Felipe P. Vista IV



Course Outline

- Mathematical Thinking
 - Convincing Arguments, Find Example, Recursion, Logic, Invariants
- Probability & Combinatronics
 - Counting, Probability, Random Variables
- Graph Theory
 - Graphs (cycles, classes, parameters)
- Number Theory & Cryptography
 - Arithmetic in modular form
 - Intro to Cryptography

Mathematical Thinking – Combinatronics & Probability Probability

WHAT IS PROBABILITY

Probability & Combinatronics – Probability

- Paradox of Probability Theory
- Galton Board
- Natural Sciences and Mathematics
- Rolling Dice
- More Examples

What is Probability

Predicting Unpredictable

tossing a coin

What is Probability

- tossing a coin
- is unpredictable

- tossing a coin
- is unpredictable
- repeated experiments:

- tossing a coin
- is unpredictable
- repeated experiments:

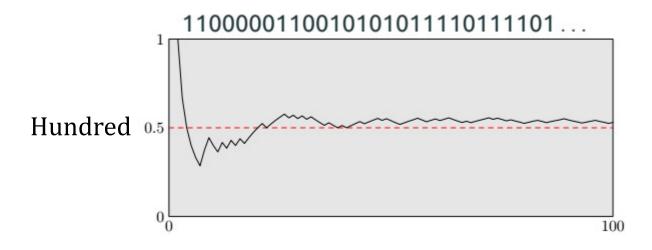
- tossing a coin
- is unpredictable
- repeated experiments:
 - -1100000110010101111011111101...
 - $-0 \rightarrow head, 1 \rightarrow tail$

- tossing a coin
- is unpredictable
- repeated experiments:
 - -1100000110010101111011111101...
 - $-0 \rightarrow head, 1 \rightarrow tail$
- zeroes and ones appear equally open

- tossing a coin
- is unpredictable
- repeated experiments:
 - -1100000110010101111011111101...
 - $-0 \rightarrow head, 1 \rightarrow tail$
- zeroes and ones appear equally open
- frequency of 1's:

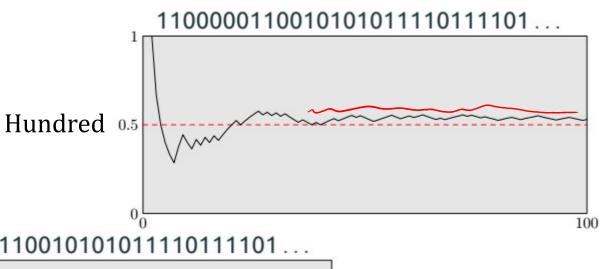
- tossing a coin
- is unpredictable
- repeated experiments:
 - *11000001100101011111011111101...*
 - $-0 \rightarrow head, 1 \rightarrow tail$
- zeroes and ones appear equally open
- frequency of 1's: $(\#ones)/(length) \approx 1/2$

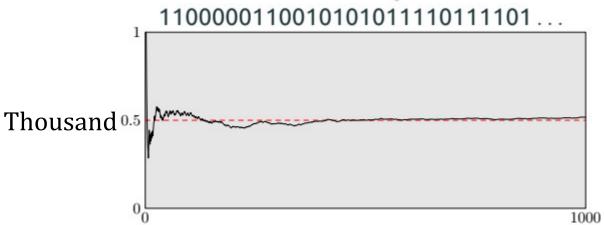
Random Bits



By: George Marsaglia, 1995

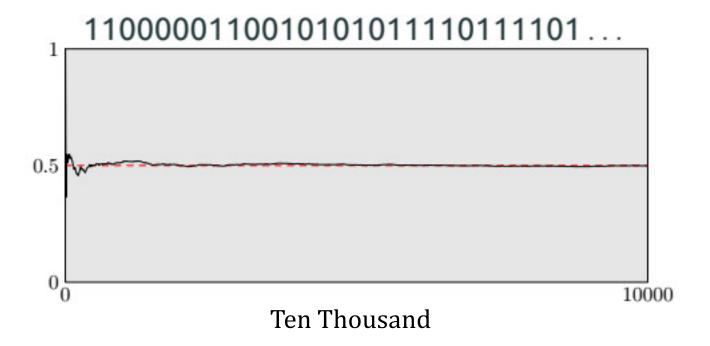
Random Bits





By: George Marsaglia, 1995

Random Bits



By: George Marsaglia, 1995

Probability & Combinatronics – Probability

- Paradox of Probability Theory
- Galton Board
- Natural Sciences and Mathematics
- Rolling Dice
- More Examples

