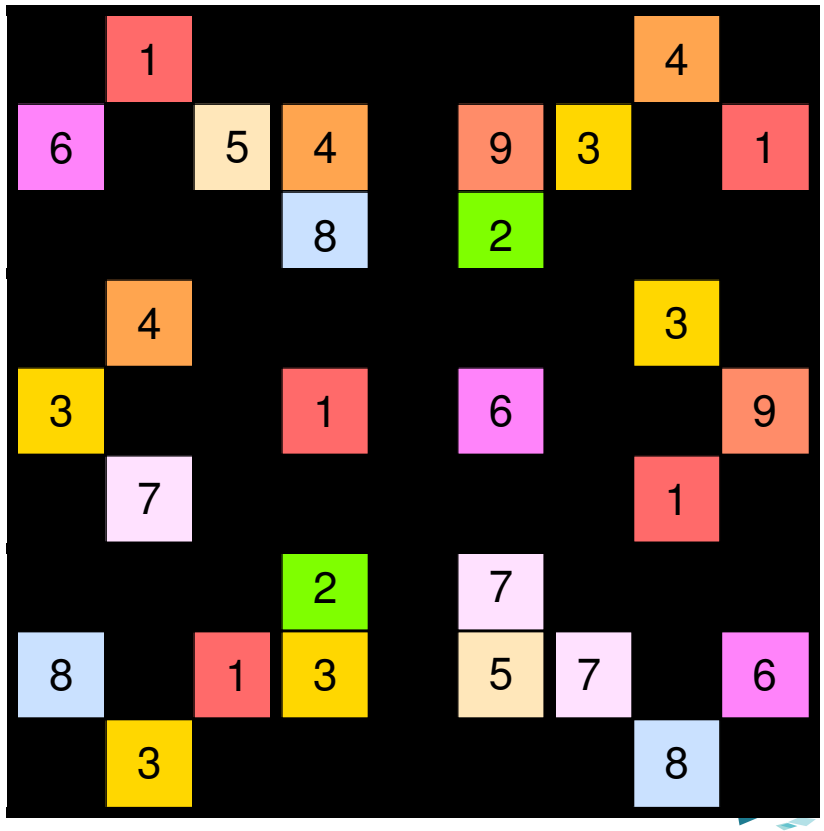
$$\sigma(1) = 5\ \sigma(2) = 1\ \sigma(3) = 6\ \sigma(4) = 2\ \sigma(5) = 3\ \sigma(6) = 9\ \sigma(7) = 7\ \sigma(8) = 8\ \sigma(9) = 4$$

Bob chooses to see the permutation

The shuffled solution (hidden)

7	1	2	5	6	3	9	4	8
6	8	5	4	7	9	3	2	1
4	9	3	8	1	2	5	6	7
1	4	9	7	5	8	6	3	2
3	5	8	1	2	6	4	7	9
2	7	6	9	3	4	8	1	5
9	6	4	2	8	7	1	5	3
8	2	1	3	4	5	7	9	6
5	3	7	6	9	1	2	8	4

The shuffled revealed problem



Alice computes another random (uniform) permutation σ

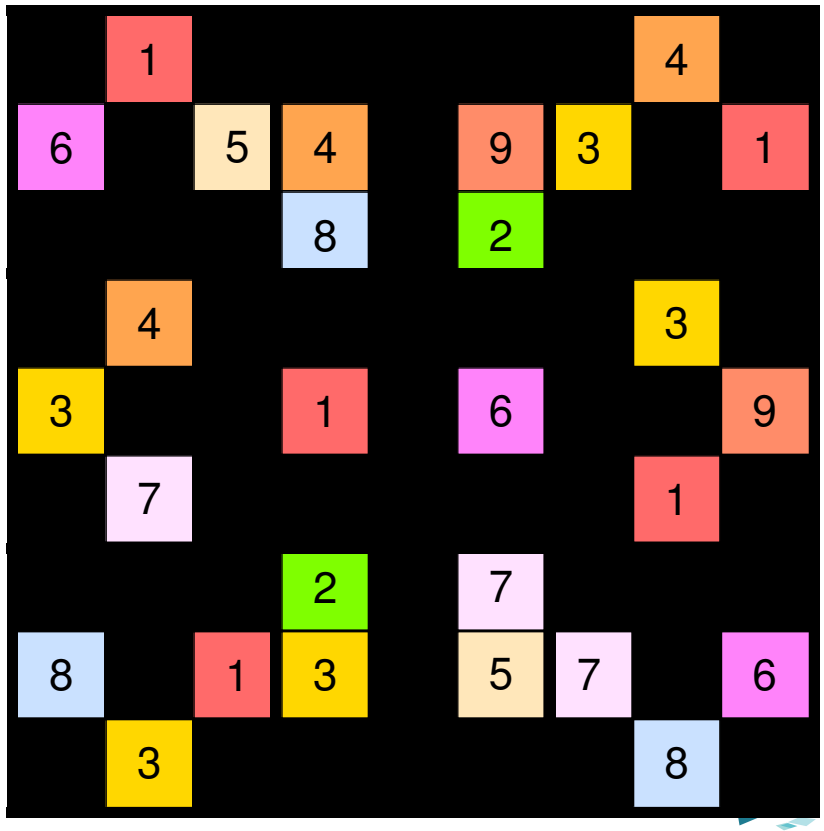
$$\sigma(1) = 5\ \sigma(2) = 1\ \sigma(3) = 6\ \sigma(4) = 2\ \sigma(5) = 3\ \sigma(6) = 9\ \sigma(7) = 7\ \sigma(8) = 8\ \sigma(9) = 4$$

