Randomness

Florence Perronnin

Univ. Grenoble Alpes, LIG, Inria

October 8, 2018

Outline

Birthday

Birthday

Two people in the room have the same birthday ! What is the probability?

for N people,
the probability of a birthday collision for $N = 57$ people is :
$1 - \frac{365 \times 364 \times ... \times 309}{365^{57}} = 0.99$

Birthday with parents

Two people (not necessarily in the room...) have the same birthday, *and* their mothers have the same birthday, *and* their fathers have the same birthday ! What is the probability?

With N= 431 people with *same birthday*, $p >= 50\%$. For *uniformly chosen* (not "randomly" chosen...) people, in France the probability is 1 ($365^3 \approx 48,000,000$).

Casino

A group of 60 students go to the casino together. They agree to play 37\$ each.
They all bet on a "even" number at the roulette ($\mathbb{P}[\text{win}] = \frac{18}{37}$).
What is the probability that every student wins exactly 18\$?

Bad stuff happens

A newspaper depicts a $10,000$-people city with a cancer rate that is 50% above national average. What do you think?

"loi des séries"

What would you think of a country where all 10,000-people cities have the same exact cancer rate?

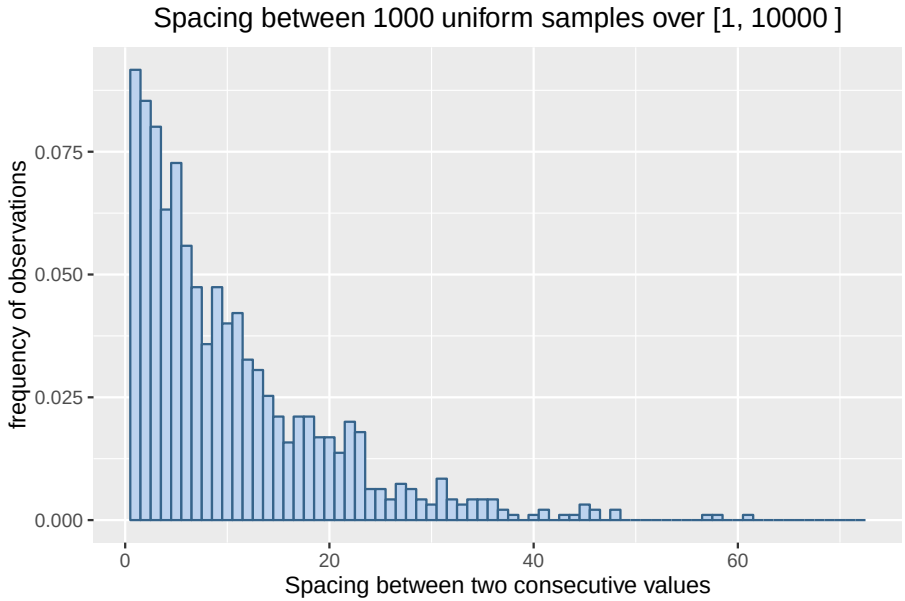
Rightarrow Sometimes random variables take "unexpected" values (for no reason other than the underlying distribution).

Spread

Let us pick 12 random dates in the year.
(for example, 15, 180, 114, 11, 69, 29, 356, 307, 161, 222, 35, 87)

Let us compute the maximum "closeness" of these dates. What is the expected minimum between two of 12 randomly chosen dates?

2.53 days



Heads or tails

Let's play

Write down 51 symbols "H" (for *heads*) or "T" (*tails*).
Now count how many times the result *changes* ("H" $\rightarrow$ "T" or vice-versa).

Consider the following series:
$y = 000010100001100001110011111011001000011101010000100$

- 21 "1"s (out of 50)
- flips 23 times (out of 50)

Is it random?