Bean Machine aka Galton Board



https://en.wikipedia.org/wiki/Bean_machine#/media/File:Galton_box.jpg

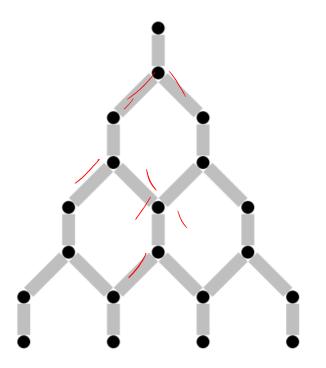
What is Probability

Bean Machine aka Galton Board

https://upload.wikimedia.org/wikipedia/commons/transcoded/d/dc/Galton_box.webm/Galton_box.webm.1080p.webm

Analysis

Assume that at each level, the beans are split evenly



What is Probability

Galcon and Pascal

assume that beans are divided evenly at all times

What is Probability

- assume that beans are divided evenly at all times
- compute the next line:

What is Probability

- assume that beans are divided evenly at all times
- compute the next line: $z = \frac{(x+y)}{2}$

- assume that beans are divided evenly at all times
- compute the next line: $z = \frac{(x+y)}{2}$

- assume that beans are divided evenly at all times
- compute the next line: $z = \frac{(x+y)}{2}$

$$\frac{Pascal\ Triangle}{2^n} = \binom{n}{k} / 2^n$$

What is Probability

Concentration

more beans near the centre

What is Probability

- more beans near the centre
- how strong is the effect?

- more beans near the centre
- how strong is the effect?
- 100 layers, bins 0 ... 100

- more beans near the centre
- how strong is the effect?
- *100* layers, bins *0* ... *100*
 - what fraction in bins $40 \dots 60$?

- more beans near the centre
- how strong is the effect?
- 100 layers, bins 0 ... 100
 - what fraction in bins $40 \dots 60$?
- 1000 layers

- more beans near the centre
- how strong is the effect?
- *100* layers, bins *0* ... *100*
 - what fraction in bins $40 \dots 60$?
- *1000* layers
 - What fraction in bins $400 \dots 600$?

Probability & Combinatronics – Probability

- Paradox of Probability Theory
- Galton Board
- Natural Sciences and Mathematics
- Rolling Dice
- More Examples

What is Probability Theory?

 "Probability theory says that the coin gives heads and tails equally often"

- "Probability theory says that the coin gives heads and tails equally often"
- false,

- "Probability theory says that the coin gives heads and tails equally often"
- false, if probability theory is understood in modern way, as part of mathematics

- "Probability theory says that the coin gives heads and tails equally often"
- false, if probability theory is understood in modern way, as part of mathematics
- a coin with two tail sides do not destroy probability theory

- "Probability theory says that the coin gives heads and tails equally often"
- false, if probability theory is understood in modern way, as part of mathematics
- a coin with two tail sides do not destroy probability theory
- distinction:

What is Probability Theory?

- "Probability theory says that the coin gives heads and tails equally often"
- false, if probability theory is understood in modern way, as part of mathematics
- a coin with two tail sides do not destroy probability theory
- distinction:
 - Natural Science: do real coins behave according to model

What is Probability Theory?

- "Probability theory says that the coin gives heads and tails equally often"
- false, if probability theory is understood in modern way, as part of mathematics
- a coin with two tail sides do not destroy probability theory
- distinction:
 - Natural Science: do real coins behave according to model
 - Mathematics: the implications of the model

* implication – conclusion that can be drawn

Introduction to Discrete Math

What is Probability

Tossing Two Coins

Probability of 1 head or 1 tail?

Introduction to Discrete Math

What is Probability

- Probability of 1 head or 1 tail?
 - Janin starts

- Probability of 1 head or 1 tail?
 - Janin starts
 - four outcomes: *HH*, *HT*, *TH*, $TT \rightarrow 2/4$

- Probability of 1 head or 1 tail?
 - Janin starts
 - four outcomes: HH, HT, TH, $TT \rightarrow 2/4$
 - Pat arrives

- Probability of 1 head or 1 tail?
 - Janin starts
 - four outcomes: HH, HT, TH, $TT \rightarrow 2/4$
 - Pat arrives
 - three outcomes: $two\ heads$, head + tail, $two\ tails \rightarrow 1/3$