Bob chooses to see the permutation

The initial problem

	2						9	
3		1	9		6	5		2
			8		4			
	9						5	
5			2		3			6
	7						2	
			4		7			
8		2	5		1	7		3
	5						8	

The shuffled revealed problem



ZERO-KNOWLEDGE INTERACTIVE PROOF

Alice has the solution

The protocol answers *OK* for all the questions and for an arbitrary long sequence of questions
What is the information given by the answer *Ok* ? (no difference with a uniform random sampling of a conditional permutation)

Alice is cheating

Then any permutation of the figures of Alice proposition is not a solution.
For a wrong proposition, at least one constraint is not satisfied and the probability of detecting the cheat is lower bounded by

$$p = \frac{1}{28}$$

and the probability that the cheat is not detected with n questions is bounded by

$$(1 - p)^n$$

Take $n = 500$, the probability that the cheat is not revealed is less than 10^{-7}.

Cryptography : **one-time pad** Gilbert S. Vernam (1919)
XOR : hide information, Tausworthe Random Generators (1965)

COMPUTING WITH COINS

1 A SIMPLE RANDOM GAME : Head or Tail

2 NUMERICAL COMPUTATION : Π

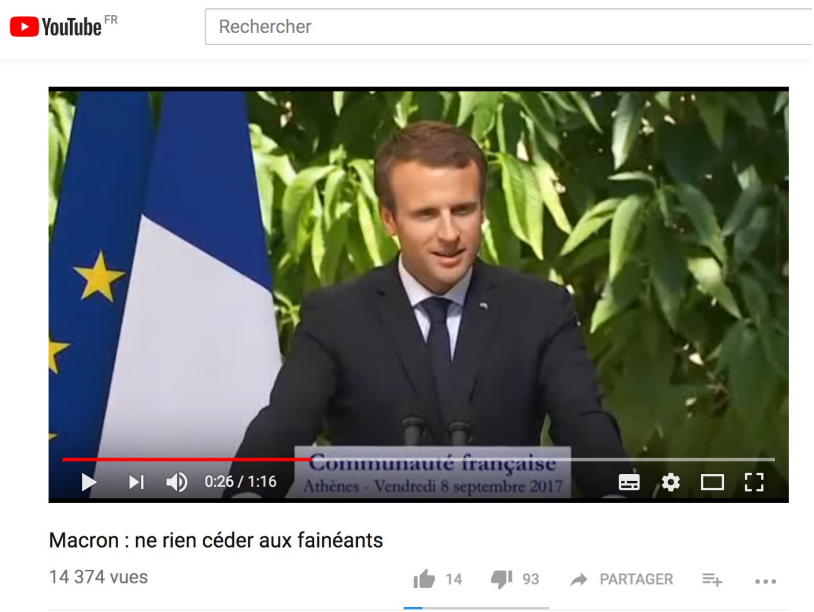
3 DOBBLE : INTERSECTING SUBSETS FAMILIES