Humans

- 60% flips - 40% repeat (random : 50%)
- local equity

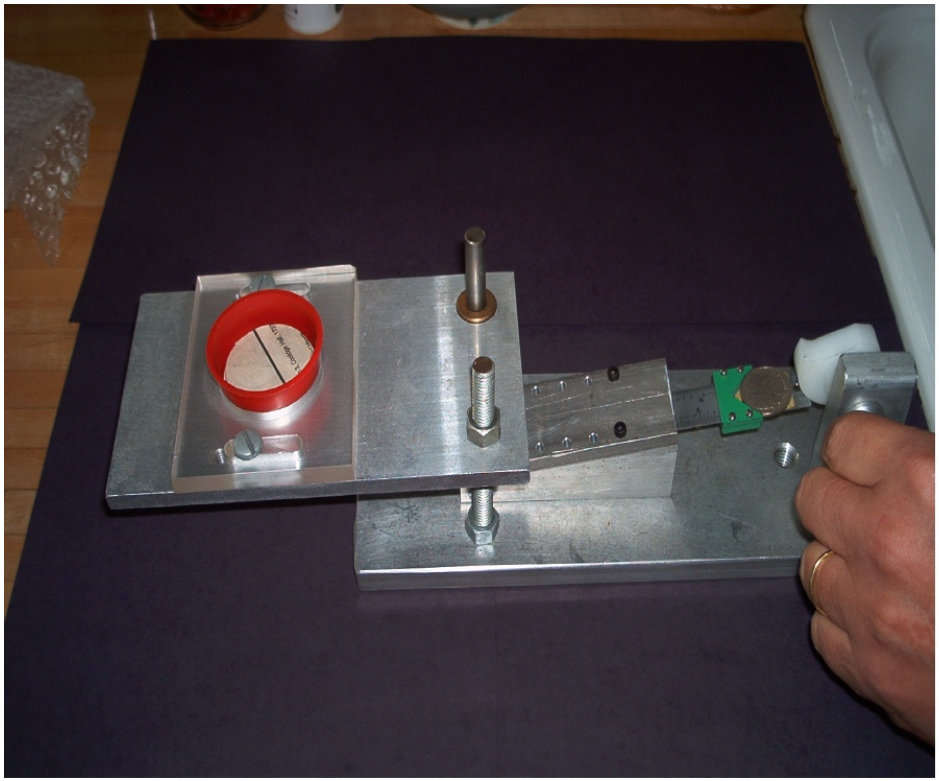
Outline

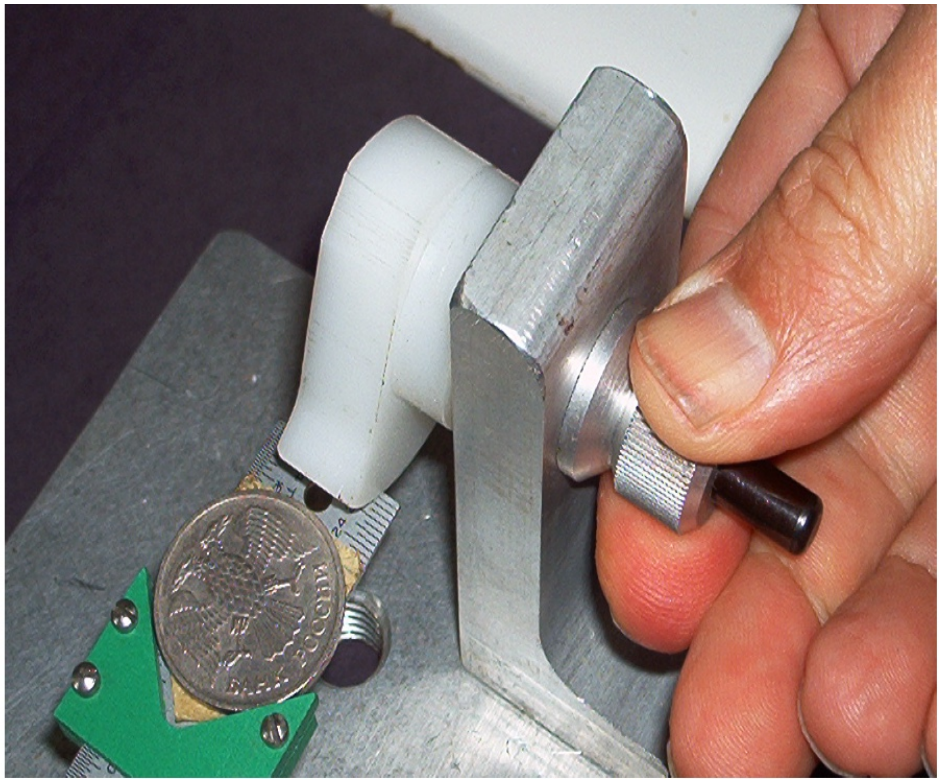
Random sequence

See Jean-Marc Vincent's slides for various randomness tests.

- Human randomness testing/production pp. 83-86, 87-89
- What is a random sequence? pp. 2-26, 27-42, 59-60.

Outline





Diaconis, P., Holmes, S., and Montgomery, R. (2007). Dynamical bias in the coin toss. SIAM review, 49(2), 211-235.

Producing randomness

Algorithmic Random Number Generator

- Not "random" according to the "strong randomness" definition.
- 100% deterministic
- yet, a necessary tool that mimics randomness and passes all randomness tests.
- unpredictible outcome... (except if parameters and algorithm are known, of course)

$\Rightarrow$Pseudo-random number generators.

Challenge

How to build a PRNG that is unpredictible ?

Pseudo-Random Number Generators

See last week's exercices about pseudo-random number generation. More details in Jean-Marc Vincent's slides pp. 88-101.

Sources

- Delahaye, J.-P., Notre vision du hasard est bien hasardeuse, Pour La Science n. 293, mars 2002.
- Delahaye, J.-P., Les Dés pipés du cerveau, Pour La Science n. 326, décembre 2004.
- Delahaye, J.-P., L'Impossible Hasard, Pour La Science n. 413, décembre 2012.
- Diaconis, P., Holmes, S., and Montgomery, R. (2007). Dynamical bias in the coin toss. SIAM review, 49(2), 211-235.