Random machines

How algorithms emulate randomness

Jean-Marc Vincent[1]

[1]Laboratoire LIG
Jean-Marc.Vincent@imag.fr

Flip a coin with a computer

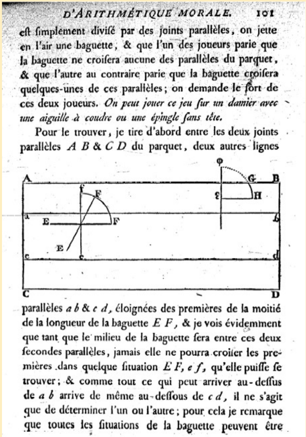
Outline of the lecture

1 **Random machines**
- Why generate random numbers ?
- Random machines
- Pseudo-random generators

2 **and Human mind**
- Randomness detection
- Generate randomness

Randomized numerical algorithms

Buffon's needle



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

Model

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

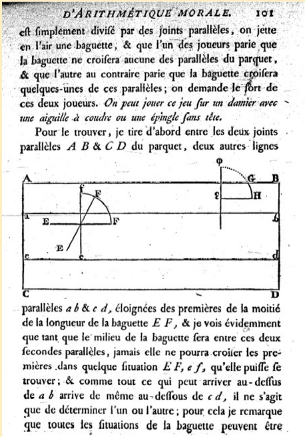
Computation of π by repeating experiments

$\longrightarrow$ Monte-Carlo methods

Computation of integrals (high dimension)

Randomized numerical algorithms

Buffon's needle



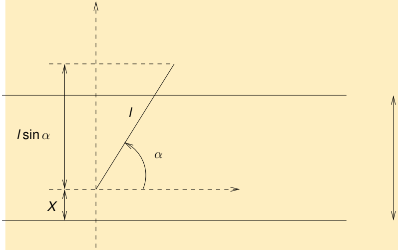
D'ARITHMÉTIQUE MORALE. 101

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

Model



X de loi uniforme sur $[0 : l]$

α de loi uniforme sur $[0, \pi]$

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

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

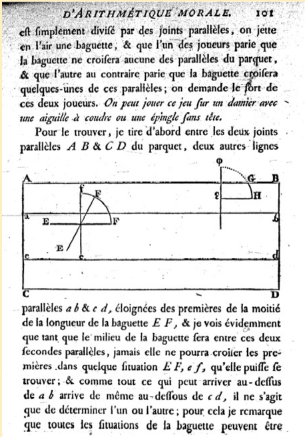
Computation of π by repeating experiments

$\longrightarrow$ Monte-Carlo methods

Computation of integrals (high dimension)

Randomized numerical algorithms

Buffon's needle



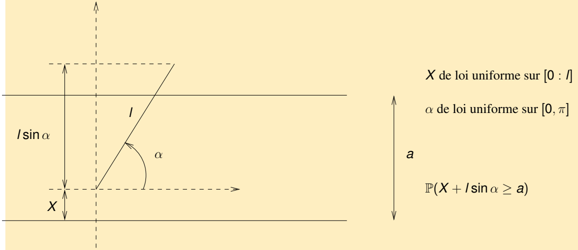
D'ARITHMÉTIQUE MORALE. 101

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

Model



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

Computation of π by repeating experiments

$\longrightarrow$ Monte-Carlo methods

Computation of integrals (high dimension)

Georges Louis Leclerc Comte de Buffon (1707-1788)

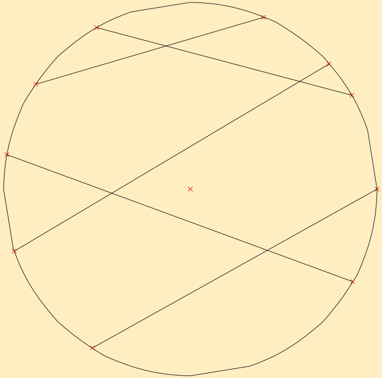
Georges-Louis Leclerc, comte de Buffon (7 septembre 1707 à Montbard - 16 avril 1788 à Paris), est un naturaliste, mathématicien, biologiste, cosmologiste et écrivain français. Ses théories ont influencé deux générations de naturalistes, parmi lesquels notamment Jean-Baptiste de Lamarck et Charles Darwin. 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.

Generation of geometrical objects

Joseph Bertrand : generate a random chord



Compute the probability that the length of the chord is greater than the length of the side of an equilateral triangle inscribed in the circle.

