Randomized Algorithm

Tutorial I

Sep. 30 2008

Your TA: Abner C.Y. Huang
BarrosH@gmail.com

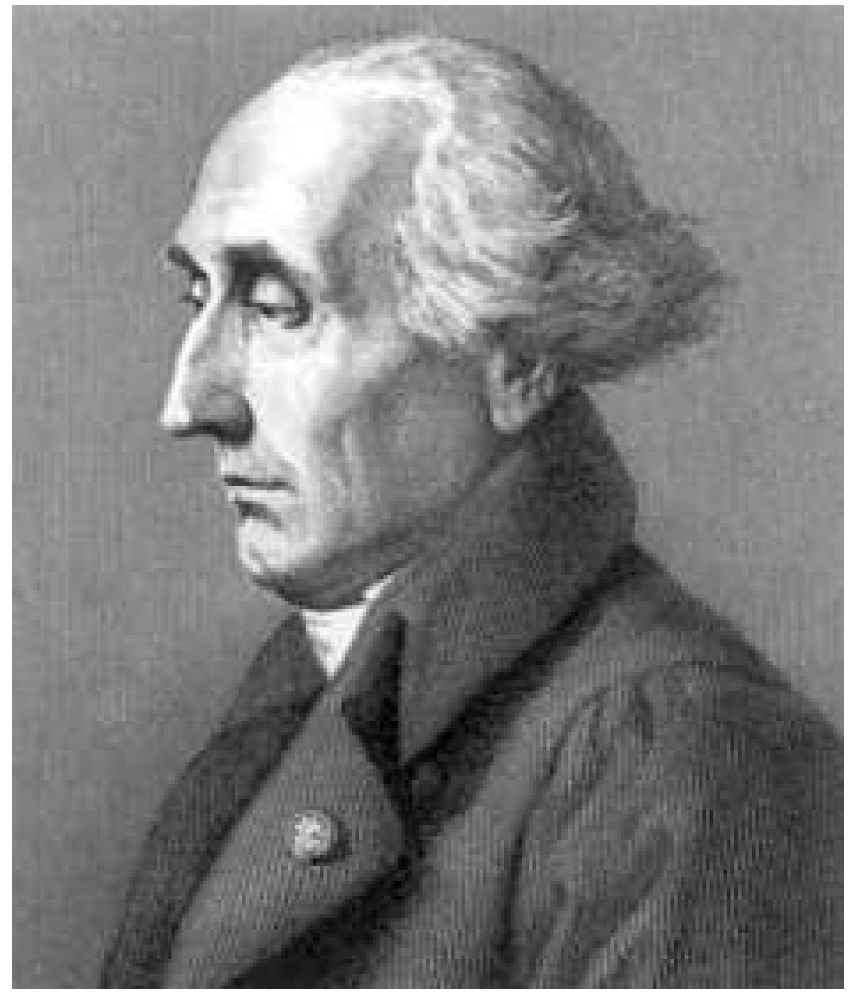
Think about Randomness

Determinism vs. Randomness

Randomness in Real World

Joseph Louis Lagrange's deterministic universe

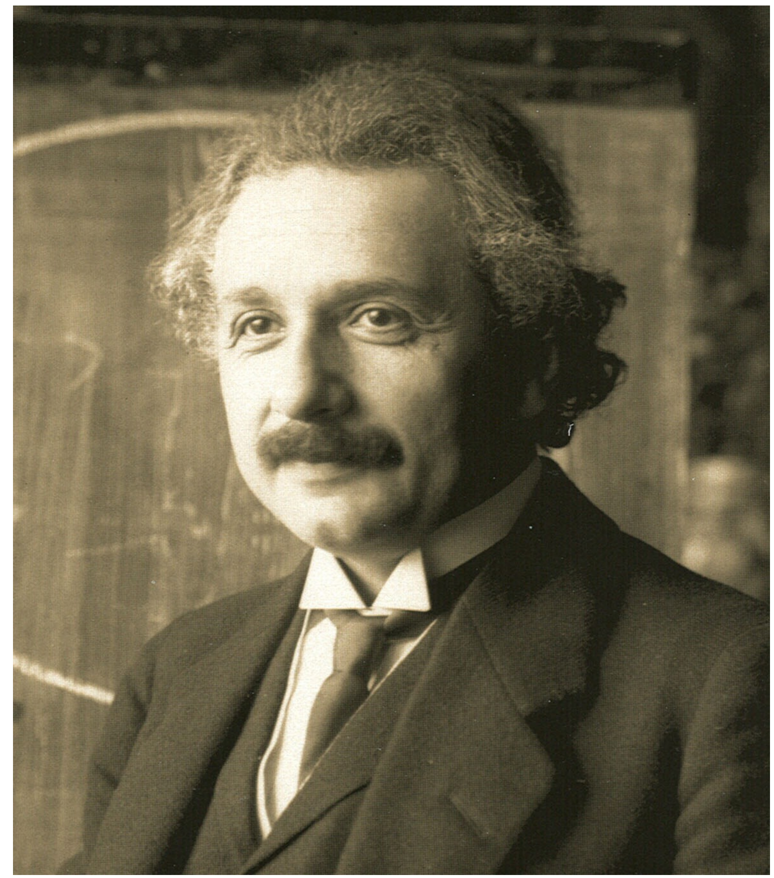
- offered the most comprehensive treatment of classical mechanics since Newton and formed a basis for the development of mathematical physics in the nineteenth century.