4 ZKIP : Sudoku

5 LIKE OR UNLIKE

LIKE OR UNLIKE

Vote on the video

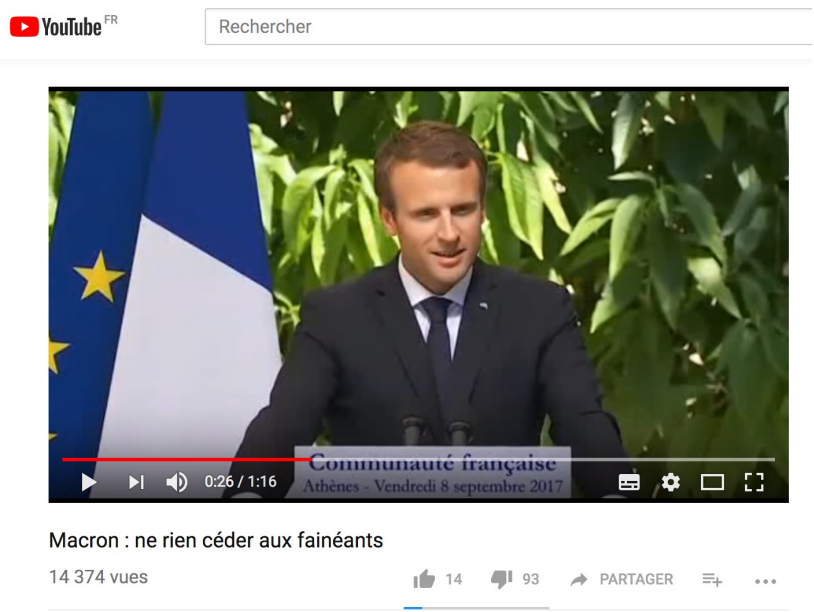


How can previous votes influence your decision ?

Information Number of likes/unlikes

LIKE OR UNLIKE

Vote on the video



How can previous votes influence your decision ?

Information Number of likes/unlikes

A stochastic Model

State of the system after n votes :

$$X_n = (N_L, N_U)$$

Dynamic (influence of previous votes) :

Vote *Like* with probability

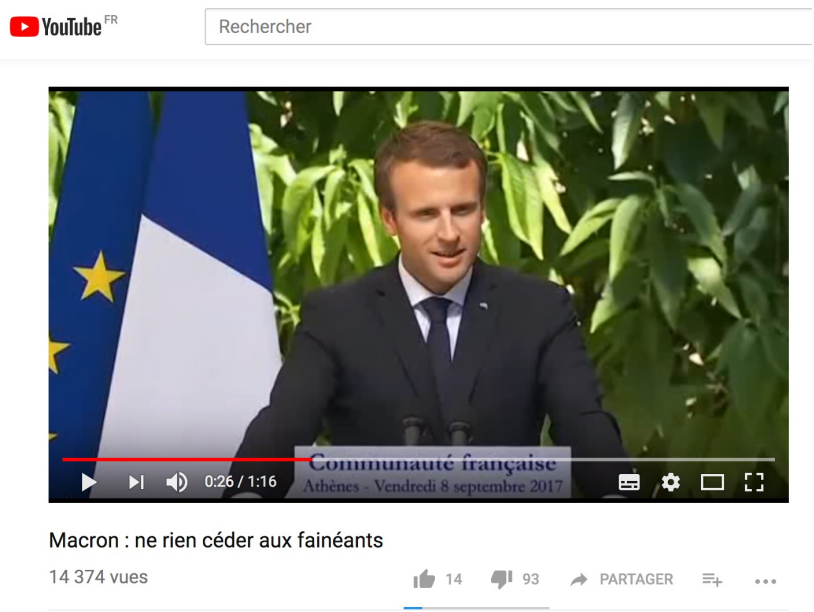
$$\frac{N_L}{N_L + N_U} = p_n$$

Vote *Unlike* with probability

$$\frac{N_L}{N_L + N_U} = 1 - p_n$$

LIKE OR UNLIKE

Vote on the video



How can previous votes influence your decision ?

Information Number of likes/unlikes

A stochastic Model

State of the system after n votes :

$$X_n = (N_L, N_U)$$

Dynamic (influence of previous votes) :

Vote *Like* with probability

$$\frac{N_L}{N_L + N_U} = p_n$$

Vote *Unlike* with probability

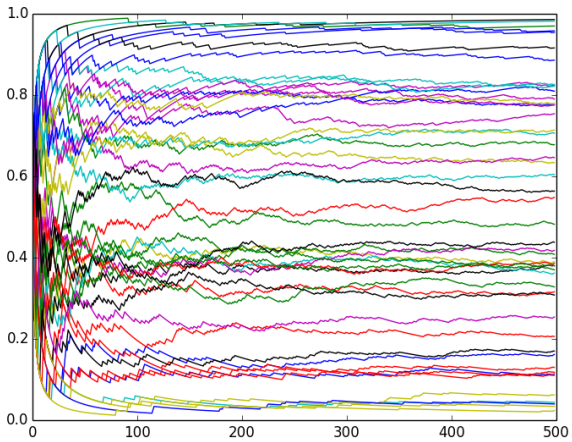
$$\frac{N_L}{N_L + N_U} = 1 - p_n$$

Questions

1. Does p_n converge to a limit ?
2. What could be the limit value ?
3. What is the impact of the initial value ?
4. How does p_n converge ?