- Probability of 1 head or 1 tail?
 - Janin starts
 - four outcomes: HH, HT, TH, $TT \rightarrow 2/4$
 - Pat arrives
 - three outcomes: $two\ heads,\ head+tail,\ two\ tails \rightarrow 1/3$
 - Navid passes by

- Probability of 1 head or 1 tail?
 - Janin starts
 - four outcomes: HH, HT, TH, $TT \rightarrow 2/4$
 - Pat arrives
 - three outcomes: $two\ heads,\ head+tail,\ two\ tails \rightarrow 1/3$
 - Navid passes by
 - pure mathematician

- Probability of 1 head or 1 tail?
 - Janin starts
 - four outcomes: *HH*, *HT*, *TH*, $TT \rightarrow 2/4$
 - Pat arrives
 - three outcomes: $two\ heads,\ head+tail,\ two\ tails \rightarrow 1/3$
 - Navid passes by
 - pure mathematician
 - both correct, different assumptions since different models

- Probability of 1 head or 1 tail?
 - Janin starts
 - four outcomes: *HH*, *HT*, *TH*, $TT \rightarrow 2/4$
 - Pat arrives
 - three outcomes: $two\ heads,\ head+tail,\ two\ tails \rightarrow 1/3$
 - Navid passes by
 - pure mathematician
 - both correct, different assumptions since different models
 - Soheil drops by

- Probability of 1 head or 1 tail?
 - Janin starts
 - four outcomes: HH, HT, TH, $TT \rightarrow 2/4$
 - Pat arrives
 - three outcomes: $two\ heads$, head + tail, $two\ tails \rightarrow 1/3$
 - Navid passes by
 - pure mathematician
 - both correct, different assumptions since different models
 - Soheil drops by
 - an experimental observation point of view from real coins

- Probability of 1 head or 1 tail?
 - Janin starts
 - four outcomes: HH, HT, TH, $TT \rightarrow 2/4$
 - Pat arrives
 - three outcomes: $two\ heads,\ head+tail,\ two\ tails \rightarrow 1/3$
 - Navid passes by
 - pure mathematician
 - both correct, different assumptions since different models
 - Soheil drops by
 - an experimental observation point of view from real coins
 - Janin is more right

Galton Board: What did we assume?

At each level, half of the beans go left and half of them go right

- At each level, half of the beans go left and half of them go right
- Nothing but the truth, but not the entire truth

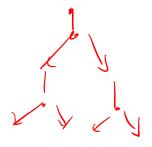
- At each level, half of the beans go left and half of them go right
- Nothing but the truth, but not the entire truth
- Imagine that the beans can remember left/right direction and it influences the next move

- At each level, half of the beans go left and half of them go right
- Nothing but the truth, but not the entire truth
- Imagine that the beans can remember left/right direction and it influences the next move
- May indeed happen in real life

- At each level, half of the beans go left and half of them go right
- Nothing but the truth, but not the entire truth
- Imagine that the beans can remember left/right direction and it influences the next move
- May indeed happen in real life
- But we assumed *independence*

- At each level, half of the beans go left and half of them go right
- Nothing but the truth, but not the entire truth
- Imagine that the beans can remember left/right direction and it influences the next move
- *May* indeed happen in real life
- But we assumed independence
- Among the beans that go left[right] at level 1

- At each level, half of the beans go left and half of them go right
- Nothing but the truth, but not the entire truth
- Imagine that the beans can remember left/right direction and it influences the next move
- May indeed happen in real life
- But we assumed *independence*
- Among the beans that go left[right] at level 1
 - half go left[right] at level 2



- At each level, half of the beans go left and half of them go right
- Nothing but the truth, but not the entire truth
- Imagine that the beans can remember left/right direction and it influences the next move
- *May* indeed happen in real life
- But we assumed *independence*
- Among the beans that go left[right] at level 1
 - half go left[right] at level 2
 - Etc...

Probability & Combinatronics – Probability

- Paradox of Probability Theory
- Galton Board
- Natural Sciences and Mathematics
- Rolling Dice
- More Examples

Introduction to Discrete Math

What is Probability

Rolling a Dice



https://wherethewindsblow.com/wp-content/uploads/2019/04/DSC_2954-x600.jpg

Natural Sciences:

Introduction to Discrete Math

What is Probability

Rolling a Dice



https://wherethewindsblow.com/wp-content/uploads/2019/04/DSC_2954-x600.jpg

• Natural Sciences: 1, 2, ..., 6 appear equally often

Rolling a Dice



https://wherethewindsblow.com/wp-content/uploads/2019/04/DSC_2954-x600.jpg

- Natural Sciences: 1, 2, ..., 6 appear equally often
- Mathematics: if it is the case:

