Hasard et Chaos

Jean-Marc Vincent[1]

[1] Laboratoire LIG, projet Inria-Mescal
Universités de Grenoble
Jean-Marc.Vincent@imag.fr

Du grand bazar au bazar productif

Déterminisme (Trésor de la Langue Française)

subst. masc.

1. Ensemble des causes ou conditions nécessaires à la détermination d'un phénomène :
2. P. ext., vocab. sc. et philos. [D'un point de vue théorique] Principe scientifique d'après lequel tout phénomène est régi par une (ou plusieurs) loi(s) nécessaire(s) telle(s) que les mêmes causes entraînent dans les mêmes conditions ou circonstances, les mêmes effets. Déterminisme objectif de la science.

Déterminisme (Wikipedia)

Le déterminisme est une notion philosophique selon laquelle chaque événement est déterminé par un principe de causalité.

Les événements actuels ont avec les précédents une liaison fondée sur le principe évident, qu'une chose ne peut pas commencer d'être, sans une **cause** qui la produise. Cet axiome, connu sous le nom de *principe de la raison suffisante*, s'étend aux actions mêmes que l'on juge indifférentes.

"Nous devons considérer l'état présent de l'univers comme l'effet de son état antérieur, et comme la cause de celui qui va suivre. Une intelligence qui pour un instant donné connaîtrait toutes les forces dont la nature est animée et la situation respective qui la composent, si par ailleurs elle était assez vaste pour soumettre ces données à l'analyse, embrasserait dans la même formule les mouvements des plus grands corps de l'univers et ceux du plus léger atome : rien ne serait incertain pour elle, et l'avenir comme le passé serait présent à ses yeux."

P-S. Laplace (1814)

Pierre-Simon de Laplace (1749-1827)

Né à Beaumont-en-Auge, fils de cultivateur, Laplace s'initia aux mathématiques à l'Ecole militaire de cette petite ville. Il y commença son enseignement. Il doit cette éducation à ses voisins aisés qui avait détecté son intelligence exceptionnelle.
A 18 ans, il arrive à Paris avec une lettre de recommandation pour rencontrer le mathématicien d'Alembert, mais ce dernier refuse de rencontrer l'inconnue. Mais Laplace insiste: il envoie à d'Alembert un article qu'il a écrit sur la mécanique classique. D'Alembert en est si impressionné qu'il est tout heureux de patronner Laplace. Il lui obtient un poste d'enseignement en mathématique. En 1783, il devint examinateur du corps de l'artillerle et fut élu, en 1785, à l'Académie des Sciences. A la Révolution, il participa à l'organisation de l'Ecole Normale et de l'Ecole Polytechnique, et fut membre de l'Institut, dès sa création. Bonaparte lui confia le ministère de l'Intérieur, mais seulement pour 6 mois.
L' œuvre la plus importante de Laplace concerne le calcul des probabilités et la mécanique céleste. Il établit aussi, grâce à ses travaux avec Lavoisier entre 1782 et 1784 la formule des transformations adiabatiques d'un gaz, ainsi que deux lois fondamentales de l'électromagnétisme. En mécanique, c'est avec le mathématicien Joseph-Louis de Lagrange, Laplace résume ses travaux et réunit ceux de Newton, Halley, Clairaut, d'Alembert et Euler, concernant la gravitation universelle, dans les cinq volumes de sa mécanique céleste (1798-1825).
On rapporte que, feuilletant la Mécanique céleste, Napoléon fit remarquer à Laplace qu'il n'y était nulle part fait mention de Dieu. "Je n'ai pas eu besoin de cette hypothèse", rétorqua le savant.

Plan de l'exposé

1. **Systèmes dynamiques**
   - Formalisation
   - Théories et applications
2. **Le chapeau du clown**
   - Itérations discrètes
   - Théorème fondamental
3. **La folle randonnée**
   - Approche mesure
   - Ergodicité
   - Modèles logistiques
4. **Le calcul chaotique**
   - Pourquoi générer ?
   - Fabriquer le hasard
   - Générateurs pseudo-aléatoires

Systèmes dynamiques

Définition (Grand robert): dynamique
(1692); gr. dunamikos, de dunamis “force”

1 (adj) Relatif aux forces, à la notion de force. “Traité de la science dynamique”, de Leibniz.
2 (adj) Qui considère les choses dans leur mouvement, leur devenir.
...
1 (n.f.)(1752) Phys. Branche de la mécanique qui étudie le mouvement d’un mobile considéré dans ses rapports avec les forces qui en sont les causes.
2 (n.f.) Sociol. Partie de la sociologie qui étudie les faits en évolution et non dans leur état actuel.
3 (n.f.) (v. 1940) Psychol., sociol. Dynamique de(s) groupe(s) : ensemble des règles qui président à la conduite des groupes sociaux dans le cadre de leur activité propre.

Systèmes dynamiques : formalisation

Espace d'état

Modélisation du système :
- description/quantification du système : ensemble $\mathcal{X}$
- structuré : topologie, opérateurs, métrique, ...
- sémantique : lien avec l'observation et la mesure

Discret ou continu

Espace du temps

Variable temps ensemble totalement ordonné $\mathcal{T}$
- discret ($\mathbb{N}$ ou $\mathbb{Z}$) : sauts (cf observation)
- continu ($\mathbb{R}$)
- avec ou sans passé

Systèmes dynamiques : formalisation (2)

X_t état du système à l'instant $t \in \mathcal{T}$ Trajectoire $T = \{X_t\}_{t\in\mathcal{T}} \in \mathcal{X}^{\mathcal{T}}$

Système clos

Pas d'influence extérieure
Temps discret :

$$X_{t+1} = \Phi(X_t)$$ Suites récurrentes, itérations de fonctions

Temps continu :

$$\frac{dX_t}{dt} = \Psi(X_t)$$ Équations différentielles

Système ouvert

Processus exogène d'innovation $\{\xi_t\}_{t\in\mathcal{T}}$
Temps discret :

$$X_{t+1} = \Phi(X_t, \xi_{t+1})$$ Processus de décision

Temps continu :

$$\frac{dX_t}{dt} = \Psi(X_t, \xi_t)$$Théorie du contrôle

Systèmes dynamiques : formalisation (3)

Théories

1. $\mathcal{X} = \mathbb{N}$ $\mathcal{T} = \mathbb{N}$ automate, théorie des graphes, théorie des langages, chaînes de Markov,...
2. $\mathcal{X} = \mathbb{N}$ $\mathcal{T} = \mathbb{R}$ automate temporisé, langages temps réel, chaîne de Markov en temps continu,...
3. $\mathcal{X} = \mathbb{N}$ $\mathcal{T} = \mathbb{R}$ théorie du contrôle, processus stochastiques de saut,...
4. $\mathcal{X} = \mathbb{R}$ $\mathcal{T} = \mathbb{R}$ systèmes différentiels, processus stochastiques, mouvement Brownien...

Changement d'échelle

discrétisation, renormalisation, fluidification,...

Systèmes dynamiques : formalisation (4)

Questions ?

Horizon infini

1. Stabilité : $T \in A$
2. Existence d'un (ou plusieurs) régime(s) stationnaire(s)
3. Vitesse de convergence, séparabilité
4. Caractérisation du régime stationnaire (calcul)

points fixes, cycles, contraction, ...

Le chapeau du clown

$\mathcal{X} = [0, 1]$, $\mathcal{T} = \mathbb{R}$, $\Phi : [0, 1] \to [0, 1]$ continue, $\mathcal{C}^1$ par morceaux

Questions

Constat

1. existence de cycles limite;
2. dépend de l'état initial;
3. cas particuliers : $\frac{k}{2^n}$

QUESTIONS

1. existe-t-il des cycles limite de tout ordre ?
2. toute valeur initiale admet-elle un cycle limite ?

Cycles

Cycles

1. $x_0 = \frac{1}{2^k} \Rightarrow$ converge vers 0;
2. $x_0 = \frac{2}{2^p - 1} \Rightarrow$ cycle d'ordre p;
   ex: $x_0 = \frac{2}{3}$ cycle d'ordre 2, $x_0 = \frac{2}{7}$ cycle d'ordre 3, ...
3. ??