- Werner Heisenberg

Heinsberg's Uncertainty Principle

- Albert Einstein



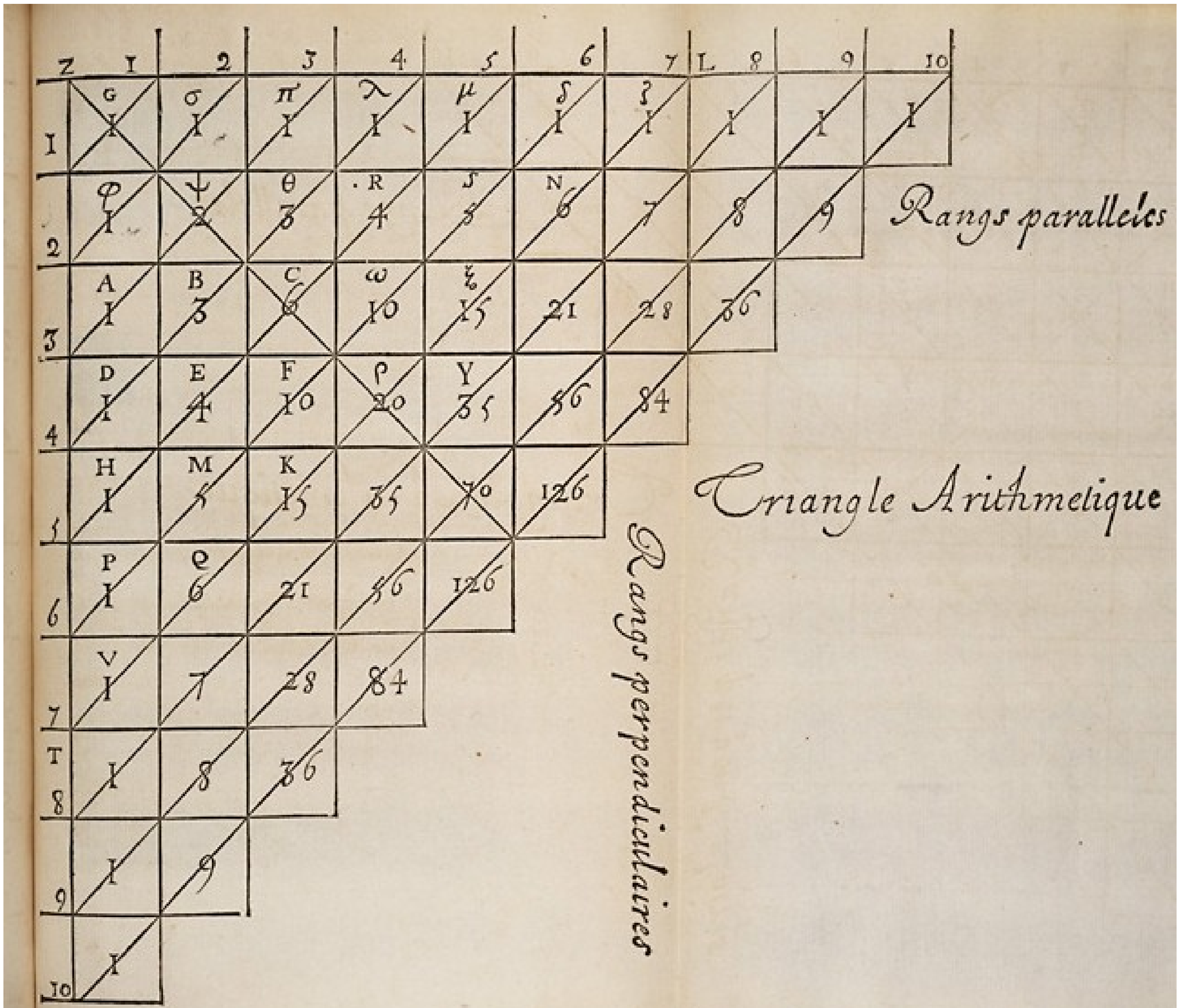
God doesn't play dice with the universe.

Randomness in Math.