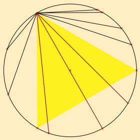
Alternatives

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

Generation of geometrical objects

Joseph Bertrand : generate a random chord

Circle



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

Rays

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

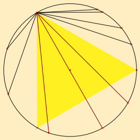
Disc

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

Generation of geometrical objects

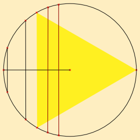
Joseph Bertrand : generate a random chord

Circle



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

Rays



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

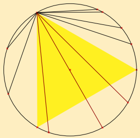
Disc

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

Generation of geometrical objects

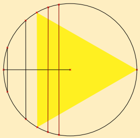
Joseph Bertrand : generate a random chord

Circle



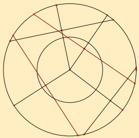
$$p = \frac{1}{3}.$$

Rays



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

Disc



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

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'École 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'École 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'École des mines. Il fut professeur de mathématiques au lycée Saint-Louis, répetiteur, examinateur puis professeur d'analyse en 1852 à l'École 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.

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

Outline of the lecture

1 Random machines
- Why generate random numbers ?
- Random machines
- Pseudo-random generators

2 and Human mind
- Randomness detection
- Generate randomness

Physical instruments

Lottery

- Wheel, sectors
  Dynamical amortized chaotic system
- Coins, dices
  Chaotic system
- Bingo, roulette
- Card shuffling
  repeated perturbed permutations

seed : human action

Machines

Physical instruments

Lottery

- Wheel, sectors
  Dynamical amortized chaotic system
- Coins, dices
  Chaotic system
- Bingo, roulette
- Card shuffling
  repeated perturbed permutations

seed : human action

Machines

Pre-computed randomness

Rand corporation

Tables with random figures

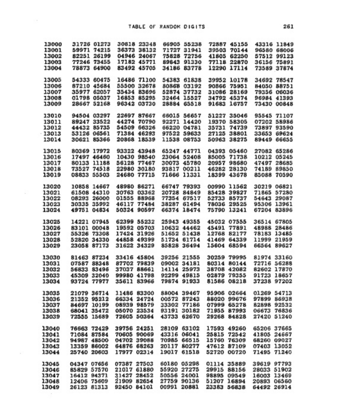


TABLE OF RANDOM DIGITS 261

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	89843	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	86938
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

Random bits

- RandomNumber.org
- Hotbits
  http ://www.fourmilab.ch/hotbits/
- Marsaglia's generator
  http ://www.stat.fsu.edu/pub/diehard/
- etc.

Pre-computed randomness

Rand corporation

Tables with random figures

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	89843	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	86938
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

Random bits

- RandomNumber.org
- Hotbits
  http ://www.fourmilab.ch/hotbits/
- Marsaglia's generator
  http ://www.stat.fsu.edu/pub/diehard/
- etc.

Outline of the lecture

1. **Random machines**
   - Why generate random numbers ?
   - Random machines
   - Pseudo-random generators
2. **and Human mind**
   - Randomness detection
   - Generate randomness

Monte-Carlo method

Numeric integration

Manhattan Project Simulation of nuclear chain reaction => solve partial differential equations

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

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

Computer : Eniac 1943

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

Monte-Carlo method

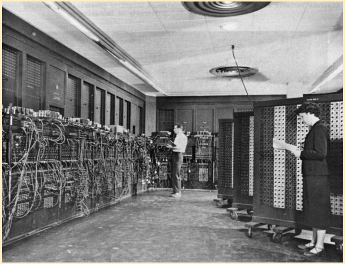
Numeric integration

Manhattan Project Simulation of nuclear chain reaction => solve partial differential equations

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

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

Computer : Eniac 1943



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

John von Neuman (1903-1957)

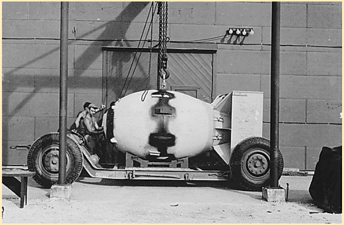
Mathématicien américain d'origine hongroise. Il a apporté d'importantes contributions tant en mécanique quantique, qu'en analyse fonctionnelle, en théorie des ensembles, en informatique, en sciences économiques ainsi que dans beaucoup d'autres domaines des mathématiques et de la physique. Il a de plus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

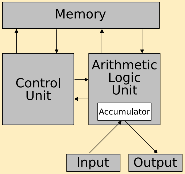
Computer Architecture

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.

Computer Architecture





Nicholas Metropolis (1915-1999)

Nick Metropolis

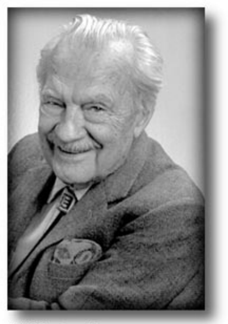
Metropolis contributed several original ideas to mathematics and physics. Perhaps the most widely known is the Monte Carlo method. Also, in 1953 Metropolis co-authored the first paper on a technique that was central to the method known now as simulated annealing. He also developed an algorithm (the Metropolis algorithm or Metropolis-Hastings algorithm) for generating samples from the Boltzmann distribution, later generalized by W.K. Hastings.