Ecriture binaire de x_0

$$x = \sum_i \frac{\alpha_i}{2^i} = 0, \alpha_1 \alpha_2 \alpha_3 \cdots \alpha_n \cdots$$

$$\begin{cases} si\ \alpha_1 = 0 & f(x) = 0, \alpha_2 \alpha_3 \cdots \alpha_n \cdots ; \\ si\ \alpha_1 = 1 & f(x) = 1 - 0, \alpha_2 \alpha_3 \cdots \alpha_n \cdots ; \end{cases}$$

Bazar complet

1. x_0 rationnel $\Rightarrow$ converge vers un cycle 0;
2. $x_0 = 0,10100100010000100000 1 \cdots$;
   Points d'adhérence de la suite
   $$\left\{0, \frac{1}{2}, \frac{1}{4}, \cdots, \frac{1}{2^n}, \cdots\right\}$$
3. Nombre de Champernowne
   $$C = 0,0101110010111011110001001101010111100110111101111 \cdots$$
   $\Rightarrow$ partout dense

David Gawen Champernowne (1912-2000)

Pas de photo pour l'instant

David Gawen Champernowne (July 9, 1912 - August 19, 2000) was Professor of Statistical Economics at Oxford (1948 -1959), and professor of Economics and Statistics at Cambridge (1970-2000). He published work on Champernowne's Number in 1933, while still an undergraduate at the University of Cambridge.
After academic work at Cambridge and the London School of Economics, he worked in the Prime Minister's Statistical department ao supply quantitative information to help Winston Churchill make decisions. However, he did not get on well with the department head Prof FA Lindemann, and in 1941 he moved on to become a programme director in the Ministry of Aircraft Production.
Working with an old college friend, Alan Turing in 1948, he helped develop one of the first chess-playing computer programs.
The book for which he is most renowned, synthesising a life's work, Economic Inequality and Income Distribution (Cambridge University Press), was published in 1998.

Enfin un peu de théorie

Théorème (Sharkowski 1964)

Si Φ est continue et s'il existe un cycle d'ordre 3 alors il existe des cycles de tout ordre et des attracteurs infinis.

$$
\begin{array}{cccccccc}
3 & 5 & 7 & 9 & 11 & 13 & \cdots & \cdots \\
6 & 10 & 14 & 18 & 22 & 26 & \cdots & \cdots \\
12 & 20 & 28 & 36 & 44 & 52 & \cdots & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\cdots & \cdots & \cdots & \cdots & 8 & 4 & 2 & 1
\end{array}
$$

Oleksandr Sharkovsky (1936 -)

Oleksandr Sharkovsky attended his local university of Kiev, graduating in 1958. In 1961 he was appointed to the Institute of Mathematics of the Academy of Sciences of the Ukraine in Kiev. He also taught at the University of Kiev from 1967.
Sharkovsky's main areas of interest are the theory of dynamical systems, the theory of stability and the theory of oscillations. He also works in the theory of functional and functional differential equations, and the study of difference equations and their application.
He is perhaps best known for an important theorem on continuous functions which he proved in 1964. Although the result did not attract a great deal of interest at the time of its publication, during the 1970s other surprising results were proved which turned out to be special cases of Sharkovsky's theorem.

Généralisation

Remarques

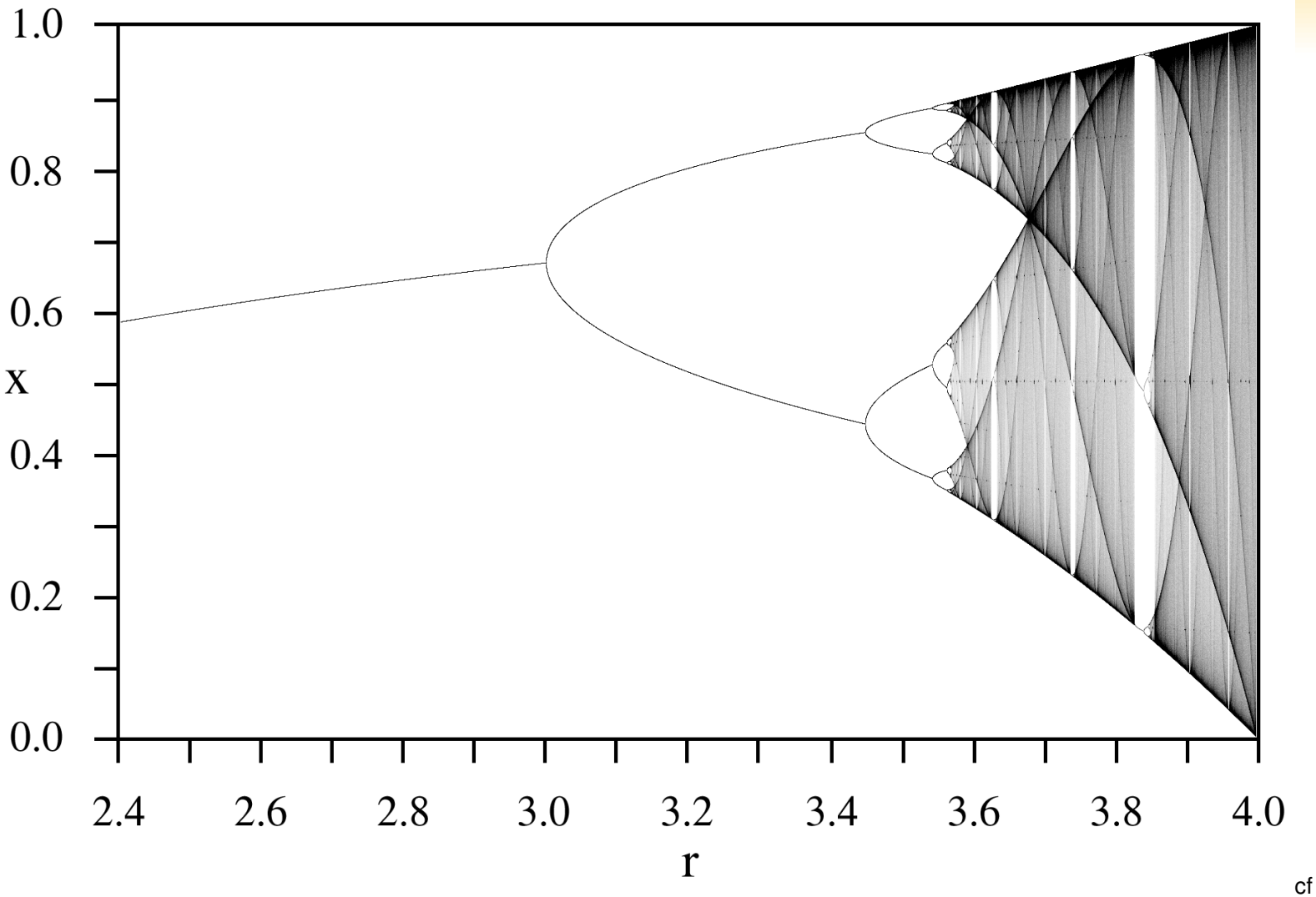
1. Φ d'ordre $2^i \Rightarrow$ pas d'attracteur infini
2. Φ d'ordre $2^i \times$ *impair* $\Rightarrow$ attracteur infini
3. Φ d'ordre 2^i pour tout $i \Rightarrow$ on ne sait pas

Fonction logistique

$$f(x) = \mu x(1 - x).$$

- diagramme de bifurcation
- Nombre de Feigenbaum

Diagramme de bifurcation



cf

Wikipedia (Feigenbaum)

Feigenbaum (1944-)

Dr. Feigenbaum received his Ph.D. in theoretical high energy physics from the Massachusetts Institute of Technology in 1970, under Francis E. Low. He was a research associate at Cornell University from 1970 to 1972, and a research associate at Virginia Polytechnic Institute from 1972 to 1974. He then moved to Los Alamos National Laboratory, where he was a staff member from 1974 to 1981 and a fellow from 1981 to 1982. (Dr. Feigenbaum, while creating his work on chaos, shared his office with Murray Gell-Mann in 1976.) From 1982 to 1986 he was a professor of physics at Cornell University. Dr. Feigenbaum was a visiting member at the Institute for Advanced Studies at Princeton in 1978 and 1984. He joined Rockefeller University in 1986. In addition to being the university's Toyota Professor, he is also director of the Center for Studies in Physics and Biology.

`http://www.rockefeller.edu/research/abstract.php?id=38`

Que peut-on dire ?

- Ensemble des trajectoires : $\Rightarrow$ développement binaire de l'état initial (contient toute l'information)
- Trajectoires périodiques : $\Rightarrow$ état initial $x_0 \in \mathbb{Q}$ (rationnel)
- Trajectoires avec un attracteur dénombrable
- Trajectoires partout denses

Préservation de la mesure

Soit $I \subset [0,1]$

$$longueur\Phi^{-1}(A) = longueur(A);$$

Φ préserve la mesure de longueurs sur $[0,1]$
Dynamique sur des points devient une dynamique sur des ensembles

Ensemble invariant

Un ensemble A est invariant ssi $\Phi^{-1}(A) = A$.
Une transformation Φ est **ergodique** si et seulement si pour tout A invariant $mesure(A) = 0$ ou 1.