Randomness in Mathematics

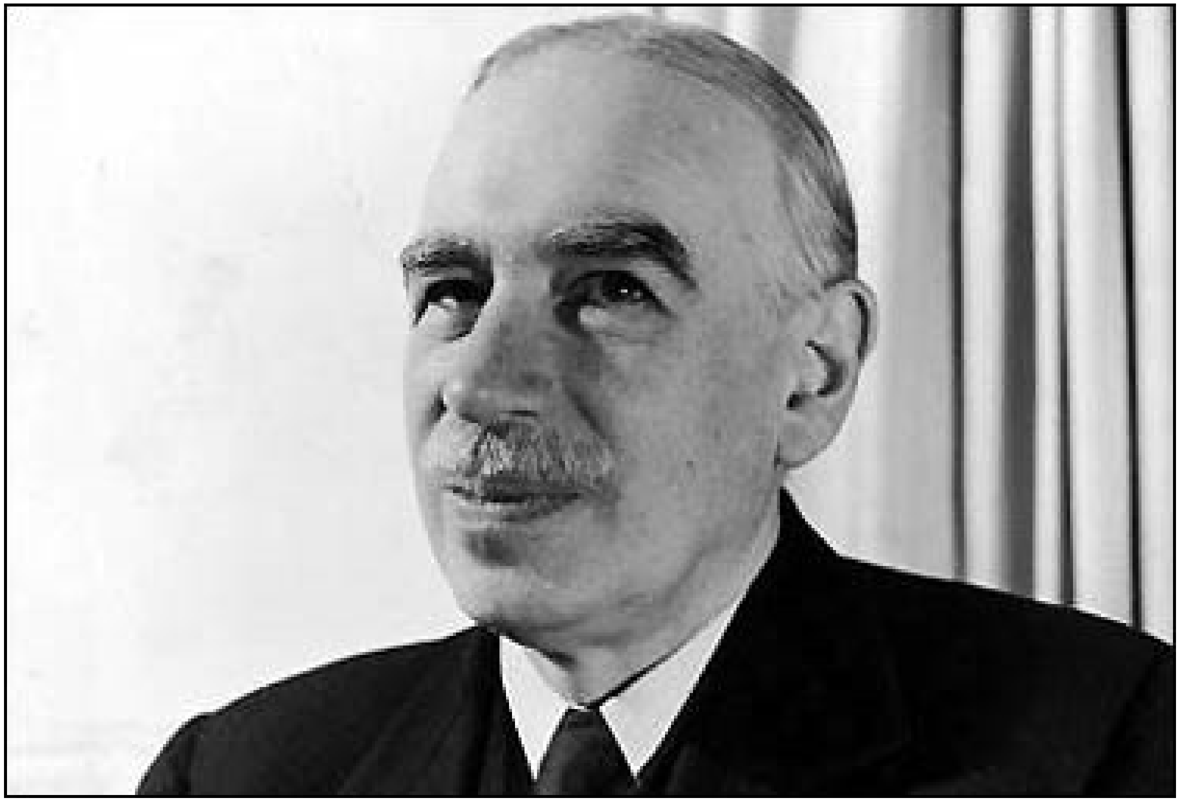
- Pascal was a mathematician of the first order. He helped create major new area of research, probability theory, with Pierre de Fermat.

Pascal's triangle



Source of Probability theory: Gambling

John Maynard Keynes



The long run is a misleading guide to current affairs. In the long run we are all dead.

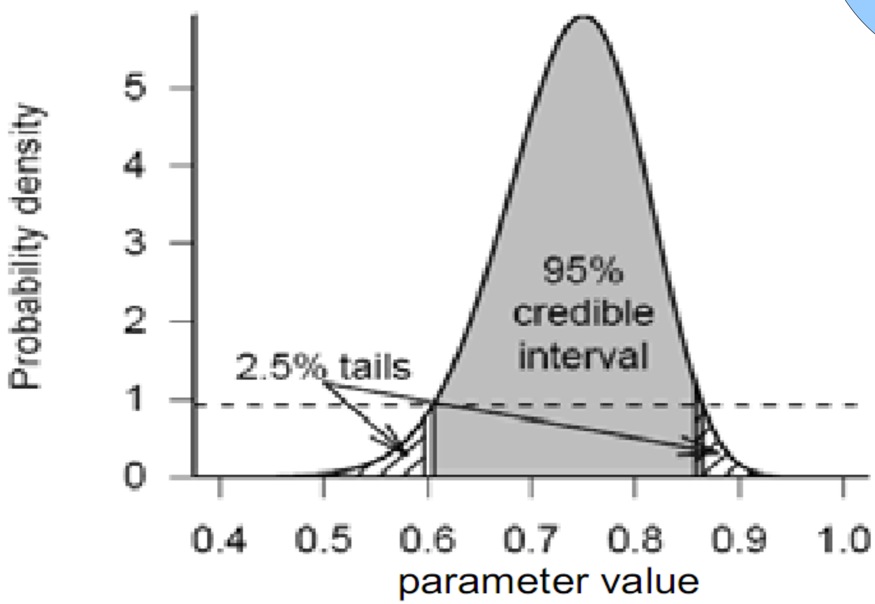
- He got the Ph.D degree of mathematics at King’s College, Cambridge.
- His thesis is about logic in probabilistic viewpoint.
- Keynes published his Treatise on Probability in 1921, a notable contribution to the philosophical and mathematical underpinnings of , championing the important view that probabilities were no more or less than truth values intermediate between simple truth and falsity.