Simulated annealing

Convergence to a global minimum by a control stochastic gradient algorithm

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

Nicholas Metropolis (1915-1999)



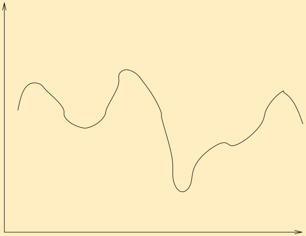
Nick Metropolis

Metropolis contributed several original ideas to mathematics and physics. Perhaps the most widely known is the Monte Carlo method. Also, in 1953 Metropolis co-authored the first paper on a technique that was central to the method known now as simulated annealing. He also developed an algorithm (the Metropolis algorithm or Metropolis-Hastings algorithm) for generating samples from the Boltzmann distribution, later generalized by W.K. Hastings.

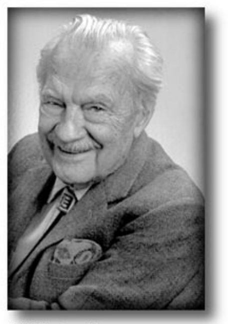
Simulated annealing

Convergence to a global minimum by a control stochastic gradient algorithm

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



Nicholas Metropolis (1915-1999)



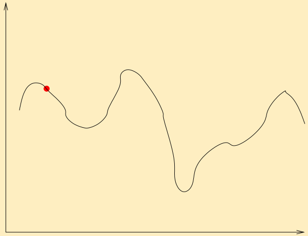
Nick Metropolis

Metropolis contributed several original ideas to mathematics and physics. Perhaps the most widely known is the Monte Carlo method. Also, in 1953 Metropolis co-authored the first paper on a technique that was central to the method known now as simulated annealing. He also developed an algorithm (the Metropolis algorithm or Metropolis-Hastings algorithm) for generating samples from the Boltzmann distribution, later generalized by W.K. Hastings.

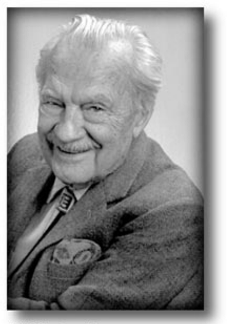
Simulated annealing

Convergence to a global minimum by a control stochastic gradient algorithm

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



Nicholas Metropolis (1915-1999)



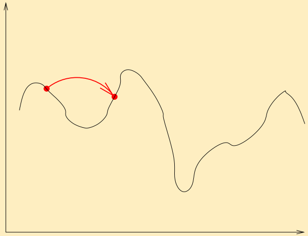
Nick Metropolis

Metropolis contributed several original ideas to mathematics and physics. Perhaps the most widely known is the Monte Carlo method. Also, in 1953 Metropolis co-authored the first paper on a technique that was central to the method known now as simulated annealing. He also developed an algorithm (the Metropolis algorithm or Metropolis-Hastings algorithm) for generating samples from the Boltzmann distribution, later generalized by W.K. Hastings.

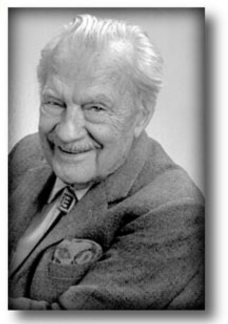
Simulated annealing

Convergence to a global minimum by a control stochastic gradient algorithm

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



Nicholas Metropolis (1915-1999)



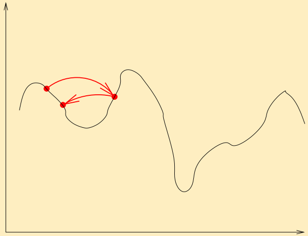
Nick Metropolis

Metropolis contributed several original ideas to mathematics and physics. Perhaps the most widely known is the Monte Carlo method. Also, in 1953 Metropolis co-authored the first paper on a technique that was central to the method known now as simulated annealing. He also developed an algorithm (the Metropolis algorithm or Metropolis-Hastings algorithm) for generating samples from the Boltzmann distribution, later generalized by W.K. Hastings.

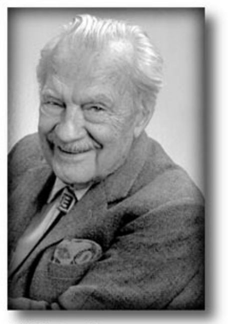
Simulated annealing

Convergence to a global minimum by a control stochastic gradient algorithm

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



Nicholas Metropolis (1915-1999)



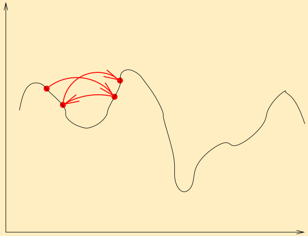
Nick Metropolis

Metropolis contributed several original ideas to mathematics and physics. Perhaps the most widely known is the Monte Carlo method. Also, in 1953 Metropolis co-authored the first paper on a technique that was central to the method known now as simulated annealing. He also developed an algorithm (the Metropolis algorithm or Metropolis-Hastings algorithm) for generating samples from the Boltzmann distribution, later generalized by W.K. Hastings.