Théorème ergodique (corollaire Birkhoff 1931)

On a l'équivalence suivante

- Φ est ergodique sur $([0,1], \mathcal{A}, \mu)$
- Pour tout A tel que $\mu(A) > 0$

$$\mu\left(\bigcup_{n\geqslant 1} \Phi^{-n}(A)\right) = 1;$$

- Pour tout A, B tel que $\mu(A) > 0$, $\mu(B) > 0$, il existe $n \geqslant 1$ tel que

$$\mu(\Phi^{-n}(A) \cap B) > 0;$$

- Pour toute fonction f

$$\frac{1}{n}\sum_{k=0}^{n-1} f(\Phi^n(x_0)) \longrightarrow \int f d\mu.$$

Georges David Birkhoff (1884-1944)

George David Birkhoff was an American mathematician, best known for what is now called the ergodic theorem. Birkhoff was one of the most important leaders in American mathematics in his generation, and during his prime he was considered by many to be the preeminent American mathematician.
Birkhoff obtained his A.B. and A.M. from Harvard. He completed his Ph.D. in 1907, on differential equations, at the University of Chicago. While Eliakim Hastings Moore was his supervisor, he was most influenced by the writings of Henri Poincaré. After teaching at the University of Wisconsin and Princeton University, he taught at Harvard University from 1912 until his death.
In 1912, attempting to solve the four color problem, Birkhoff introduced the chromatic polynomial. Even though this line of attack did not prove fruitful, the polynomial itself became an important object of study in algebraic graph theory. In 1913, he proved Poincaré's "Last Geometric Theorem," a special case of the three-body problem, a result that made him world famous. In 1927, he published his Dynamical Systems. He wrote on the foundations of relativity and quantum mechanics, publishing (with R E Langer) the monograph Relativity and Modern Physics in 1923. In 1923, Birkhoff also proved that the Schwarzschild geometry is the unique spherically symmetric solution of the Einstein field equations. A consequence is that black holes are not merely a mathematical curiosity, but could result from any spherical star having sufficient mass.
Birkhoff's most durable result has been his 1931 discovery of what is now called the ergodic theorem. Combining insights from physics on the ergodic hypothesis with measure theory, this theorem solved, at least in principle, a fundamental problem of statistical mechanics. The ergodic theorem has also had repercussions for dynamics, probability theory, group theory, and functional analysis. He also worked on number theory, the Riemann–Hilbert problem, and the four colour problem. He proposed an axiomatization of Euclidian geometry different from Hilbert's; this work culminated in his text Basic Geometry (1941).

Exemple : $\Phi(x) = 2x$ **mod** 1

Doublement de l'angle
On montre que Φ préserve la mesure usuelle sur $[0, 1[$ et la transformation est ergodique.

Exemple : $\Phi(x) = x + \theta$ mod 1

$\theta \in \mathbb{Q}$

$\theta = \frac{p}{q}$, soit $B \in [0, \frac{1}{q}[$

$$A = \bigcup_{k=0}^{q-1} (B + \frac{k}{q}),$$

est invariant de mesure > 0, la transformation n'est pas ergodique.

$\theta \in \mathbb{R} - \mathbb{Q}$

Par passage à la transformée de Fourier on montre que A invariant est de mesure 0 ou 1.
La transformation est ergodique, les trajectoires sont partout denses et le nombre moyen de passage dans un intervalle converge vers la longueur de celui-ci.

Exemple : $\Phi(x) = \frac{1}{x} - \lfloor \frac{1}{x} \rfloor$, $x \in [0, 1[$

Développement en fractions continues :

$$x = \cfrac{1}{a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots}}} \quad g(x) = \lfloor \frac{1}{x} \rfloor$$

$a_n = g(\Phi^n(x))$

On montre que Φ préserve la mesure $\mu([a, b[) = \int_a^b \frac{dx}{1+x}$ et la transformation est ergodique.

Synthèse

Théorème ergodique

Les transformations ergodiques vérifient la loi des grands nombres
Interprétation:
Connaître une trajectoire $\Leftrightarrow$ connaître la mesure invariante

Application

physique statistique: trajectoire d'une particule définit la répartition de l'ensemble
connaissance de la vie complète de l'individu revient à connaître la répartition de la communauté
mesure sur le temps est équivalente à une mesure sur l'espace

Hasard et Chaos

L'instabilité d'une dynamique déterministe conduit à l'apparition de l'aléatoire.
Y.G. Sinai

$\Rightarrow$ Méthodes probabilistes/statistiques d'analyse de dynamiques instables.

Problèmes

1. Calcul de la probabilité invariante
2. Analyse du régime transitoire

Exemple : la fonction logistique $L_a(x) = ax(1-x)$

Modèles de dynamique des populations

- Modèle de Malthus 1766-1834

  $$y' = \alpha y.$$

  Explosion de la population
- Modèle de Verhulst 1804-1849

  $$y' = \beta y(M - y).$$

  Auto-contrôle de la population.

Solution :

$$y(t) = K \frac{1}{1 + \left(\frac{K}{y_0} - 1\right) e^{-rt}}.$$

Discrétisation

Schéma d'intégration d'Euler

$$\begin{aligned} y_{n+1} &= y_n + h\beta y_n(M - y_n) = y_n(1 + h\beta M - h\beta y_n) \\ &= (1 + h\beta M)y_n(1 - \frac{h\beta}{1 + h\beta M} y_n) \end{aligned}$$

$z_n = \frac{h\beta}{1+h\beta M} y_n$

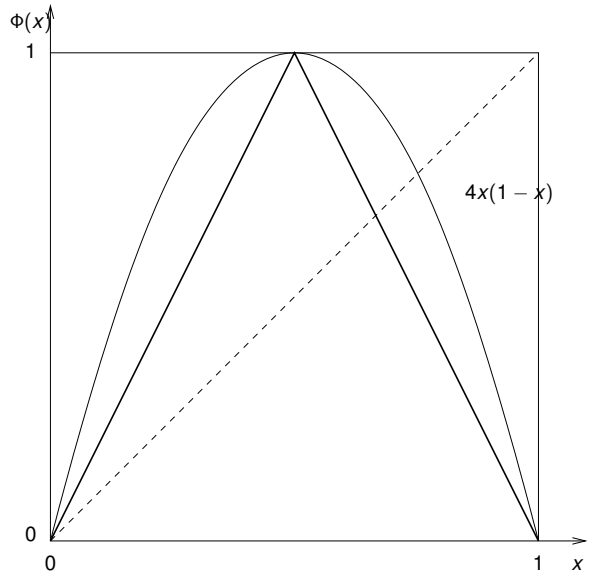
$$z_{n+1} = (1 + h\beta M)z_n(1 - z_n).$$

Forme $y_{n+1} = L_a(y_n)$

$$\begin{cases} \mu \leqslant 1 & \text{0 unique point fixe,} \\ 1 < \mu \leqslant 3 & \text{2 points fixes,} \\ \dots & \dots \\ \mu = 4 & \text{all cycles and infinite trajectories.} \end{cases}$$

Highly unstable

Exemple : la fonction logistique $L_4(x) = 4x(1-x)$



Mesure invariante μ, densité f

$$\mu(L_4^{-1}(A) = \mu(A), \text{ c'est à dire } \int_{L_4^{-1}(A)} f(x)dx = \int_A f(x)dx,$$

pour tout A mesurable (intervalles de la forme $[0, x]$)

Exemple : la fonction logistique $L_4(x) = 4x(1-x)$ (suite)

Fonction conjuguées

g et h sont des fonctions **conjuguées** ssi il existe C bijective et continue telle que $C \circ g = h \circ C$.
Théorème : L_4 et T sont conjuguées et la fonction

$$C(x) = \frac{1 - \cos \pi x}{2}.$$

$$L_4(C(x)) = 4C(x)(1 - C(x)) = 4\frac{1 - \cos \pi x}{2}\frac{1 + \cos \pi x}{2} = \sin^2 \pi x.$$

$$C(T(x)) = \frac{1 - \cos \pi T(x)}{2} = \frac{1 - \cos \pi 2x}{2} = \sin^2 \pi x.$$

Exemple : la fonction logistique $L_4(x) = 4x(1-x)$ (suite)