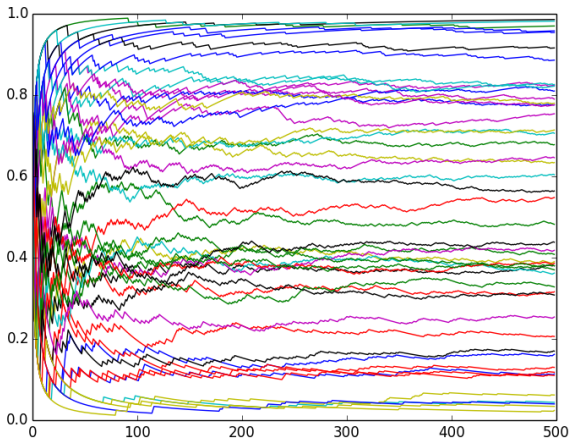
EXPERIMENTS

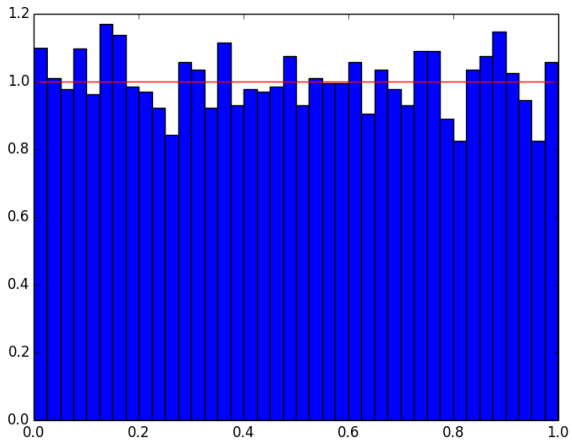
50 trajectories, $(a, b) = (1, 1)$**,**



EXPERIMENTS

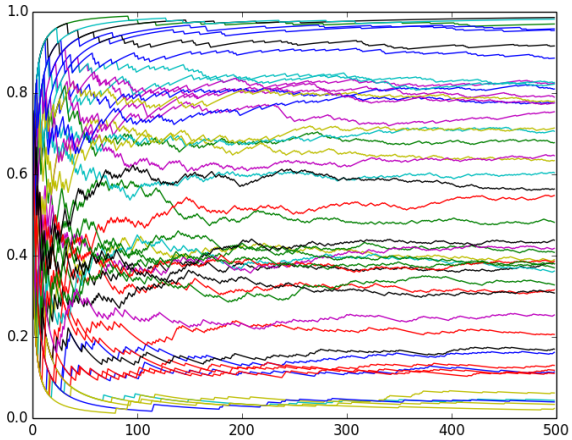
50 trajectories, $(a, b) = (1, 1)$**, histogram** $nexp = 5000$

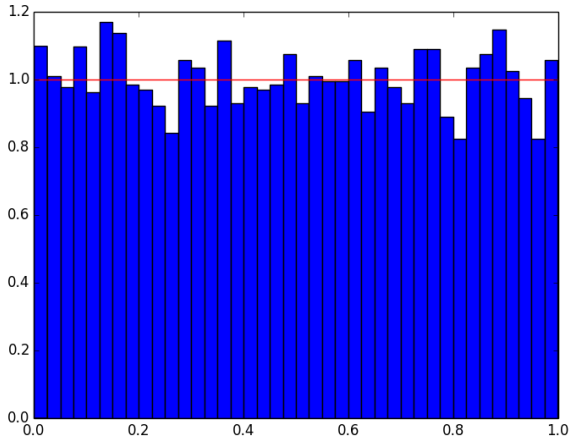




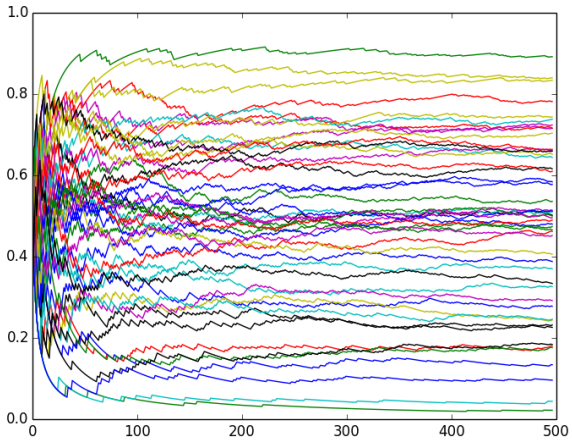
EXPERIMENTS

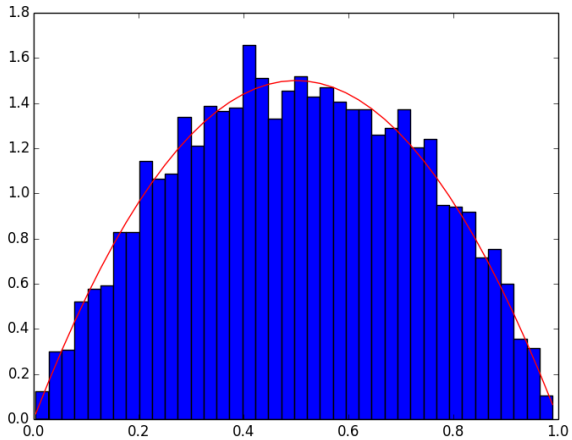
50 trajectories, $(a, b) = (1, 1)$**, histogram** $nexp = 5000$