Epistemology

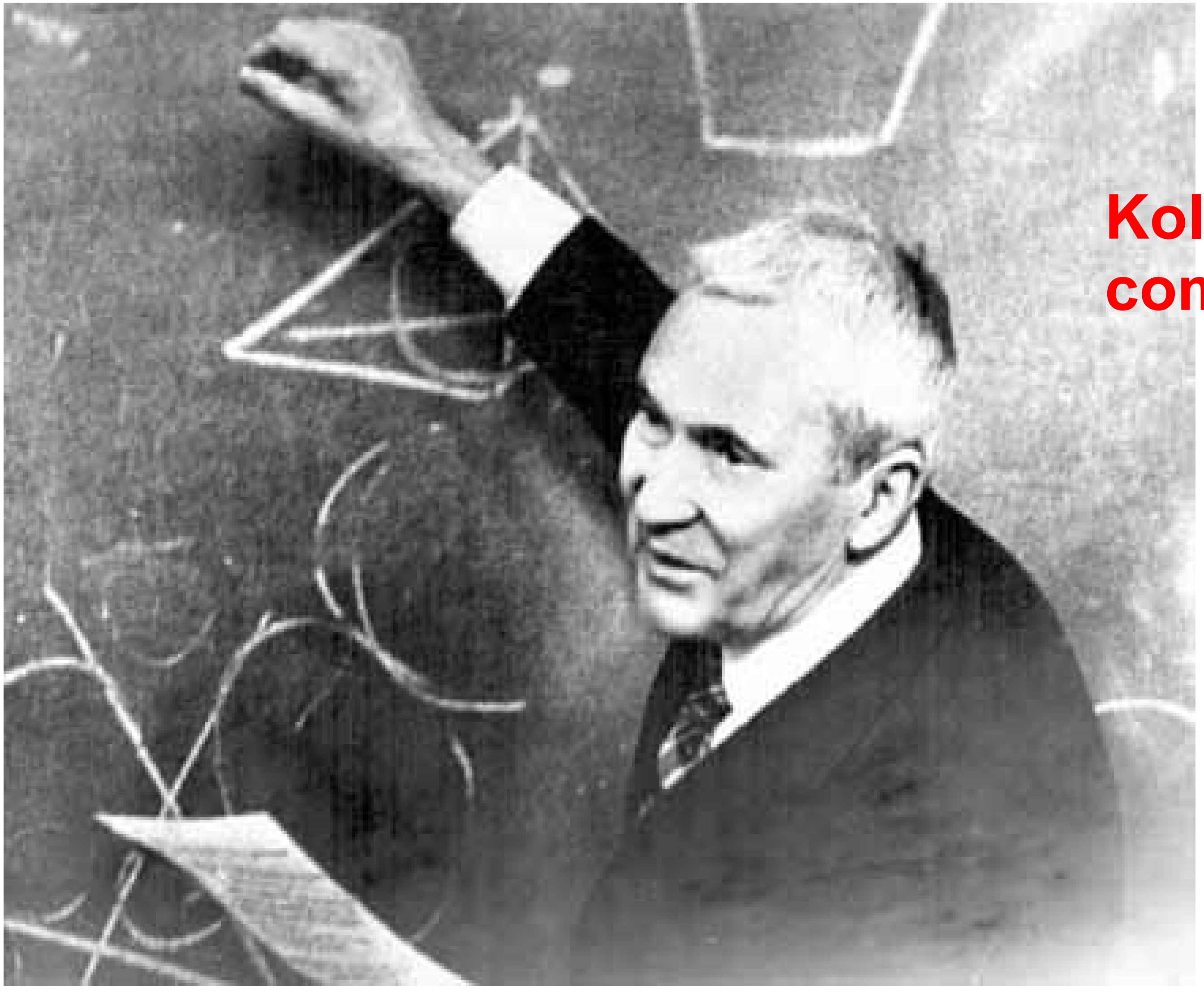
- Bayesian and frequentist interpret idea of probability differently.
  - Frequentist : an event's probability as the limit of its relative frequency in a large number of trials.
    - i.e., parameters are constants.
  - Bayesian : 'probability' should be interpreted as degree of believability
    - i.e., parameters are random variables.

Bayesian will say: "There is a 95% probability that this interval contains the mean."

frequentist will say "95% of similar intervals would contain the true mean, if each interval were constructed from a different random sample like this one."