Mesure invariante

$$\mu(A) = \lambda(C^{-1}(A)).$$

λ mesure de Lebesgue sur $\mathbb{R}$

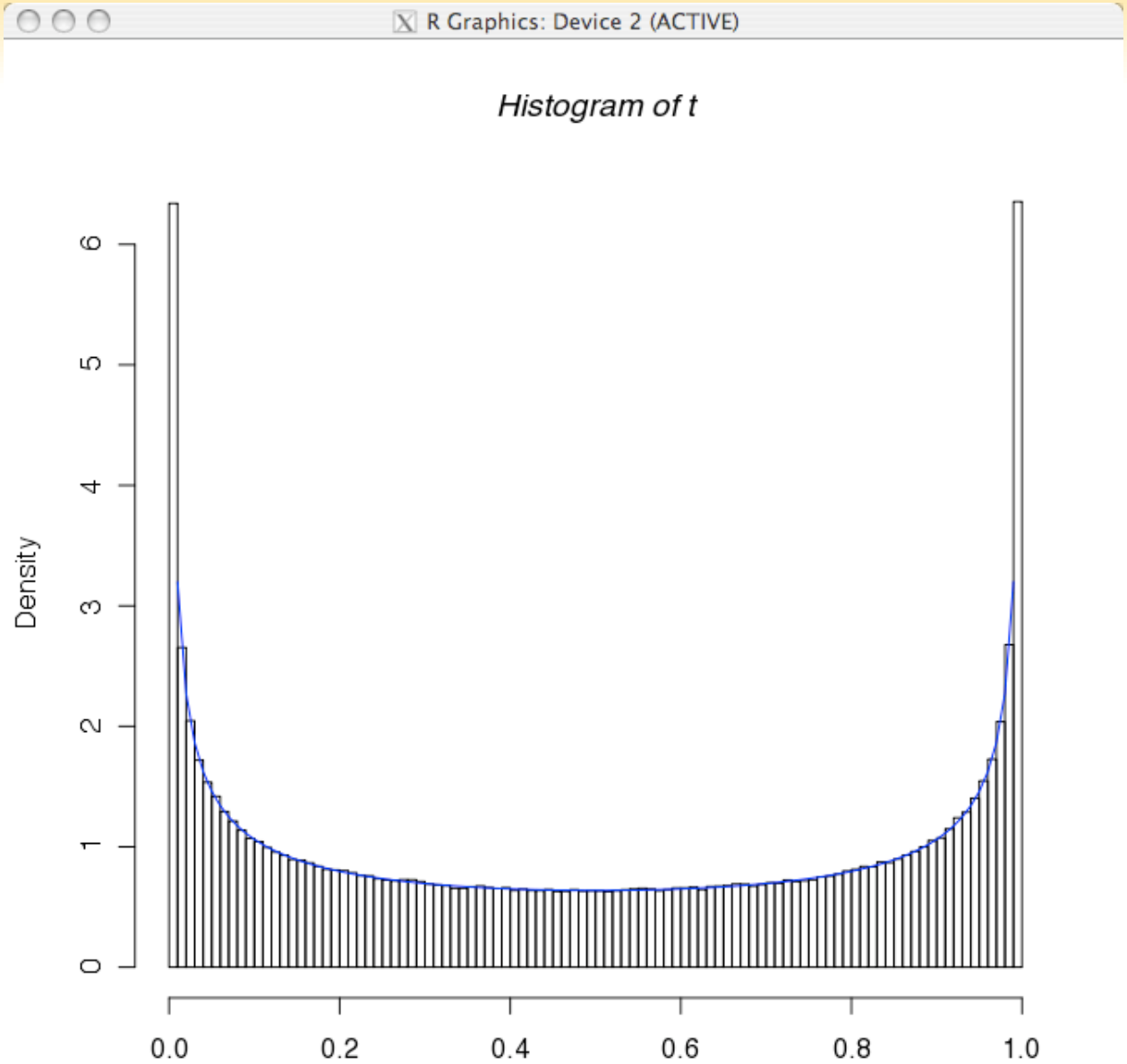
$$\begin{aligned}
\mu(L_4^{-1}(A)) &= \lambda(C^{-1}L_4^{-1}(A)),\\
&= \lambda(C^{-1}L_4^{-1}CC^{-1}(A)),\ L_4 \text{ et } T \text{ conjuguées},\\
&= \lambda(T^{-1}(C^{-1}(A))),\ \lambda \text{ mesure invariante de } T,\\
&= \lambda(C^{-1}(A)),\\
&= \mu(A).
\end{aligned}$$

Densité : $\frac{1}{\pi\sqrt{x(1-x)}}$

$$\mu(A) = \int_{C^{-1}(A)} dx = \int_A (C^{-1})' dy.$$

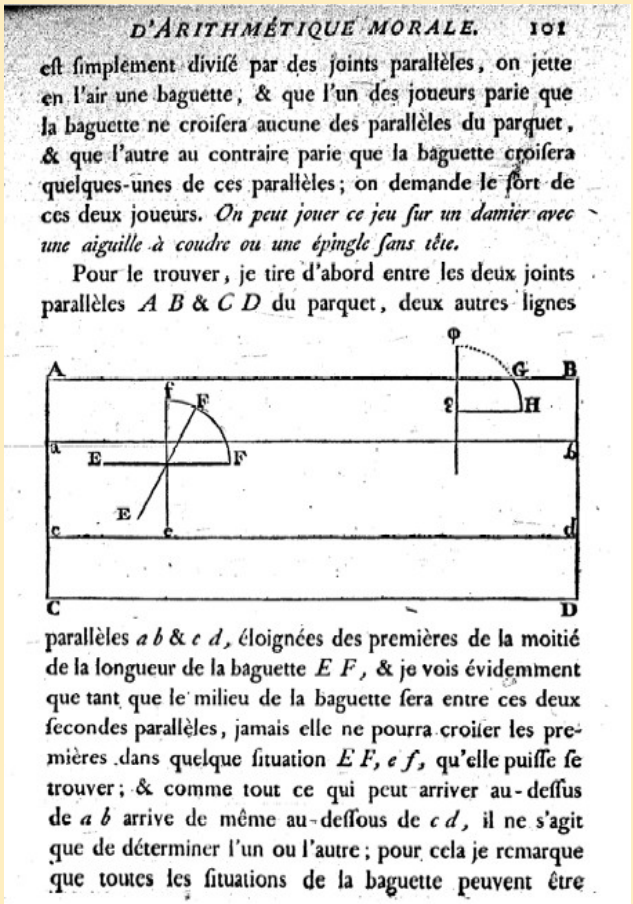
Changement de variable $y = C(x) = \frac{1-\cos \pi x}{2}$, $C^{-1}(y) = \frac{1}{\pi} arccos(1-2y)$

Exemple : la fonction logistique $L_4(x) = 4x(1-x)$ (fin)



Algorithmes numériques randomisés

Aiguille de Buffon



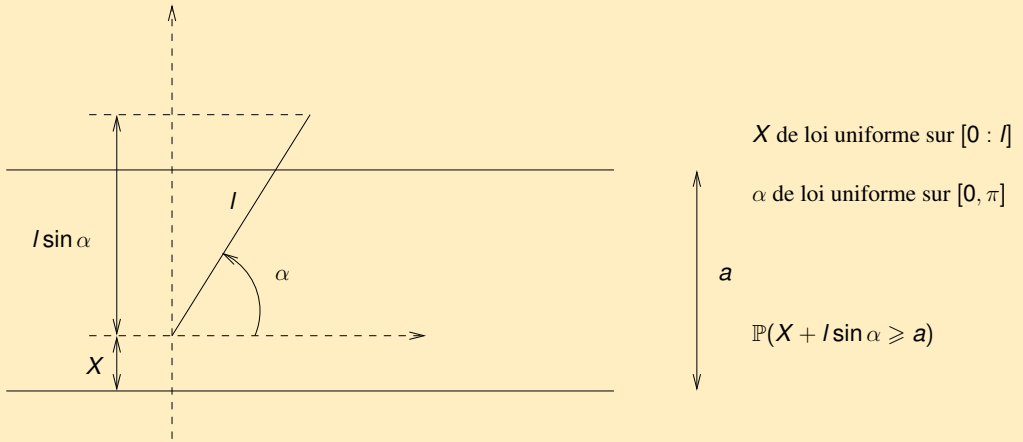
D'ARITHMÉTIQUE MORALE. 101

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

Modèle



$$\mathbb{P}(X + l\sin\alpha \leqslant a) = \frac{\int_0^\pi (a - l\sin\alpha)d\alpha}{\pi a} = \frac{2l}{\pi a}.$$

Calcul de π par la répétition d'expériences
$\longrightarrow$ Méthode de Monte-Carlo
Calcul numérique d'intégrales (grdes dim)

