

MODERN CRYPTOGRAPHY

RANDOM DEFINITIONS: NOTES ON SEPTEMBER 17, 2021

Jeffrey Goldberg

`jeffrey@goldmark.org`

September 17, 2021

Revised May 8, 2024

“Random” means different things depending on who is talked to whom

- Ordinary language
- Statistics
- Information Theory
- Cryptography

DEFINITIONS

DEFINITIONS

IN STATISTICS






































INDEPENDENT & IDENTICALLY DISTRIBUTED

Using the example of rolling a pair of D6s and computing their sum. (Question: Is this a uniform distribution?)

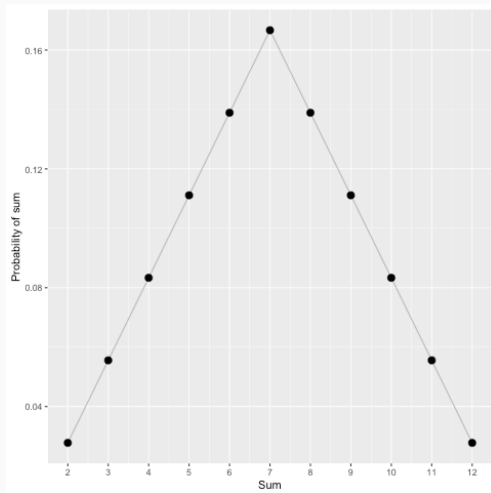
- If each roll of the dice does not depend on the results of prior or subsequent rolls the rolls are *independent*.
- If each roll of the dice gives with results with the same probability as other rolls, they are *identically distributed*.

Random variables that meet those two criteria are *independent and identically distributed* (iid).

ANSWER

Sum	No. of ways	Rolls	
2	1		
3	2	 	
4	3	  	
5	4	   	
6	5	    	
7	6	     	
8	5	    	
9	4	   	
10	3	  	
11	2	 	
12	1	 	

ANSWER



STATISTICIANS ARE INDISCRETE: REAL MEASURES

- Probabilities are real numbers and not just ratios of whole numbers
- Statisticians do Calculus
- So underlying definitions are based on Measure Theory.

None of this matters, as we are going to ignore notions of randomness from statistics.

DEFINITIONS

IN INFORMATION THEORY

THREE DEFINITIONS

Incompressible The more a bit sequence can be compressed the less random it is.

Indescribable The shorter a program is for describing (generating) a bit sequence the less random a bit sequence is.

Unpredictable The more one can win by placing bets on the next bit in a sequence the less random the sequence is.

2024-05-08

Modern Cryptography

└ Definitions

└ In Information Theory

└ Three definitions

THREE DEFINITIONS

Incompressible The more a bit sequence can be compressed the less random it is.

Indescribable The shorter a program is for describing (generating) a bit sequence the less random a bit sequence is.

Unpredictable The more one can win by placing bets on the next bit in a sequence the less random the sequence is.

Must be defined very carefully, and it must avoid the paradox of “the smallest natural number that cannot be described in fewer than fourteen words”

Randomness in these senses require (among other things) that a distribution be uniform.

When Incompressible, Indescribable, and Unpredictable are defined precisely, it turns out that anything that's perfectly random under one of those definitions is perfectly random under the others.

DEFINITIONS

IN CRYPTOGRAPHY

Cryptography defines random as *indistinguishable* from perfectly random typically using the **Unpredictability** notion for perfectly random.

A pseudo random generator (**PRG**) takes a seed and generates a stream of bits. To be useful, the number of bits that it can output should be longer than the seed. The seed is assumed to be truly random and uniform, and its length places an upper limit on the security of the **PRG**.

Perfect Perfection means “there is no algorithm”

Secure Cryptographically secure means “there is no algorithm running under certain limits of computation power that has a non-negligible chance of winning.” For random number generators, these are called cryptographically secure pseudo-random number generators.

To focus on the essence of definitions, I will typically avoid talking about the constraints or “negligible.”

Definition 1 (Distinguishing game)

1. The system picks a bit b uniformly.
2. The adversary \mathcal{A} asks the system for a bit sequence of a particular length.
3. If $b = 0$ the system returns a true random bit sequence to \mathcal{A} . If $b = 1$ it returns a bit sequence from its generator.
4. \mathcal{A} wins the game if it guesses b correctly

Note that this definition skips over stuff needed for talking about the computational limitations on \mathcal{A} .

Definition 2 (Indistinguishable from random)

There is no \mathcal{A} that can win the distinguishing game at a better than chance rate.

Recall that we are constraining the computational capacity of \mathcal{A} and we give a negligible amount of wiggle room for “better than chance.”

2024-05-08

Modern Cryptography

└ Definitions

└ In Cryptography

└ Indistinguishable from random

INDISTINGUISHABLE FROM RANDOM

Definition 2 (Indistinguishable from random)

There is no A that can win the distinguishing game at a better than chance rate.

Recall that we are constraining the computational capacity of A and we give a negligible amount of wiggle room for "better than chance."

Writing out the definition with the constraints and the wiggle room requires a lot of extra notation that distracts from the gist of the definitions

SEEDS AND ENTROPY

A deterministic PRNG takes a seed, and will produce the same sequence of bits given the same seed.

- A *deterministic* PRNG takes a seed, and will produce the same sequence of bits given the same seed.
- Ultimately the sequence is no stronger than the seed.
- Good seeds must come from the physical world. See the 2012 blog post [Alan Turing's contribution can't be computed](#).
- Physical sources are rarely uniform. Ten flips of a biased coin doesn't give you ten bits of entropy.

- Should be secret (No Lava Lamps)
- Should not be controllable by attackers
- Should give enough data quickly enough to be available
- Should be unpredictable

- Network timings, temperature readings, keyboard entry timings, disk reads.
- Direct quantum sources: UHF static, quantum tunneling.

WHAT WE NEED FROM A PRG

WHAT WE MAY NEED FROM A PRG

- Secrecy
- Non-secret output to give no information about other output.
- Uniformity
- Large set of possible outputs