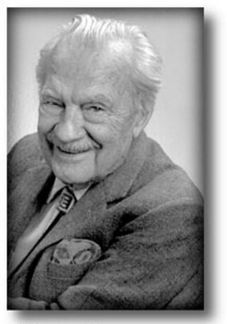
Simulated annealing

Convergence to a global minimum by a control stochastic gradient algorithm

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



Nicholas Metropolis (1915-1999)



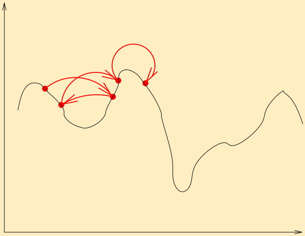
Nick Metropolis

Metropolis contributed several original ideas to mathematics and physics. Perhaps the most widely known is the Monte Carlo method. Also, in 1953 Metropolis co-authored the first paper on a technique that was central to the method known now as simulated annealing. He also developed an algorithm (the Metropolis algorithm or Metropolis-Hastings algorithm) for generating samples from the Boltzmann distribution, later generalized by W.K. Hastings.

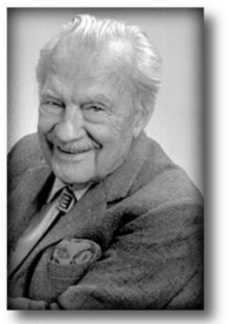
Simulated annealing

Convergence to a global minimum by a control stochastic gradient algorithm

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



Nicholas Metropolis (1915-1999)



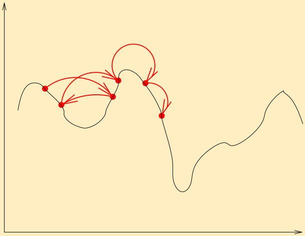
Nick Metropolis

Metropolis contributed several original ideas to mathematics and physics. Perhaps the most widely known is the Monte Carlo method. Also, in 1953 Metropolis co-authored the first paper on a technique that was central to the method known now as simulated annealing. He also developed an algorithm (the Metropolis algorithm or Metropolis-Hastings algorithm) for generating samples from the Boltzmann distribution, later generalized by W.K. Hastings.

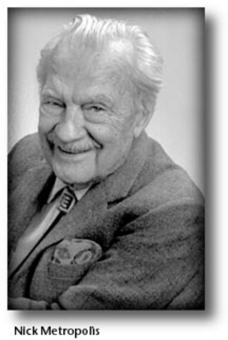
Simulated annealing

Convergence to a global minimum by a control stochastic gradient algorithm

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



Nicholas Metropolis (1915-1999)

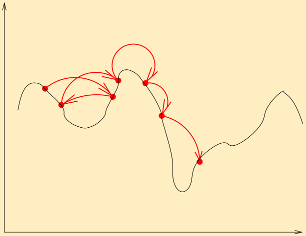


Metropolis contributed several original ideas to mathematics and physics. Perhaps the most widely known is the Monte Carlo method. Also, in 1953 Metropolis co-authored the first paper on a technique that was central to the method known now as simulated annealing. He also developed an algorithm (the Metropolis algorithm or Metropolis-Hastings algorithm) for generating samples from the Boltzmann distribution, later generalized by W.K. Hastings.

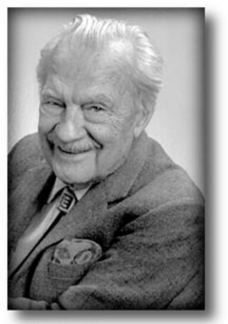
Simulated annealing

Convergence to a global minimum by a control stochastic gradient algorithm

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



Nicholas Metropolis (1915-1999)



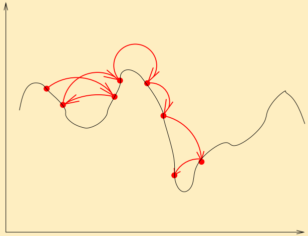
Nick Metropolis

Metropolis contributed several original ideas to mathematics and physics. Perhaps the most widely known is the Monte Carlo method. Also, in 1953 Metropolis co-authored the first paper on a technique that was central to the method known now as simulated annealing. He also developed an algorithm (the Metropolis algorithm or Metropolis-Hastings algorithm) for generating samples from the Boltzmann distribution, later generalized by W.K. Hastings.