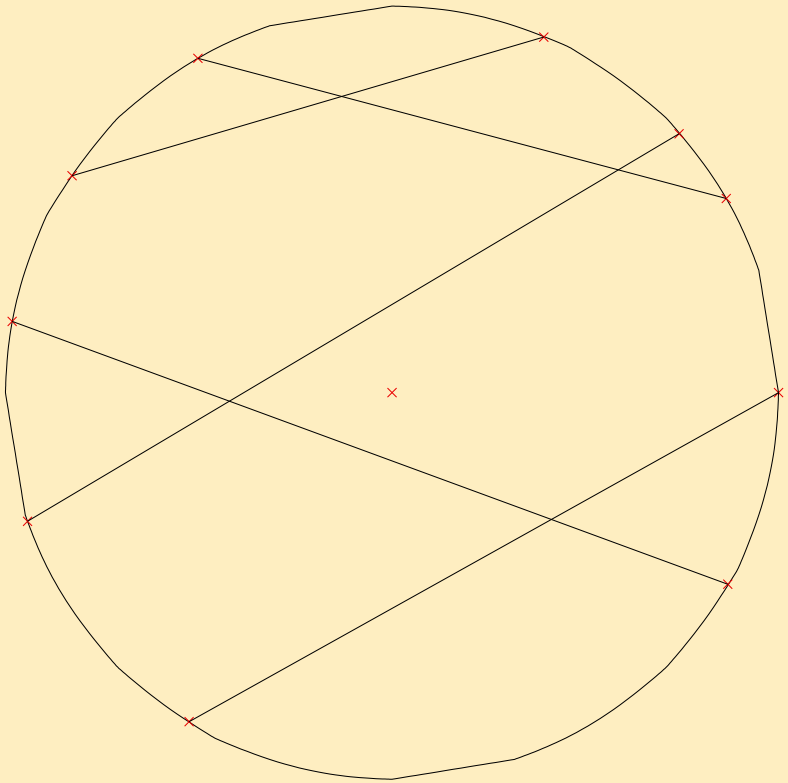
Georges Louis Leclerc Comte de Buffon (1707-1788)

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 temp rament rationaliste l'emporte alors sur sa formation philosophique, d'inspiration sceptique.

Génération d'objets géométriques

Joseph Bertrand : Générer une corde au hasard



Calculer la probabilité que la longueur de la corde dépasse la longueur du coté du triangle équilatéral inscrit dans le cercle.

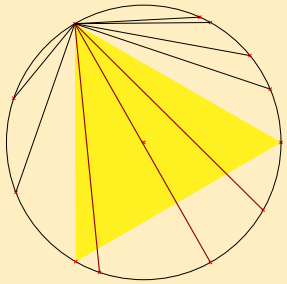
Propositions

$$p = \frac{1}{2} \quad p = \frac{1}{3} \quad p = \frac{1}{4}$$

Génération d'objets géométriques

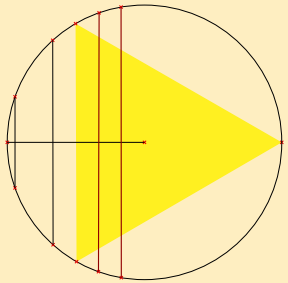
Joseph Bertrand : Générer une corde au hasard

Cercle



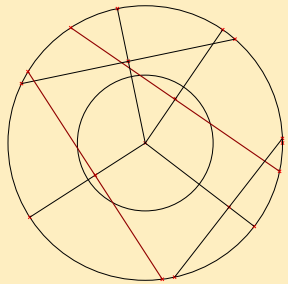
$$p = \frac{1}{3}.$$

Rayons



$$p = \frac{1}{2}.$$

Disque



$$p = \frac{1}{4}.$$

Joseph Bertrand (1822-1900)

Joseph Louis François Bertrand, habituellement appelé Joseph Bertrand, né le 11 mars 1822 à Paris, mort le 3 avril 1900 à Paris, était un mathématicien, historien des sciences et académicien français.

Enfant prodige, à onze ans il suit les cours de l'...cole Polytechnique en auditeur libre. Entre onze et dix-sept ans il obtient deux baccalauréats, une licence et le doctorat ès sciences avec une thèse sur la théorie mathématique de l'électricité, puis est admis premier au concours d'entrée 1839 de l'...cole Polytechnique. Il est ensuite reçu au concours de l'agrégation de mathématiques des facultés et premier au premier concours d'agrégation de mathématiques des lycées avec Charles Briot, ainsi qu'à l'...cole des mines. Il fut professeur de mathématiques au lycée Saint-Louis, répetiteur, examinateur puis professeur d'analyse en 1852 à l'...cole polytechnique et titulaire de la chaire de physique et mathématiques au Collège de France en 1862 en remplacement de Jean-Baptiste Biot.
En 1845, en analysant une table de nombres premiers jusqu'à 6 000 000, il fait la conjecture qu'il y a toujours au moins un nombre premier entre n et 2n-2 pour tout n plus grand que 3. Tchebychev a démontré cette conjecture, le postulat de Bertrand, en 1850.
Pour l'étude de la convergence des series numériques, il mit au point un critère de comparaison plus fin que le critère de Riemann.

$$\sum \frac{1}{n^{\alpha} \log n^{\beta}} \text{ converge ssi } (\alpha, \beta) \geqslant (1, 1).$$

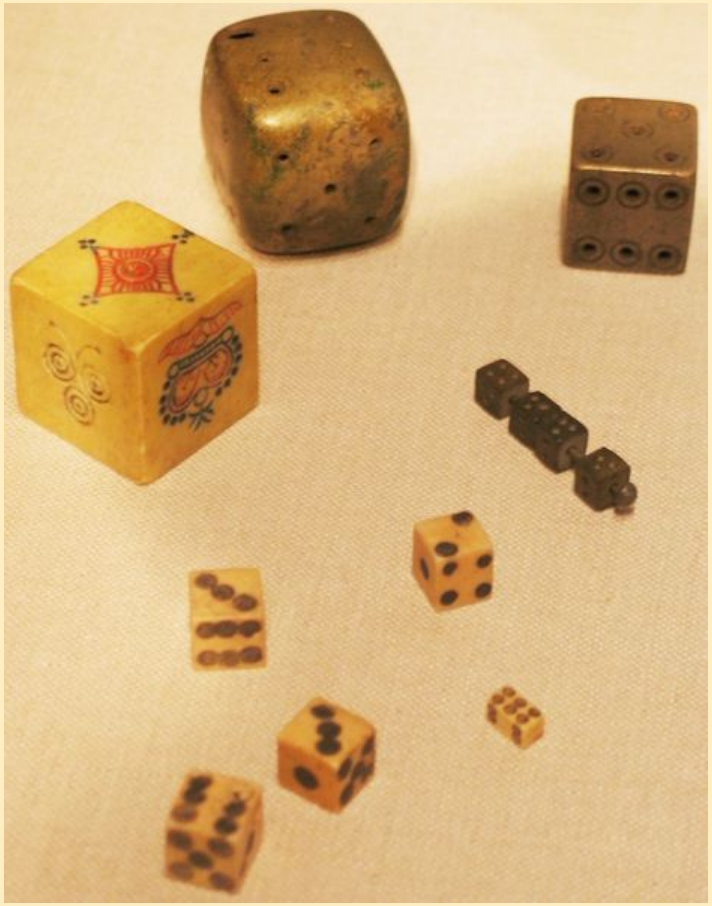
Machine à fabriquer du hasard

Loterie

- Roue sur pivot, secteurs
  Principe : système dynamique chaotique avec amortissement
- Pièces, dés
  Principe : système complexe chaotique
- Machine à boule, loto, roulette
- Mélange de cartes
  Principe : coupes permutations mélanges