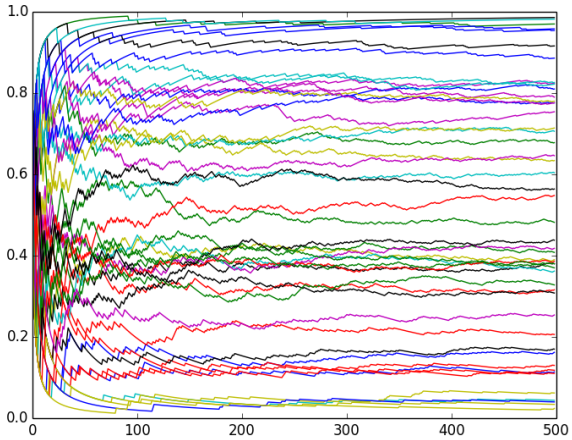
50 trajectories, $(a, b) = (2, 2)$**, histogram** $nexp = 5000$

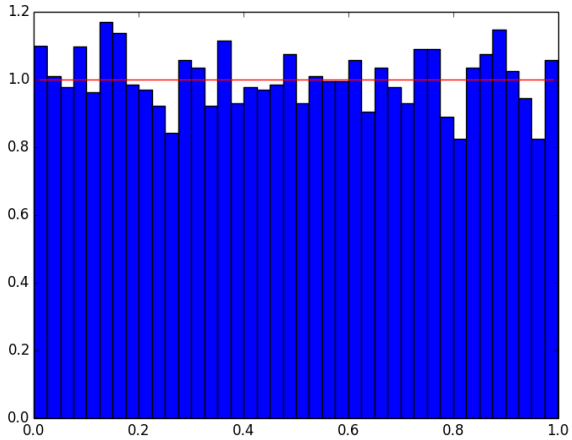




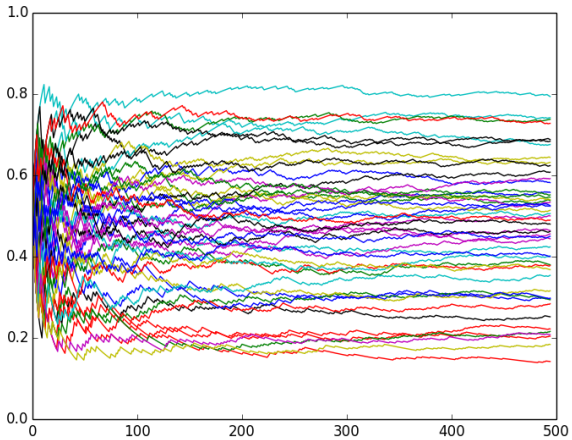
EXPERIMENTS

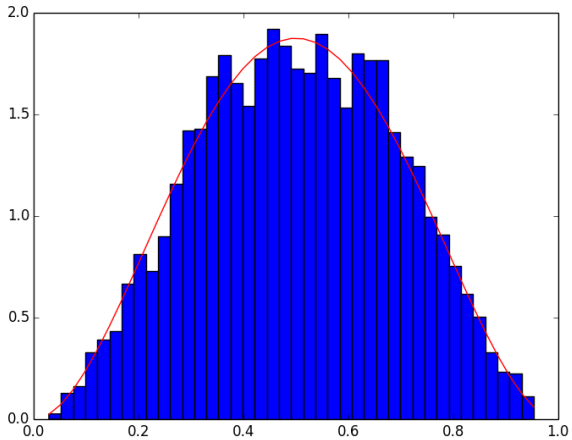
50 trajectories, $(a, b) = (1, 1)$**, histogram** $nexp = 5000$





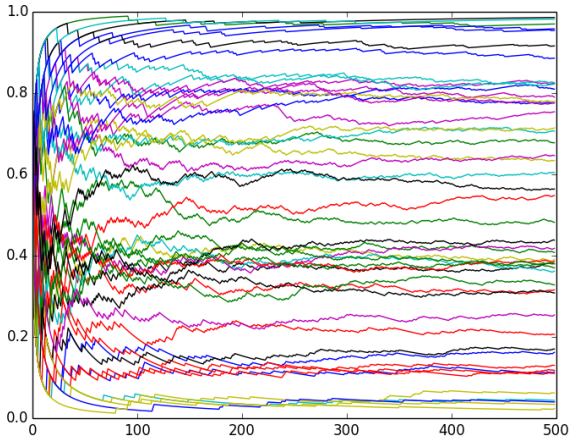
50 trajectories, $(a, b) = (3, 3)$**,histogram** $nexp = 5000$