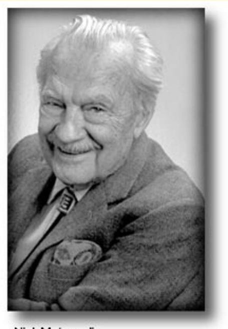
Simulated annealing

Convergence to a global minimum by a control stochastic gradient algorithm

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



Nicholas Metropolis (1915-1999)

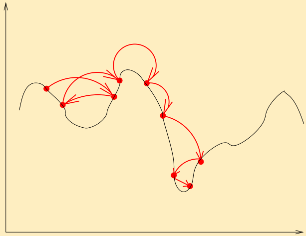


Metropolis contributed several original ideas to mathematics and physics. Perhaps the most widely known is the Monte Carlo method. Also, in 1953 Metropolis co-authored the first paper on a technique that was central to the method known now as simulated annealing. He also developed an algorithm (the Metropolis algorithm or Metropolis-Hastings algorithm) for generating samples from the Boltzmann distribution, later generalized by W.K. Hastings.

Simulated annealing

Convergence to a global minimum by a control stochastic gradient algorithm

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



Pseudo-random generator (1)

Middle of squares

Objects : integers
Idea : shuffle procedure
Generation algorithm

$x \leftarrow seed$
repeat
$y \leftarrow x^2$
$x \leftarrow middle(y)$
$write(x)$
until End of simulation

Example

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

Pseudo-random generator (1)

Middle of squares

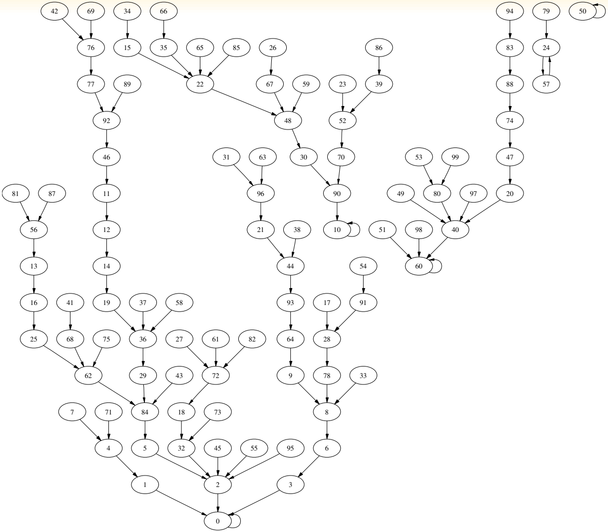
Objects : integers
Idea : shuffle procedure
Generation algorithm

$x \leftarrow seed$
repeat
  $y \leftarrow x^2$
  $x \leftarrow middle(y)$
  $write(x)$
until End of simulation

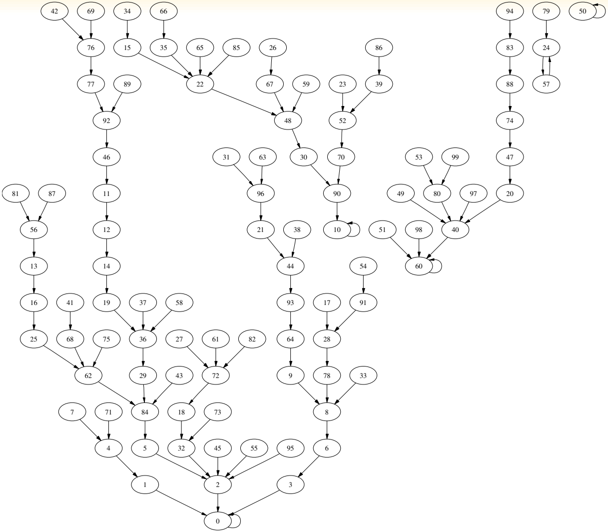
Example

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

Middle of squares



Middle of squares



Pseudo-random generator (2)

Modulo transform

Linear transform
Objets : integers
$\{0, \cdots m-1\}$
Parameters :
$a, b \in \{0, \cdots m-1\}$
$x_{n+1} = a * x_n + b \mod m$

$x \leftarrow seed$
repeat
$x \leftarrow a * x + b \mod n$
$write(x)$
until End of simulation

Example

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

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

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

Pseudo-random generator (2)

Modulo transform

Linear transform
Objets : integers
$\{0, \cdots m-1\}$
Parameters :
$a, b \in \{0, \cdots m-1\}$
$x_{n+1} = a * x_n + b \mod m$

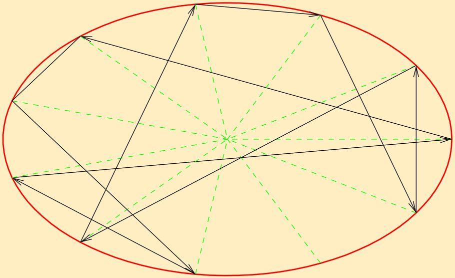
$x \leftarrow seed$
repeat
$x \leftarrow a * x + b \mod n$
$write(x)$
until End of simulation

Example

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

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

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



Congruent generators

Find a maximum cycle length

Théorème

Hull-Dobell, (1962) Let $\{x_n\}$ *the sequence defined by* $x_{n+1} = ax_n + b \mod m$*. Then the maximal cycle has length m if and only if the 3 conditions are verified :*

1. $GCD(a, m) = 1$, $GCD(b, m) = 1$;
2. *if a prime number p is a divisor of m, then p divide* $a - 1$;
3. *if* 4 *divide m, then* 4 *divide* $a - 1$.