Andrey Kolmogorov



Kolmogorov complexity

Kolmogorov axioms

In 1933, Kolmogorov published the book, Foundations of the Theory of Probability, laying the **modern axiomatic foundations of probability theory** and establishing his reputation as the world's leading living expert in this field.

Randomness in CS

John von Neumann

- Monte Carlo method
- the EDVAC project
- Cellular Automata
- Merge Sort
- Min-Max theorem
- etc.

John von Neumann's algorithm for simulating a fair coin with a **biased coin**

- $1 = pp + (1-p)p + p(1-p)$ $+ (1-p)(1-p)$
- Rejects for TT, HH.
- 1 for TH
- 0 for HT

Randomness on Computer

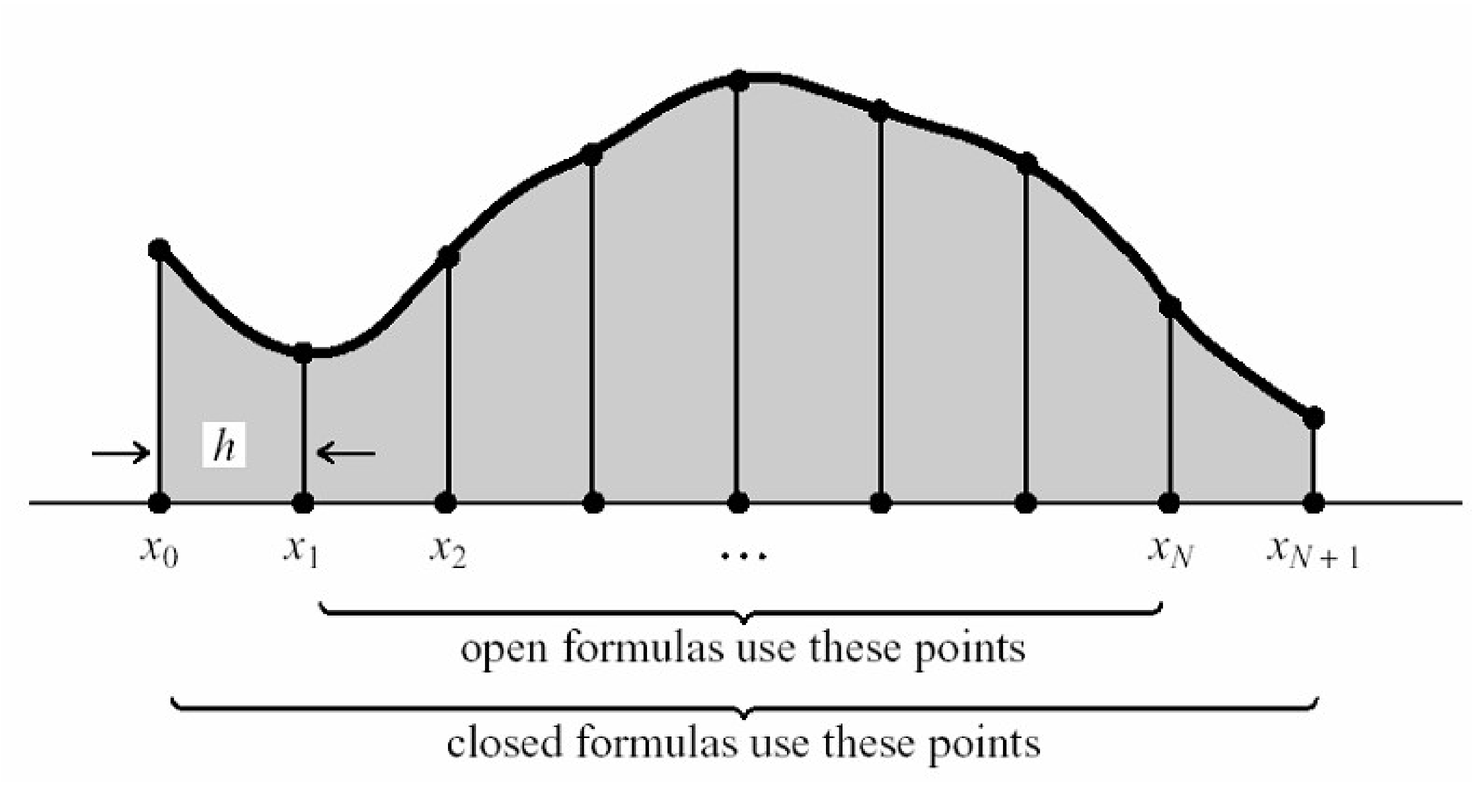
- Von Neumann's coin flipping trick (1951) was the first to get true randomness from a weak random source.
- Much research in TCS in 1980's and 90's to handle weaker dependent sources.
- Led to development of extractors and connections to pseudorandom generators.