Rolling a Dice



https://wherethewindsblow.com/wp-content/uploads/2019/04/DSC_2954-x600.jpg

- Natural Sciences: 1, 2, ..., 6 appear equally often
- Mathematics: if it is the case:
 - Even number appears in 50% of the cases

Introduction to Discrete Math

What is Probability

Rolling a Dice



https://wherethewindsblow.com/wp-content/ uploads/2019/04/DSC_2954-x600.jpg

- Natural Sciences: 1, 2, ..., 6 appear equally often
- Mathematics: if it is the case:

• Even number appears in
$$50\%$$
 of the cases $\begin{cases} 2, 4, 6 \end{cases} = \begin{cases} 3, 4 \end{cases}$
• A multiple of 3 appears in $1/3$ of the cases $\begin{cases} 3, 6 \end{cases} = \begin{cases} 3, 3 \end{cases}$

Rolling a Dice



https://wherethewindsblow.com/wp-content/uploads/2019/04/DSC_2954-x600.jpg

- Natural Sciences: 1, 2, ..., 6 appear equally often
- Mathematics: if it is the case:
 - Even number appears in 50% of the cases
 - A multiple of 3 appears in 1/3 of the cases
- Because

Rolling a Dice



https://wherethewindsblow.com/wp-content/uploads/2019/04/DSC_2954-x600.jpg

- Natural Sciences: 1, 2, ..., 6 appear equally often
- Mathematics: if it is the case:
 - Even number appears in 50% of the cases
 - A multiple of 3 appears in 1/3 of the cases
- Because
 - *3* favourable out of *6* equiprobable:

Rolling a Dice



https://wherethewindsblow.com/wp-content/uploads/2019/04/DSC_2954-x600.jpg

- Natural Sciences: 1, 2, ..., 6 appear equally often
- Mathematics: if it is the case:
 - Fiven number appears in 50% of the cases
 - A multiple of 3 appears in 1/3 of the cases
- \Because
 - 3 favourable out of 6 equiprobable: $(1, \frac{2}{2}, 3, \frac{4}{4}, 5, \frac{6}{6})$

Rolling a Dice



https://wherethewindsblow.com/wp-content/uploads/2019/04/DSC_2954-x600.jpg

- Natural Sciences: 1, 2, ..., 6 appear equally often
- Mathematics: if it is the case:
 - Even number appears in 50% of the cases
 - A multiple of 3 appears in 1/3 of the cases
- Because
 - 3 favourable out of 6 equiprobable: (1, 2, 3, 4, 5, 6)
 - 2 out of 6:

Rolling a Dice



https://wherethewindsblow.com/wp-content/uploads/2019/04/DSC_2954-x600.jpg

- Natural Sciences: 1, 2, ..., 6 appear equally often
- Mathematics: if it is the case:
 - Even number appears in 50% of the cases
 - A multiple of 3 appears in 1/3 of the cases
- Because
 - 3 favourable out of 6 equiprobable: (1, 2, 3, 4, 5, 6)
 - 2 out of 6: (1, 2, 3, 4, 5, 6)

Introduction to Discrete Math

What is Probability

Rolling Two Dice

Let's have a red and a blue dice

Introduction to Discrete Math

What is Probability

Rolling Two Dice

- Let's have a red and a blue dice
- Outcome (x, y) where x, y in 1, ..., 6

Rolling Two Dice

- Let's have a red and a blue dice
- Outcome (*x*, *y*) where *x*, *y* in 1, ..., 6
- Total number of outcomes:

Rolling Two Dice

- Let's have a red and a blue dice
- Outcome (*x*, *y*) where *x*, *y* in 1, ..., 6
- Total number of outcomes: *36*

Rolling Two Dice

- Let's have a red and a blue dice
- Outcome (*x*, *y*) where *x*, *y* in 1, ..., 6
- Total number of outcomes: 36
- Assumption:

Rolling Two Dice

- Let's have a red and a blue dice
- Outcome (*x*, *y*) where *x*, *y* in 1, ..., 6
- Total number of outcomes: 36
- Assumption: all 36 equiprobable

Rolling Two Dice

- Let's have a red and a blue dice
- Outcome (x, y) where x, y in 1, ..., 6
- Total number of outcomes: 36
- Assumption: all 36 equiprobable

```
11
          13
                14
                     15
                           16
21
     22
          23
                24
                           26
     32
          33
                34
                     35
31
                           36
                44
                     45
41
     42
          43
                           46
51
          53
                54
                     55
                           56
61
     62
          63
                64
                     65
                           66
```