Gives uniformity, but not the mixing property

Examples of congruent generators

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

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

(Maple's generator 999999999989 is prime)

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

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

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

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

cycle length :

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

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

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

199 017

Random bits

$x = \{x_1, x_2, \cdots, x_n, \cdots\}$ and $y = \{y_1, y_2, \cdots, y_n, \cdots\}$ sequences of random bits

Hourra for the *XOR*

The sequence $z = \{z_1, z_2, \cdots, z_n, \cdots\}$ with $z_i = x_i$ *XOR* y_i is better than x and y.
Hypothesis x_i and y_i are independent.

Proof :

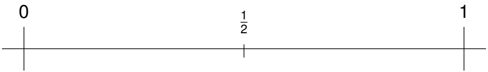
Random bits

$x = \{x_1, x_2, \cdots, x_n, \cdots\}$ and $y = \{y_1, y_2, \cdots, y_n, \cdots\}$ sequences of random bits

Hourra for the *XOR*

The sequence $z = \{z_1, z_2, \cdots, z_n, \cdots\}$ with $z_i = x_i$ *XOR* y_i is better than x and y.
Hypothesis x_i and y_i are independent.

Proof :



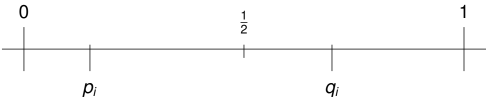
Random bits

$x = \{x_1, x_2, \cdots, x_n, \cdots\}$ and $y = \{y_1, y_2, \cdots, y_n, \cdots\}$ sequences of random bits

Hourra for the *XOR*

The sequence $z = \{z_1, z_2, \cdots, z_n, \cdots\}$ with $z_i = x_i \; XOR \; y_i$ is better than x and y.
Hypothesis x_i and y_i are independent.

Proof :



$$\mathbb{P}(X_i \; XOR \; Y_i = 1) = p_i(1 - q_i) + (1 - p_i)q_i$$

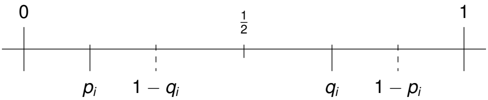
Random bits

$x = \{x_1, x_2, \cdots, x_n, \cdots\}$ and $y = \{y_1, y_2, \cdots, y_n, \cdots\}$ sequences of random bits

Hourra for the *XOR*

The sequence $z = \{z_1, z_2, \cdots, z_n, \cdots\}$ with $z_i = x_i \ XOR \ y_i$ is better than x and y.
Hypothesis x_i and y_i are independent.

Proof :



$$\mathbb{P}(X_i \ XOR \ Y_i = 1) = p_i(1 - q_i) + (1 - p_i)q_i$$

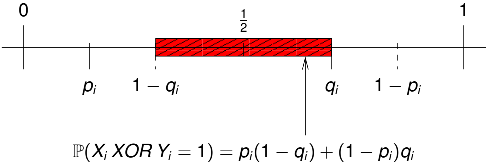
Random bits

$x = \{x_1, x_2, \cdots, x_n, \cdots\}$ and $y = \{y_1, y_2, \cdots, y_n, \cdots\}$
sequences of random bits

Hourra for the *XOR*

The sequence $z = \{z_1, z_2, \cdots, z_n, \cdots\}$ with $z_i = x_i \; XOR \; y_i$ is better than x and y.
Hypothesis x_i and y_i are independent.

Proof :



Random bits (2)

Biased generator of independent bits : $p = \mathbb{P}(x_i = 1)$
$x = \{x_1, x_2, \cdots, x_n, \cdots\}$

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

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

Approximation of an unbiased coin (error control)
Ex : $p = \frac{1}{3}$, $k = 10$

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

Random bits (the end)

Biased generator of independent bits : $p = \mathbb{P}(x_i = 1)$

$x = \{x_1, x_2, \cdots, x_n, \cdots\}$

Generate an unbiased coin :

```
repeat
   X= coin() ;
   Y= coin() ;
until (X≠Y)
return X ;
```

Rejection base algorithm : $\mathbb{P}(accept) = 2p(1-p)$

Mean number of iterations : $\overline{N} = \frac{1}{2p(1-p)}$

Ex : $p = \frac{1}{3}$,

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

Random bits (the end)