germe : action d'un individu

Machines



Hasard pré-fabriqué

Rand corporation

Tables de chiffres aléatoires

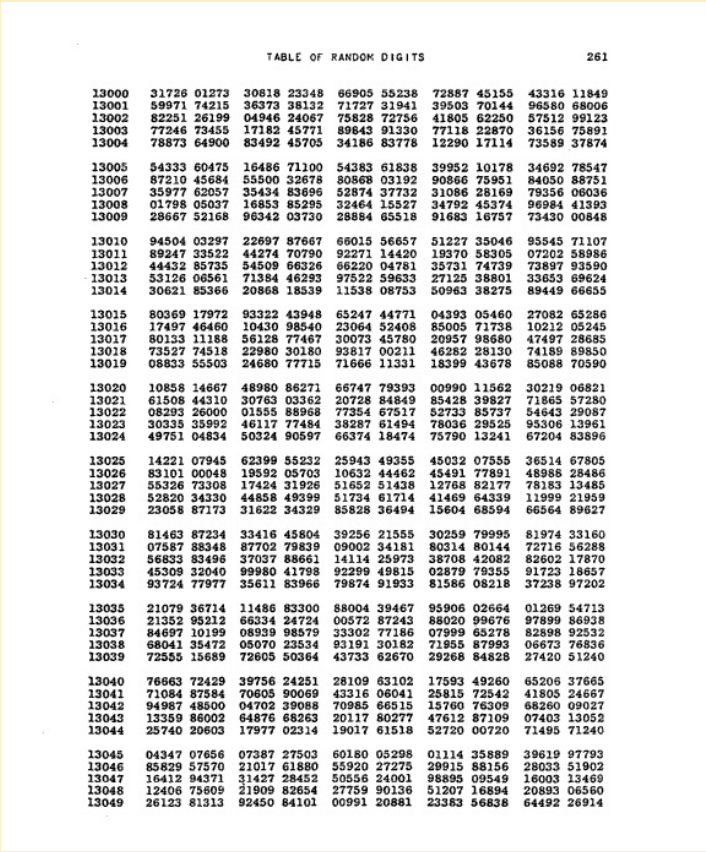


TABLE OF RANDOM DIGITS 261

13000	31726	01273	30818	23348	66905	55238	72887	45155	43316	11849
13001	59971	74215	36373	38132	71727	31941	39503	70144	96580	68006
13002	82251	26199	04946	24067	75828	72756	41805	62250	57512	99123
13003	77246	73455	17182	45771	89643	91330	77118	22870	36156	75891
13004	78873	64900	83492	45705	34186	83778	12290	17114	73589	37874
13005	54333	60475	16486	71100	54383	61838	39952	10178	34692	78547
13006	87210	45684	55500	32678	80868	03192	90866	75951	84050	88751
13007	35977	62057	35434	83696	52874	37732	31086	28169	79356	06036
13008	01798	05037	16853	85295	32464	15527	34792	45374	96984	41393
13009	28667	52168	96342	03730	28884	65518	91683	16757	73430	00848
13010	94504	03297	22697	87667	66015	56657	51227	35046	95545	71107
13011	89247	33522	44274	70790	92271	14420	19370	58305	07202	58986
13012	44432	85735	54509	66326	66220	04781	35731	74739	73897	93590
13013	53126	06561	71384	46293	97522	59633	27125	38801	33653	69624
13014	30621	85366	20868	18539	11538	08753	50963	38275	89449	66655
13015	80369	17972	93322	43948	65247	44771	04393	05460	27082	65286
13016	17497	46460	10430	98540	23064	52408	85005	71738	10212	05245
13017	80133	11188	56128	77467	30073	45780	20957	98680	47497	28685
13018	73527	74518	22980	30180	93817	00211	46282	28130	74189	89850
13019	08833	55503	24680	77715	71666	11331	18399	43678	85088	70590
13020	10858	14667	48980	86271	66747	79393	00990	11562	30219	06821
13021	61508	44310	30763	03362	20728	84849	85428	39827	71865	57280
13022	08293	26000	01555	88968	77354	67517	52733	85737	54643	29087
13023	30335	35992	46117	77484	38287	61494	78036	29525	95306	13961
13024	49751	04834	50324	90597	66374	18474	75790	13241	67204	83896
13025	14221	07945	62399	55232	25943	49355	45032	07555	36514	67805
13026	83101	00048	19592	05703	10632	44462	45491	77891	48988	28486
13027	55326	73308	17424	31926	51652	51438	12768	82177	78183	13485
13028	52820	34330	44858	49399	51734	61714	41469	64339	11999	21959
13029	23058	87173	31622	34329	85828	36494	15604	68594	66564	89627
13030	81463	87234	33416	45804	39256	21555	30259	79995	81974	33160
13031	07587	88348	87702	79839	09002	34181	80314	80144	72716	56288
13032	56833	83496	37037	88661	14114	25973	38708	42082	82602	17870
13033	45309	32040	99980	41798	92299	49815	02879	79355	91723	18657
13034	93724	77977	35611	83966	79874	91933	81586	08218	37238	97202
13035	21079	36714	11486	83300	88004	39467	95906	02664	01269	54713
13036	21352	95212	66334	24724	00572	87243	88020	99676	97899	86928
13037	84697	10199	08939	98579	33302	77186	07999	65278	82898	92532
13038	68041	35472	05070	23534	93191	30182	71955	87993	06673	76836
13039	72555	15689	72605	50364	43733	62670	29268	84828	27420	51240
13040	76663	72429	39756	24251	28109	63102	17593	49260	65206	37665
13041	71084	87584	70605	90069	43316	06041	25815	72542	41805	24667
13042	94987	48500	04702	39088	70985	66515	15760	76309	68260	09027
13043	13359	86002	64876	68263	20117	80277	47612	87109	07403	13052
13044	25740	20603	17977	02314	19017	61518	52720	00720	71495	71240
13045	04347	07656	07387	27503	60180	05298	01114	35889	39619	97793
13046	85829	57570	21017	61880	55920	27275	29915	88156	28033	51902
13047	16412	94371	31427	28452	50556	24001	98895	09549	16003	13469
13048	12406	75609	21909	82654	27759	90136	51207	16894	20893	06560
13049	26123	81313	92450	84101	00991	20881	23383	56838	64492	26914

Bits aléatoires

- RandomNumber.org
- Hotbits
  `http://www.fourmilab.ch/hotbits/`
- Générateur de Marsaglia
  `http://www.stat.fsu.edu/pub/diehard/`
- New dice roller :
  `http://gamesbyemail.com/News/DiceOMatic`
- etc.

Méthode de Monte-Carlo

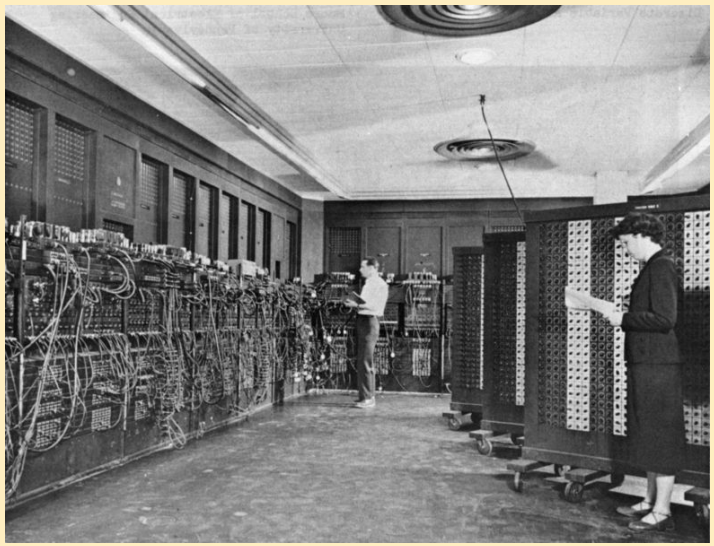
Intégration numérique

Projet Manhattan Simulation de réaction nucléaire $\Rightarrow$ équation aux dérivées partielles

$$I = \int_a^b f(x)dx \simeq \frac{1}{N}\sum_{i=1} f(U_i).$$

Stanislaw Marcin Ulam (math)
Enrico Fermi (physique)
John von Neumann (math app)
Nicholas Metropolis (physique)

Ordinateur : Eniac 1943

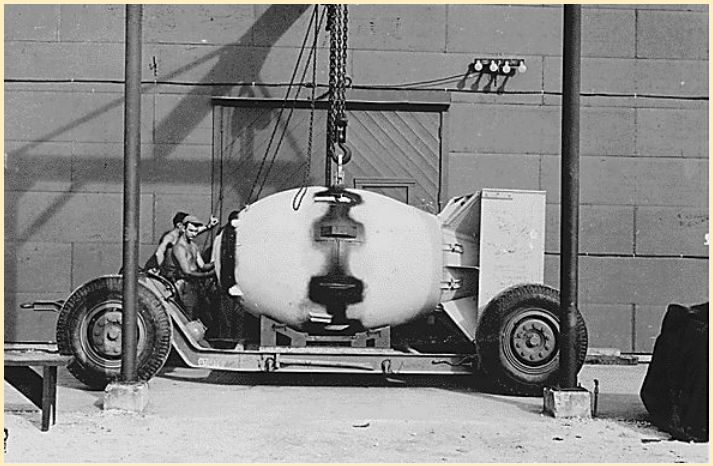


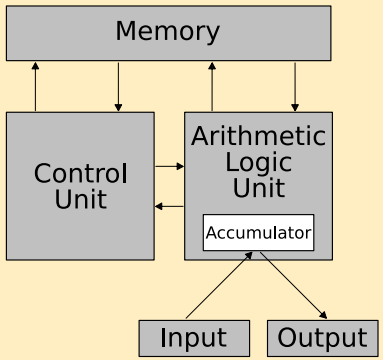
Electronic Numerical Integrator And Computer
John Mauchly et J. Presper Eckert
University of Pennsylvania.

John von Neuman (1903-1957)

Mathématicien américain d'origine hongroise. Il a apporté d'importantes contributions tant en mécanique quantique, qu'en analyse fonctionnelle, en théorie des ensembles, en informatique, en sciences économiques ainsi que dans beaucoup d'autres domaines des mathématiques et de la physique. Il a de plus participé aux programmes militaires américains.