Michael O. Rabin

- Miller-Rabin primality test.
  - 'There are many methods -- none of them as good as the randomized primality test.' by Rabin

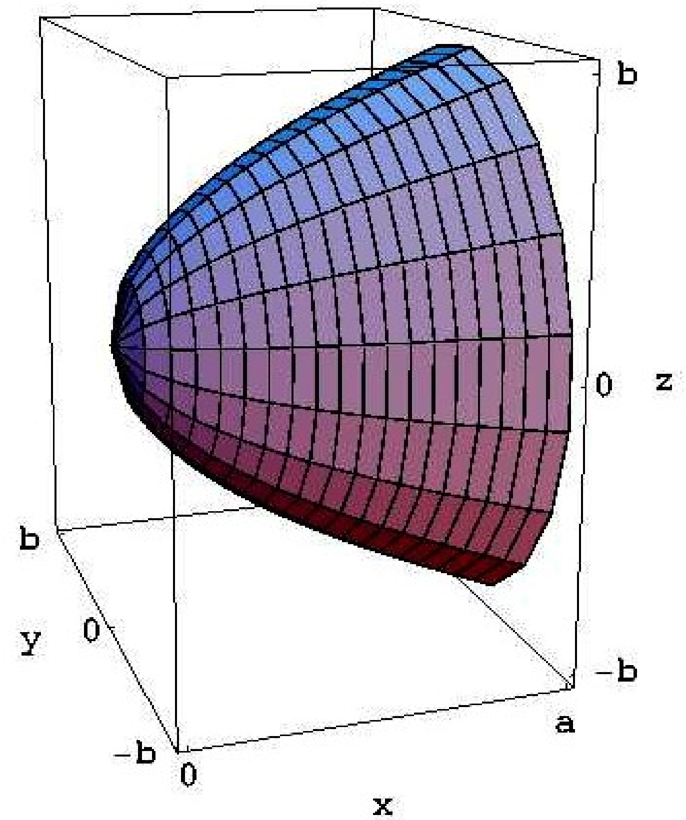
Why Use Randomized Algorithms

- Consider the Volume Estimation Problem.
- Deterministic approach is fast for 1D. Use *m* slices.



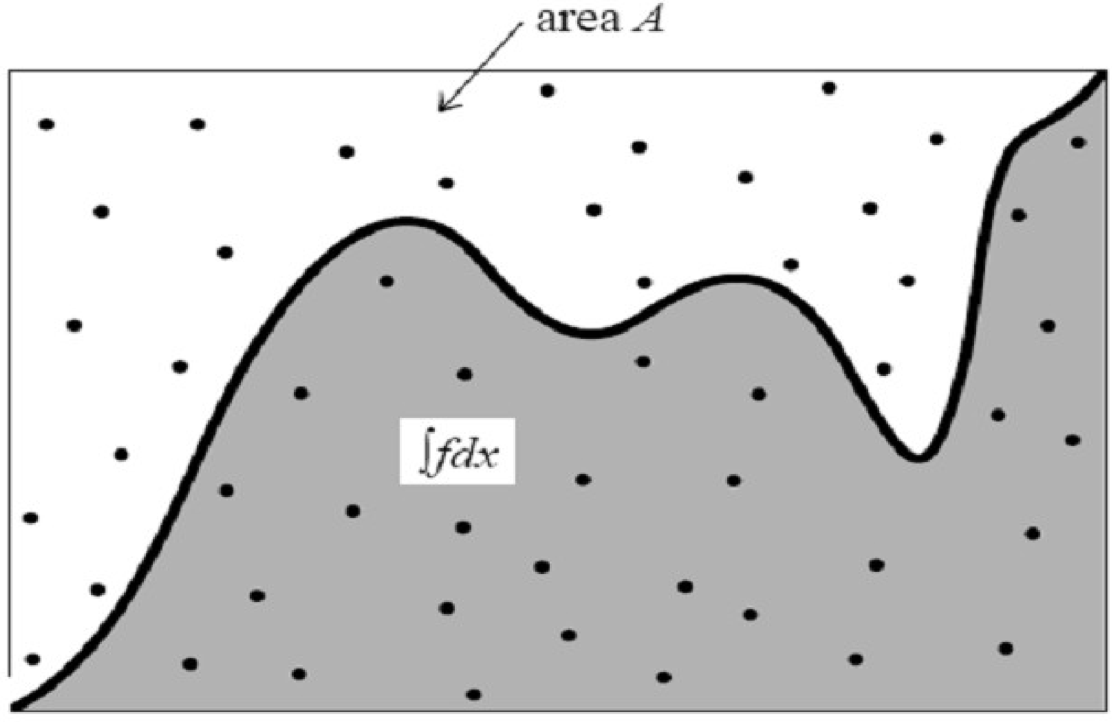
Why Use Randomized Algorithms

- How about 3D version? For the same precision, we need at least m^3 slices.
- The Curse of Dimension.