Biased generator of independent bits : $p = \mathbb{P}(x_i = 1)$
$x = \{x_1, x_2, \cdots, x_n, \cdots\}$
Generate an unbiased coin :

```
repeat
    X= coin() ;
    Y= coin() ;
until (X≠Y)
return X ;
```

Rejection base algorithm : $\mathbb{P}(accept) = 2p(1-p)$
Mean number of iterations : $\overline{N} = \frac{1}{2p(1-p)}$
Ex : $p = \frac{1}{3}$,

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

Pseudo-random generator

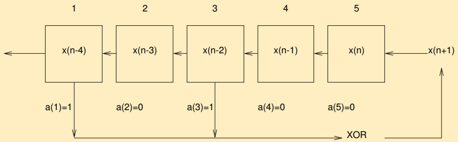
Use the *XOR* inside the algorithm

Tausworthe (1965)

initial binary vector (seed) $x^0 = (x_{-m+1}, ...x_{-1}, x_0)$,
multi-linear recurrence :

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

$a_1, a_2, \cdots, a_m$ fixed
Shifted loop register



Pseudo-random generator

Use *XOR* and modulo

Mersenne Twister (1998)

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

with a good parameter set :
cycle length = $2^{19937} - 1$

Blum Blum Shub Generator (1986)

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

Statistically bad
Excellent for cryptography

Outline of the lecture

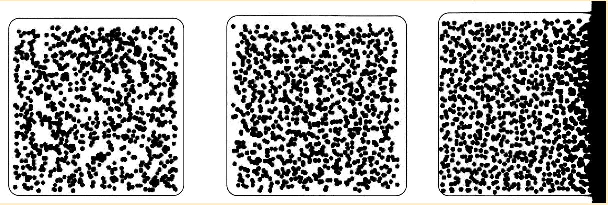
1. Random machines
   - Why generate random numbers ?
   - Random machines
   - Pseudo-random generators
2. and Human mind
   - Randomness detection
   - Generate randomness

Randomness detection

René Magritte, Golconda. 1953.

Randomness detection (2)

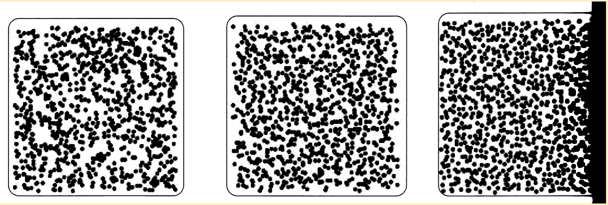
Which one is random ?



Rake effect : randomness = uniformity = equality among places

Randomness detection (2)

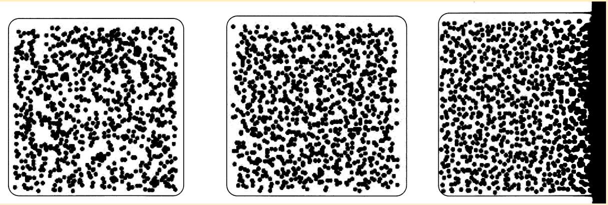
Which one is random ?



Rake effect : randomness = uniformity = equality among places

Randomness detection (2)

Which one is random ?



Rake effect : randomness = uniformity = equality among places

Randomness detection (3)

Pierre Bruegel : Children games

crowd : random (not under control)

Randomness detection (3)

Pierre Bruegel : Children games

crowd : random (not under control)

The Law of the Series

Das Gesetz der Serie (Paul Kammerer)

1. what happened is going to happen again rapidly
2. bad events are grouped
3. events from a same category happen together

causal explanation
rake effect (ex anniversary paradox)
focus of observation
true relation

The Law of the Series

Das Gesetz der Serie (Paul Kammerer)

1. what happened is going to happen again rapidly
2. bad events are grouped
3. events from a same category happen together

causal explanation
rake effect (ex anniversary paradox)
focus of observation
true relation

Outline of the lecture

1. Random machines
   - Why generate random numbers ?
   - Random machines
   - Pseudo-random generators
2. and Human mind
   - Randomness detection
   - Generate randomness

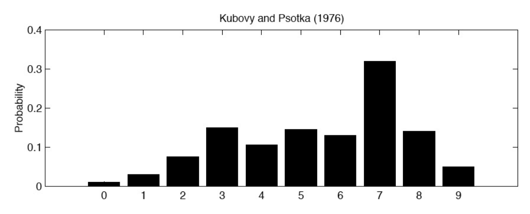
Generate randomness

Give a random figure between 0 and 9

We look for a number and considering the arithmetic properties of this number we choose the one with the less properties.