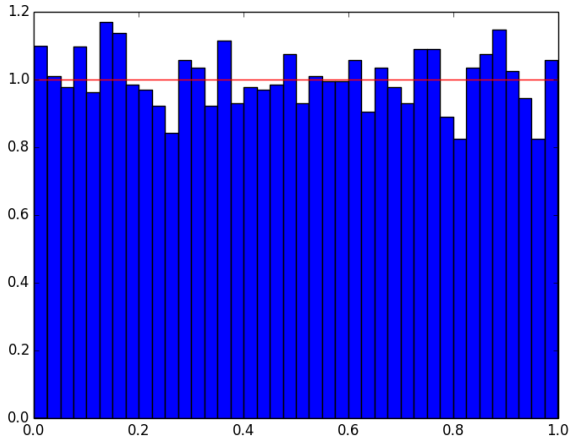




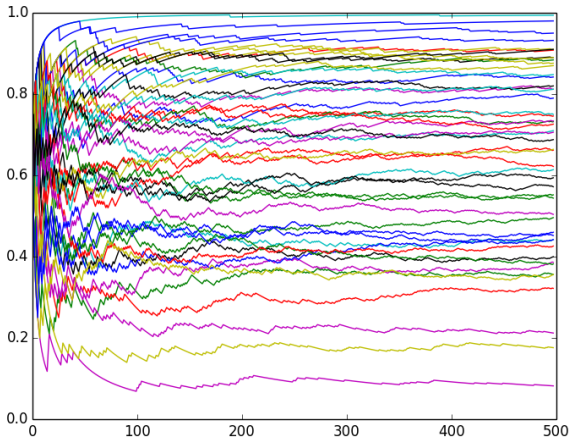
EXPERIMENTS

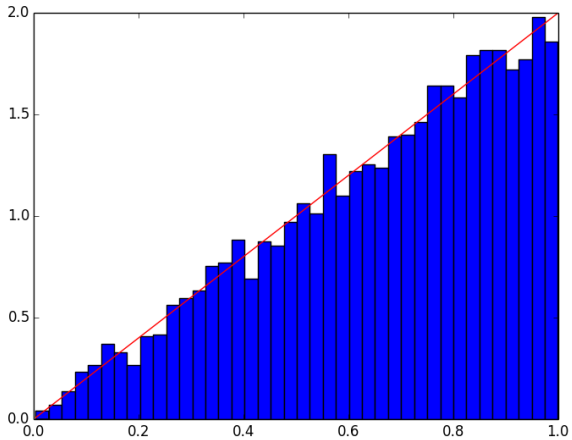
50 trajectories, $(a, b) = (1, 1)$**, histogram** $nexp = 5000$





50 trajectories, $(a, b) = (2, 1)$**, histogram** $nexp = 5000$





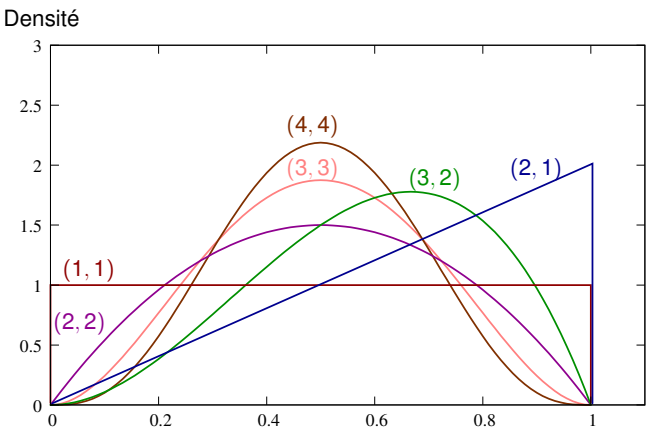
CONVERGENCE

Law convergence

For an initial condition (a, b), p_n converges in law to a random variable p_∞ with a density $\mathcal{B}eta(a, b)$ on $[0, 1]$

$$f_{a,b}(x) = \frac{(a+b-1)!}{(a-1)!(b-1)!} x^{a-1}(1-x)^{b-1};$$

$$\mathbb{E}\, p_\infty = \frac{a}{a+b} \qquad \mathbb{V}ar\, p_\infty = \frac{ab}{(a+b)^2(a+b+1)}$$



Densité limite pour différentes configurations initiales (a, b)