Why Use Randomized Algorithms

- Monte Carlo Method: The top ONE algorithm elected at 2000.
  - Its m is independent from dimension.



In Real World, a lot of examples showed that randomized algorithms help for solving Hard problems.

Another Big Open Problem

- Like Millennium Problem, NP=?=P
- Whether NP=RP?
  - Roughly, it asks whether algorithm with power of random is more powerful than algorithm without power of random?

Now let's go back to this course.

Hints for your homework.

Problem 1

Principle of deferred decision.

Try to fixed nine dices.

Problem 2

It is for fun.

No Hint, Enjoy It.

Think in mathematics is more helpful than intuition.

Problem 3

- Solve it by definitions.
- Memory-less property of geometric random variable might help!

Problem 4

Use Indicator variable/linearity of expectation

Don't look into the permutations.

Problem 5

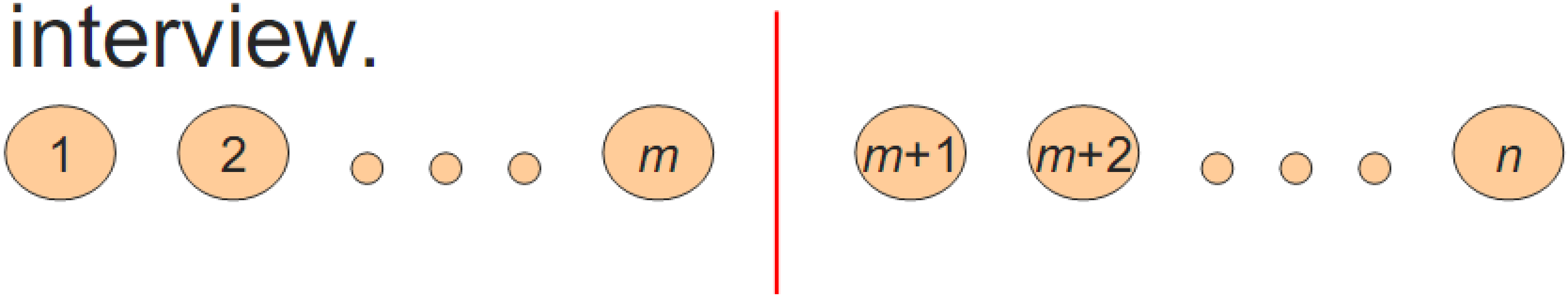
It is geometric random variable in fact.
Memory-less property of geometric random variable might help!

Problem 6

Indicator variable/linearity of expectation

Problem 7

- First, we give everyone a number card. The number card means the order of interview.