What is Probability

Computing Probabilties

probability space

Computing Probabilties

• probability space: all outcomes

```
11
     12
           13
                14
                            16
21
     22
           23
                 24
                      25
                            26
31
     32
           33
                 34
                      35
                            36
     42
                 44
                      45
41
           43
                            46
51
                      55
     52
           53
                 54
                            56
61
     62
           63
                 64
                      65
                            66
```

- probability space: all outcomes
- event:

11	12	13	14	15	16
21	22	23	24	25	26
31	32	33	34	35	36
41	42	43	44	45	46
51	52	53	54	55	56
61	<mark>62</mark>	63	64	65	66

- probability space: all outcomes
- event: some outcomes(favourable)

```
fafes 0 3 3 1dia 51,2,3,4,5,6}
```

```
11
                14
     12
           13
                            16
21
     22
           23
                 24
                      25
                            26
31
     32
           33
                 34
                      35
                            36
41
     42
           43
                 44
                      45
                            46
51
     52
           53
                 54
                      55
                            56
61
     62
           63
                 64
                      65
                            66
```

- probability space: all outcomes
- event: some outcomes(favourable)
- example :

```
11
     12
           13
                14
                            16
21
     22
           23
                24
                      25
                            26
31
     32
           33
                34
                      35
                            36
                44
                      45
41
     42
           43
                            46
51
     52
           53
                54
                      55
                            56
61
     62
           63
                64
                      65
                            66
```

- probability space: all outcomes
- event: some outcomes(favourable)
- example: "more on red dice with higher value" (R > B)

```
11
            14
         13
                       16
<u>21</u>
    22
         23
              24
                  25
                       26
         33
              34
                  35
                       36
    42
         43
              44
                  45
                       46
51 52 53 54
                       56
61
    62
              64
                  65
                       66
```

- probability space: all outcomes
- event: some outcomes(favourable)
- example: "more on red dice with higher value" (R > B)

```
11
                14
     12
           13
                            16
     22
           23
                 24
                      25
                            26
     32
           33
                 34
                       35
                            36
           43
                 44
                       45
                            46
     52
           53
51
                 54
                       55
                            56
     62
           63
                 64
                       65
61
                            66
```

- probability space: all outcomes
- event: some outcomes(favourable)
- example: "more on red dice with higher value" (R > B)
- probability of this event in the model of equiprobable outcomes:

```
11
     12
           13
                 14
                            16
     22
           23
                 24
                       25
                            26
     32
           33
                 34
                       35
                            36
           43
                 44
                       45
                            46
     52
51
           53
                 54
                       55
                            56
                       65
61
     62
           63
                 64
                             66
```

- probability space: all outcomes
- event: some outcomes(favourable)
- example: "more on red dice with higher value" (R > B)
- probability of this event in the model of equiprobable outcomes : (#favourables) / 36 / 2941/105656

```
11 12 13 14 15 16
```

- probability space: all outcomes
- event: some outcomes(favourable)
- example: "more on red dice with higher value" (R > B)
- *probability* of this event in the model of equiprobable outcomes : (#favourables) / 36

```
14
                             16
11
           13
     22
           23
                 24
                       25
                             26
           33
                 34
                       35
                             36
           43
                 44
                       45
                             46
51
     52
           53
                 54
                       55
                             56
                       65
61
     62
           63
                 64
                             66
```

- probability space: all outcomes
- event: some outcomes(favourable)
- example: "more on red dice with higher value" (R > B)
- probability of this event in the model of equiprobable outcomes : (#favourables) / 36

```
14
                          15
                                 16
11
             13
      22
             23
                   24
                          25
                                 26
             33
                    34
                          35
                                       p = \frac{15}{36} = 0.4166 \approx 41.66\%
             43
                    44
                          45
51
      52
             53
                    54
                          55
                                 56
61
      62
             63
                    64
                          65
                                 66
```

What is Probability

Independence

```
11
     12
           13
                14
                      15
                           16
     22
                      25
21
           23
                24
                           26
     32
           33
                34
                      35
                           36
31
                44
                      45
41
     42
           43
                           46
51
     52
           53
                54
                           56
     62
           63
                64
                      65
61
                           66
```