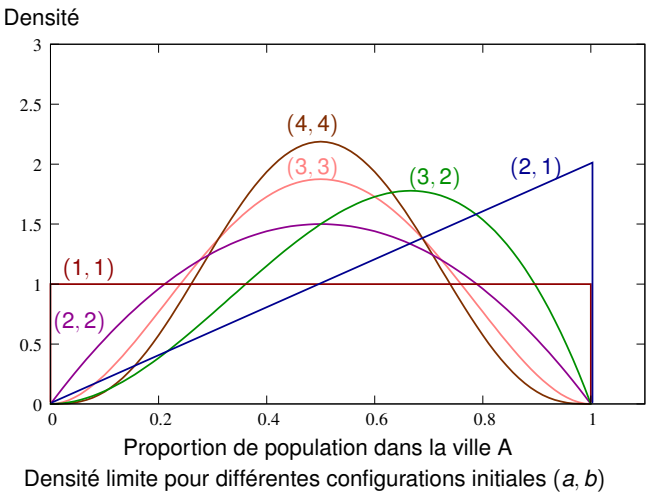
CONVERGENCE

Law convergence

For an initial condition (a, b), p_n converges in law to a random variable p_∞ with a density $\mathcal{B}eta(a, b)$ on $[0, 1]$

$$f_{a,b}(x) = \frac{(a+b-1)!}{(a-1)!(b-1)!} x^{a-1}(1-x)^{b-1};$$

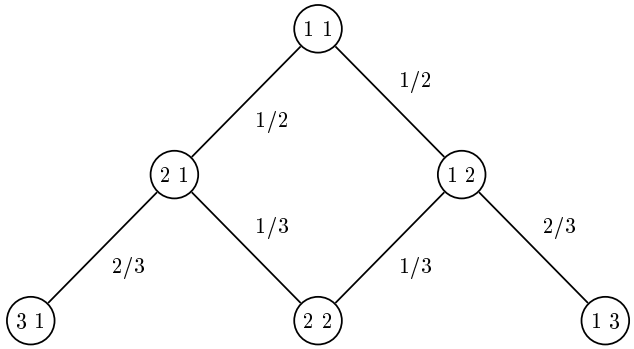
$$\mathbb{E}\, p_\infty = \frac{a}{a+b} \qquad \mathbb{V}ar\, p_\infty = \frac{ab}{(a+b)^2(a+b+1)}$$



Densité limite pour différentes configurations initiales (a, b)

A visual proof

For $(a, b) = (1, 1)$



Almost sure convergence

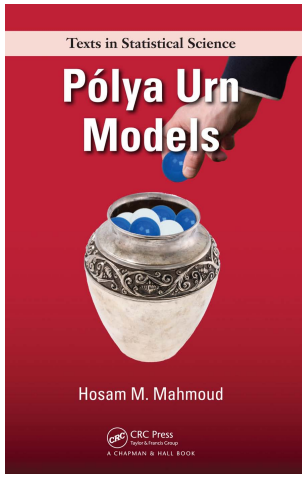
Every trajectory has a finite limit.

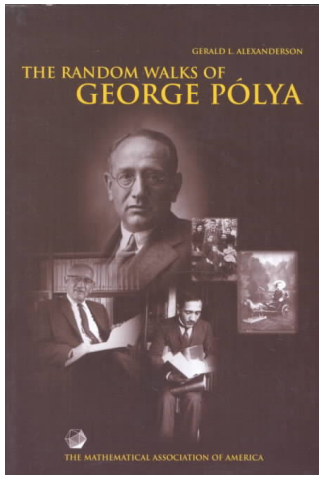
$$p_n \longrightarrow p_\infty \text{ almost surely}$$

Proof via martingale theory

REFERENCES

Generic Stochastic Model



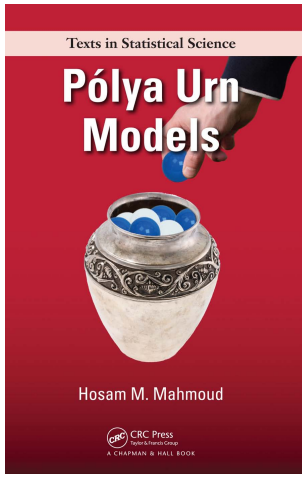


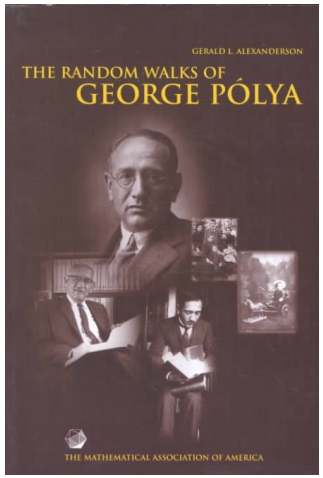
George Pólya

Sur quelques points de la théorie des probabilités Annales de l'institut Henri Poincaré, Tome 1 (1930) no. 2 , p. 117-161