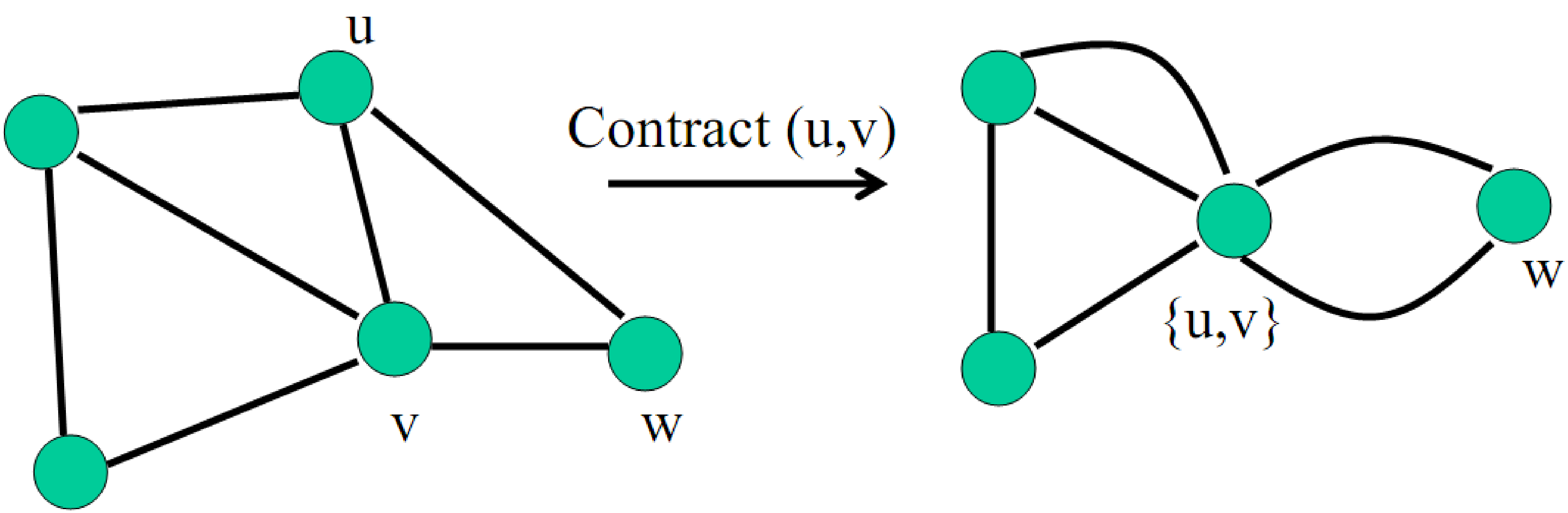


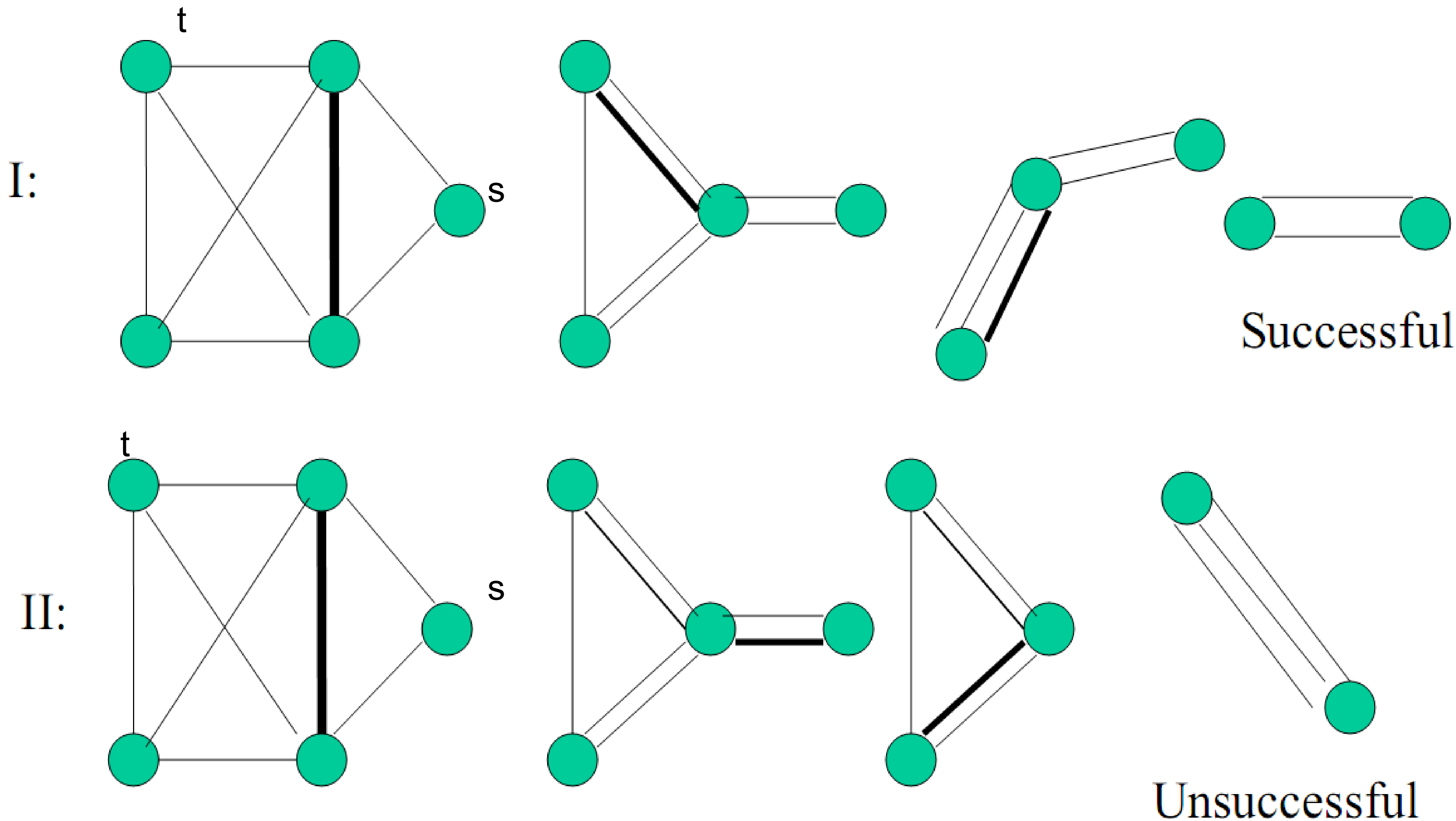
- Choose the best grade from 1 to *m* : A.
- If someone after *m* better than A, accept him. Otherwise, we choose the last one.

- Sometimes, we may not get the best candidate.
  - The best one's number card is less than $m+1$.
  - A, the best grade we chose from 1 to m, is not too good.
- What is a "nice" m?
  - The second best candidate is in $1 \sim m$.

Problem 8

- Consider the u-w min-cut
  - If picks edge {u,w}, then pick again.





I:
t
s
Successful
II:
t
s
Unsuccessful