Generate randomness

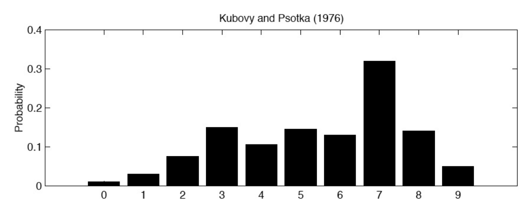
Give a random figure between 0 and 9



We look for a number and considering the arithmetic properties of this number we choose the one with the less properties.

Generate randomness

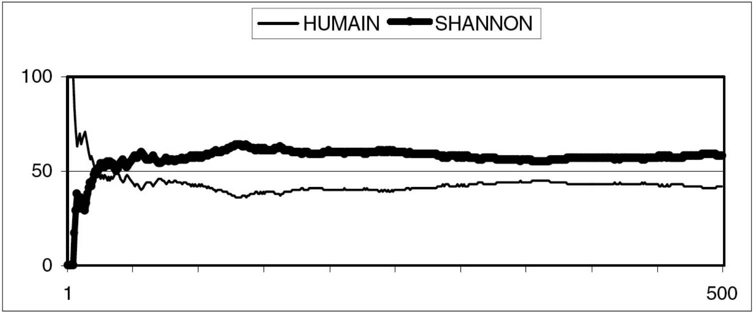
Give a random figure between 0 and 9



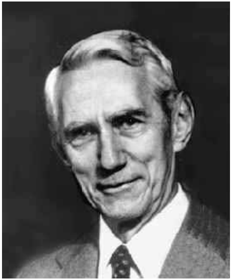
We look for a number and considering the arithmetic properties of this number we choose the one with the less properties.

Even-Odd against the machine

8 states automaton



Claude Shannon (1916-2001)



Claude Elwood Shannon (30 avril 1916 à Gaylord, Michigan - 24 février 2001), ingénieur électrique, est l'un des pères, si ce n'est le père fondateur, de la théorie de l'information. Son nom est attaché à un célèbre "schéma de Shannon" très utilisé en sciences humaines, qu'il a constamment désavoué.

Il étudia le génie électrique et les mathématiques à l'Université du Michigan en 1932. Il utilisa notamment l'algèbre booléenne pour sa maîtrise soutenue en 1938 au MIT. Il y expliqua comment construire des machines à relais en utilisant l'algèbre de Boole pour décrire l'état des relais (1 : fermé, 0 : ouvert).
Shannon travailla 20 ans au MIT, de 1958 à 1978. Parallèlement à ses activités académiques, il travailla aussi aux laboratoires Bell de 1941 à 1972.
Claude Shannon était connu non seulement pour ses travaux dans les télécommunications, mais aussi pour l'étendue et l'originalité de ses hobbies, comme la jonglerie, la pratique du monocycle et l'invention de machines farfelues : une souris mécanique sachant trouver son chemin dans un labyrinthe, un robot jongleur, un joueur d'échecs (roi tour contre roi)...
Souffrant de la maladie d'Alzheimer dans les dernières années de sa vie, Claude Shannon est mort à 84 ans le 24 février 2001.

To go further...

Historical books

Laplace, P.-S. (1812), Théorie analytique des probabilités, Mme Ve Courcier, Paris.

Laplace, P.-S. (1825), Essai philosophique sur les probabilités, Gauthier-Villard et Cie, Paris.

Poincaré, H. (1912), Calcul des probabilités, Gauthier-Villars, Paris.

Kolmogorov, A. (1933), Foundations of the theory of probability, Chelsea Publishing Company.

Borel, E. (1922), Principes et formules classiques du calcul des probabilités, Gauthier-Villars, Paris.

Shannon, C. (1948), A mathematical theory of communications, Bells Systems Technical Journal.

Li, M. et Vitananyi, P. (1990), Kolmogorov Complexity and its Applications, Elsevier Science Publisher, chapter 4, pp.

To go further (2) ...

Synthesis (in frech)

Ekeland, I. (1991), Au hasard, Le Seuil.
Dacunha-Castelle, D. (1996) Chemins de l'aléatoire,Flammarion.
Le hasard (1996), Dossier Pour la science.
Pagès, G. et Bouzitat, C. (1999) En passant par hasard... Vuibert Paris
Delahaye, J.-P. (1993), Le désordre total existe-t-il ?, Pour la Science (193), 152 ?156.
Delahaye, J.-P. (1994a), Information, complexité et hasard, Hermes.
Delahaye, J.-P. (1994b), Le complexe surgit-il du simple ?, Pour la Science (203), 102-107.

To go further (3) ...

Web sites

For biographies
- en.wikipedia.org
- http ://www-groups.dcs.st-and.ac.uk/ history/

Chaitin's web page :
http ://www.cs.auckland.ac.nz/ chaitin

Levin's web page :
http ://www.cs.bu.edu/ lnd

Delahaye's web page
http ://www2.lifl.fr/ delahaye/