REFERENCES

Generic Stochastic Model





George Pólya

Sur quelques points de la théorie des probabilités Annales de l'institut Henri Poincaré, Tome 1 (1930) no. 2 , p. 117-161

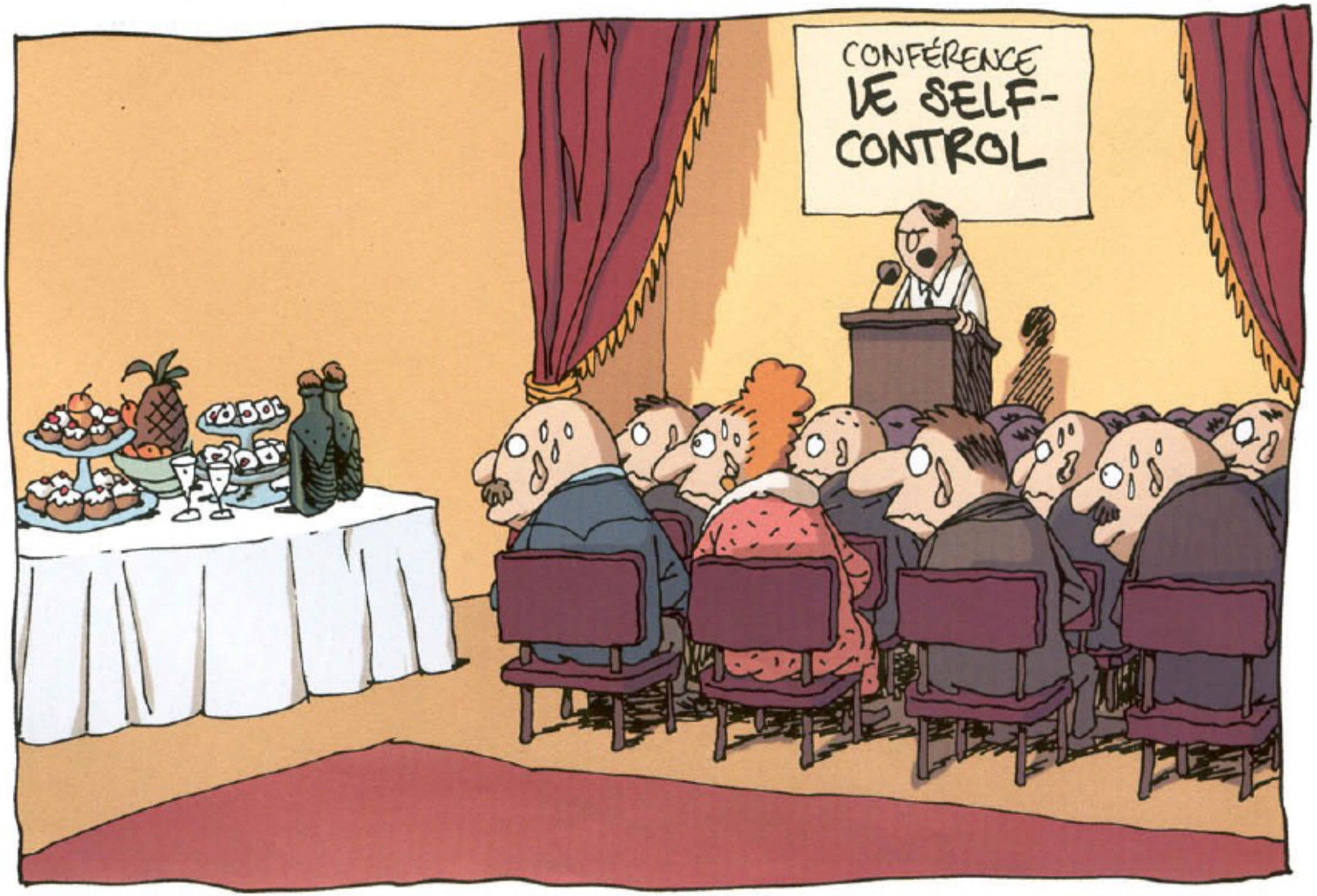
Quotations How to solve it (Princeton 1945)

—-

If you have to prove a theorem, do not rush. First of all, understand fully what the theorem says, try to see clearly what it means. Then check the theorem ; it could be false. Examine the consequences, verify as many particular instances as are needed to convince yourself of the truth. When you have satisfied yourself that the theorem is true, you can start proving it.

—-

If there is a problem you can't solve, then there is an easier problem you can solve : find it.



Remerciements à Thiriet-Larcenet *La vie est courte, tome 3 : rien ne va plus* (2000)