Architecture des ordinateurs



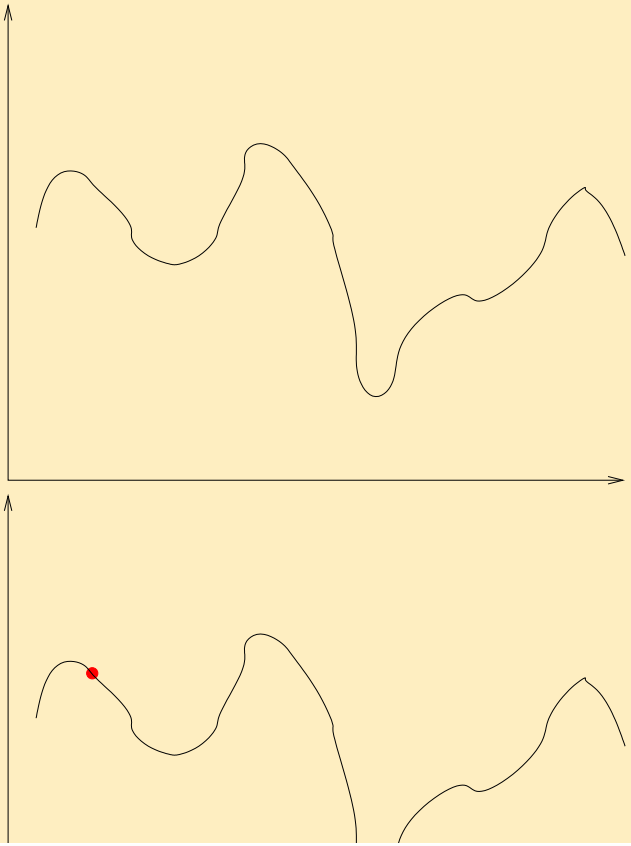


Nicholas Metropolis (1915-1999)

Recuit simulé

Convergence vers un minimum global par une descente de gradient stochastique.

$$X_{n+1} = X_n - \vec{grad}\Phi(X_n)\Delta(Random).$$



Générateur pseudo-aléatoire (1)

Milieu des carrés

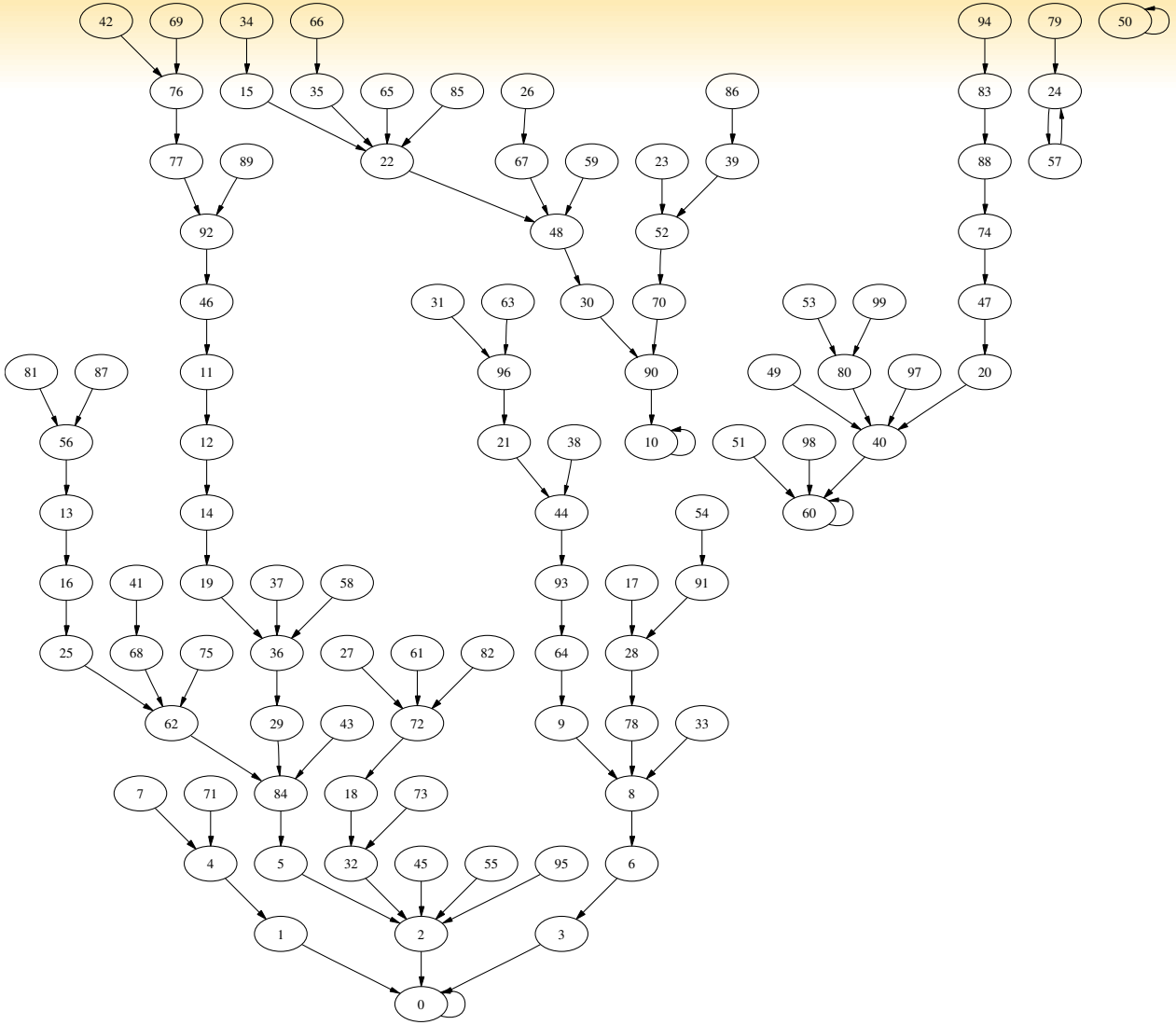
Objets : entiers
Idée : mélanger
Algorithme de génération

$x \leftarrow germe$
repeat
  $y \leftarrow x^2$
  $x \leftarrow milieu(y)$
  $ecrire(x)$
until Fin de simulation

Exemple

$$
\begin{aligned}
x_0 = 5869 &\rightarrow x_0^2 = 34|4451|61 \\
x_1 = 4451 &\rightarrow x_1^2 = 19|8114|01 \\
x_2 = 8114 &\rightarrow x_2^2 = 65|8369|96 \\
x_3 = 8369 &\rightarrow x_3^2 = 70|0401|61 \\
x_4 = 0401 &\rightarrow x_4^2 = 00|1608|01 \\
x_5 = 1608 &\rightarrow x_5^2 = 02|5856|64 \\
x_6 = 5856 &\rightarrow x_6^2 = 34|2927|36 \\
x_7 = 5856 &\rightarrow \cdots
\end{aligned}
$$

Milieu des carrés



Encore raté !

Générateur pseudo-aléatoire (2)

Transformation modulo

Transformation linéaire
Objets : entiers $\{0, \cdots m-1\}$
Données : $a, b \in \{0, \cdots m-1\}$
$x_{n+1} = a * x_n + b \mod m$

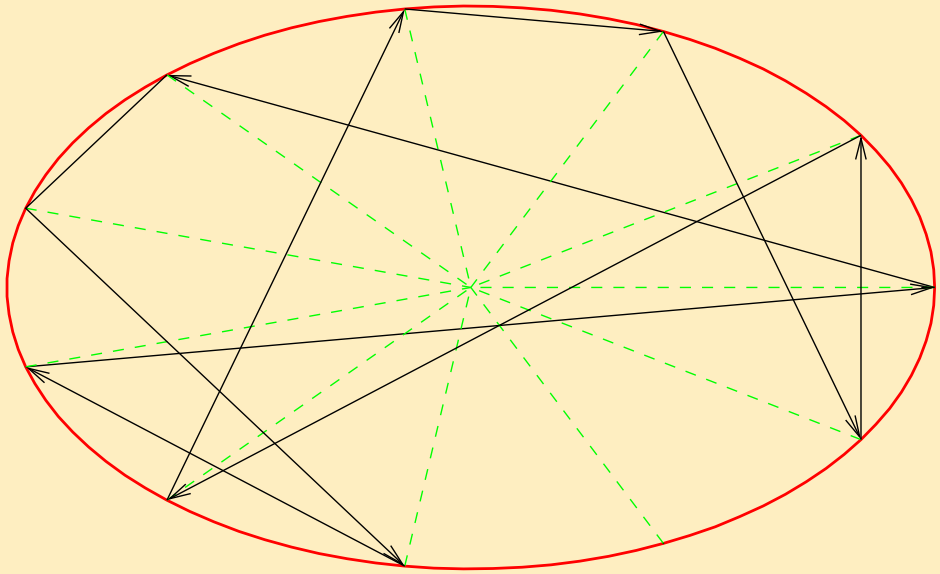
$x \leftarrow germe$
repeat
  $x \leftarrow a * x + b \mod n$
  $ecrire(x)$
until Fin de simulation

Exemple

$a = 11, b = 1, m = 71$

$$17 \to 46 \to 10 \to 40 \to 15 \to 24 \to \cdots$$

Diagramme $x_{n+1} = 3 * x_n + 4 \mod 11$



Générateurs congruents

Trouver un cycle maximum

Theorem

Théorème Hull-Dobell, (1962) Soit la suite (x_n) *produite par l'algorithme* $x_{n+1} = ax_n + b \mod m$. *Alors le cycle maximal est de longueur m si et seulement si les trois hypothèses suivantes sont vérifiés:*

1. $PGCD(a, m) = 1$, $PGCD(b, m) = 1$;
2. *si un nombre premier p divise m, alors p divise* $a - 1$;
3. *si* 4 *divise m, alors* 4 *divise* $a - 1$.

Donne l'uniformité, pas le "mélange"

Exemples de générateurs congruents

$$x_{n+1} = 7^5 x_n \mod 2^{31} - 1, \text{ (générateur IBM)}$$

$$x_{n+1} = 427419669081 x_n \mod 999999999989,$$

(générateur Maple, 999999999989 est premier)

$$x_{n+1} = 3^{15} x_n \mod 2^{32},$$

$$x_{n+1} = 3 + 2^{16} x_n \mod 2^{31},$$

$$x_{n+1} = 13^{13} x_n \mod 2^{59},$$

$$x_{n+1} = 24298 x_n + 99991 \mod 199017,$$

dont les périodes respectives sont:

$$2^{30} = 1\,073\,741\,824,$$

$$2^{29} = 536\,870\,912,$$

$$2^{57} = 144\,115\,188\,075\,855\,872,$$

$$199\,017$$

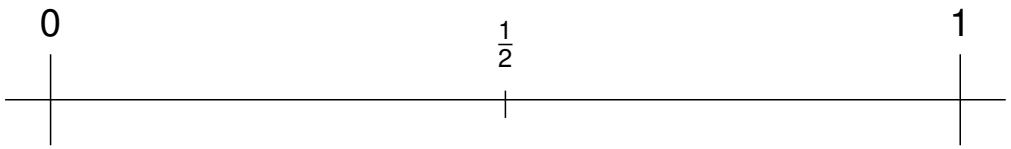
Générateurs de bits aléatoires

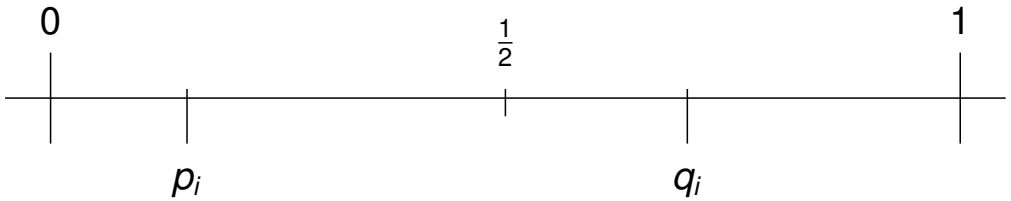
$x = \{x_1, x_2, \cdots, x_n, \cdots\}$ et $y = \{y_1, y_2, \cdots, y_n, \cdots\}$
suites de bits “au hasard”

Théorème : Vive le *XOR* (ou exclusif)

La suite $z = \{z_1, z_2, \cdots, z_n, \cdots\}$ avec $z_i = x_i$ *XOR* y_i est meilleure que x et que y.
Hypothèse x_i et y_i indépendantes.

Preuve :





Générateurs de bits aléatoires (suite)

Générateur de bits indépendants mais *biaisé* : $p = \mathbb{P}(x_i = 1)$
$x = \{x_1, x_2, \cdots, x_n, \cdots\}$

$$y_n = x_{nk+1} \; XOR \; x_{nk+2} \; XOR \; \cdots \; XOR \; x_{n(k+1)}$$

$$\mathbb{P}(y_n = 1) = \frac{1}{2}\left(1 - (1-2p)^k\right) \overset{exponentiellement}{\longrightarrow} \frac{1}{2}.$$

Approximation de la pièce sans biais (erreur contrôlée)
Ex : $p = \frac{1}{3}$, $k = 10$

$$\mathbb{P}(y_n = 1) \simeq \frac{1}{2} \pm 10^{-5}.$$

Générateurs de bits aléatoires (suite et fin)

Générateur de bits indépendants mais *biaisé* : $p = \mathbb{P}(x_i = 1)$
$x = \{x_1, x_2, \cdots, x_n, \cdots\}$
Réaliser une pièce sans biais

repeat
  X= piece();
  Y= piece();
until (X≠Y)
retourne X;

Algorithme à base de rejet : $\mathbb{P}(\textit{acceptation}) = 2p(1-p)$
Nombre moyen d'itérations : $\overline{N} = \frac{1}{2p(1-p)}$
Ex : $p = \frac{1}{3}$,

$$\overline{N} = \frac{9}{4} = 2,25.$$

Générateur pseudo-aléatoire

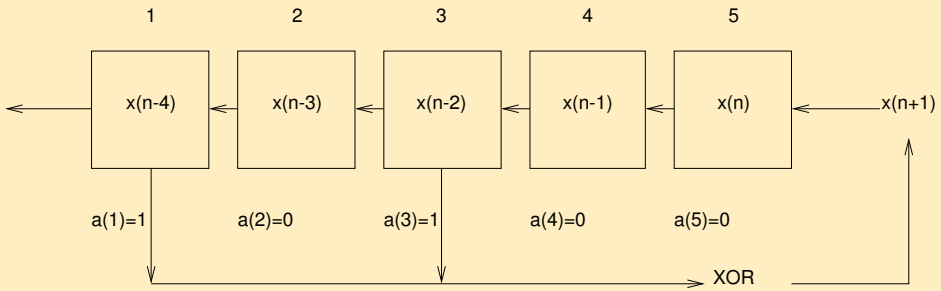
Utiliser le *XOR* dans l'algorithme

Tausworthe (1965)

mot binaire initial (le germe) $x^0 = (x_{-m+1}, \ldots x_{-1}, x_0)$,
récurrence:

$$x_{n+1} = a_1 x_{n-m+1} + a_2 x_{n-m+1} + \ldots + a_m x_n \mod 2$$

$a_1, a_2, \cdots, a_m$ fixés
Registre à décalage rebouclé



Générateurs pseudo-aléatoire (fin)

Utiliser le *XOR* dans l'algorithme

Mersenne Twister (1998)

$$x_n = x_{n-(N-M)} \oplus (x^U_{n-N} | x^L_{n-N+1}) A$$

avec le jeu de paramètres adéquat :
période = $2^{19937} - 1$

Blum Blum Shub Generator (1986)

$$x_{n+1} = x_n^2 \bmod M$$

Très mauvais du point de vue statistique
Excellent pour la cryptographie

Synthèse

Compréhension

1. dynamique déterministe chaotique $\Rightarrow$ approche probabiliste
2. théorie ergodique (invariants) $\Rightarrow$ détermination du phénomène

Mise en œuvre

1. dynamique déterministe chaotique $\Rightarrow$ objet monstrueux à éviter
2. construction de systèmes chaotiques $\Rightarrow$ calcul de valeurs déterministes

Amusez-vous...

Pour aller plus loin...

- Le calcul et l'imprévu Ivar Eckeland Points Sciences
- Delahaye, J.-P. (1994b), Le complexe surgit-il du simple ?, Pour la Science (203), 102-107.
- L'intelligence et le calcul Jean-Paul Delahaye (2002)
- Poincaré, H. (1912), Calcul des probabilités, Gauthier-Villars, Paris.
- Introduction to Ergodic Theory Ya G. Sinai, V. Scheffer, Princeton University Press (1977)
- Probability and Measure P. Billingsley (Wiley-Interscience1995)
- Essentials of Stochastic Processes R. Durrett Springer (1999)
- Probability, L. Breiman Addison-Wesley (1968)

Pour aller plus loin (2) ...

Sites Web

Pour les biographies
- fr.wikipedia.org
- http://www-groups.dcs.st-and.ac.uk/ history/

`http://www.gap-system.org/~history/`

La page de Delahaye

`http://www2.lifl.fr/~delahaye/`