More than equiprobability for both dice

Independence

11 22 33 44 55

• More than equiprobability for both dice

Independence

```
11
     12
           13
                 14
                       15
                            16
                       25
21
     22
           23
                 24
                            26
                       35
31
     32
           33
                 34
                            36
     42
           43
                 44
                       45
                            46
41
51
     52
           53
                 54
                       55
                            56
61
     62
           63
                 64
                       65
                            66
```

- More than equiprobability for both dice
- Simultaneous and sequential setting

Independence

```
11
     12
           13
                 14
                       15
                             16
21
     22
           23
                 24
                       25
                             26
31
     32
           33
                 34
                       35
                             36
     42
           43
                 44
                       45
41
                             46
51
     52
           53
                 54
                       55
                             56
     62
           63
                 64
61
                       65
                             66
```

- More than equiprobability for both dice
- Simultaneous and sequential setting
- Equiprobable model is usually OK for both settings

Probability & Combinatronics – Probability

- Paradox of Probability Theory
- Galton Board
- Natural Sciences and Mathematics
- Rolling Dice
- More Examples

What is Probability

Sequence of Coin Tosses

• Tossing a coin n times

What is Probability

- Tossing a coin n times
- Outcome:

What is Probability

- Tossing a coin n times
- Outcome: sequence of *n* bits

- Tossing a coin n times
- Outcome: sequence of *n* bits
- 2^n outcomes

- Tossing a coin *n* times
- Outcome: sequence of *n* bits
- 2^n outcomes
- Assumption :

- Tossing a coin n times
- Outcome: sequence of *n* bits
- 2^n outcomes
- Assumption : *equiprobable*

- Tossing a coin n times
- Outcome: sequence of *n* bits
- 2^n outcomes
- Assumption : *equiprobable*
- Probability of "all heads":

- Tossing a coin n times
- Outcome: sequence of *n* bits
- 2^n outcomes
- Assumption : *equiprobable*
- Probability of " $all\ heads$ ": $\frac{1}{2}$

- Tossing a coin n times
- Outcome: sequence of *n* bits
- 2^n outcomes
- Assumption : *equiprobable*
- Probability of " $all\ heads$ ": $\frac{1}{2}$
- Event:

- Tossing a coin n times
- Outcome: sequence of *n* bits
- 2^n outcomes
- Assumption : *equiprobable*
- Probability of "all heads": $\frac{1}{2}$
- Event: " $first\ bit = last\ bit$ "

- Tossing a coin n times
- Outcome: sequence of *n* bits
- 2^n outcomes
- Assumption : *equiprobable*
- Probability of " $all\ heads$ ": $\frac{1}{2}$
- Event: " $first\ bit = last\ bit$ "
 - Probability :

- Tossing a coin n times
- Outcome: sequence of *n* bits
- 2^n outcomes
- Assumption : *equiprobable*
- Probability of " $all\ heads$ ": $\frac{1}{2}$
- Event: " $first\ bit = last\ bit$ "
 - Probability: ½

- Tossing a coin n times
- Outcome: sequence of *n* bits
- 2^n outcomes
- Assumption : *equiprobable*
- Probability of "all heads": $\frac{1}{2}$
- Event: " $first\ bit = last\ bit$ "
 - Probability: ½
- "number of heads is even"

- Tossing a coin n times
- Outcome: sequence of *n* bits
- 2^n outcomes
- Assumption : *equiprobable*
- Probability of " $all\ heads$ ": $\frac{1}{2}$
- Event: " $first\ bit = last\ bit$ "
 - Probability: ½
- "number of heads is even"
 - Probability:

- Tossing a coin n times
- Outcome: sequence of *n* bits
- 2^n outcomes
- Assumption : *equiprobable*
- Probability of "all heads": $\frac{1}{2}$
- Event: " $first\ bit = last\ bit$ "
 - Probability: ½
- "number of heads is even"
 - Probability: ½

What is Probability

Galton Board Revisited

Outcomes:

What is Probability

Galton Board Revisited

• Outcomes : Sequences of L/R with length n

Introduction to Discrete Math

What is Probability

- Outcomes : Sequences of L/R with length n
- 2^n outcomes

- Outcomes : Sequences of L/R with length n
- 2^n outcomes
- Probability space

- Outcomes : Sequences of L/R with length n
- 2^n outcomes
- Probability space
- Assumption:

- Outcomes : Sequences of L/R with length n
- 2^n outcomes
- Probability space
- Assumption : *equiprobable*

Galton Board Revisited

- Outcomes : Sequences of L/R with length n
- 2^n outcomes
- Probability space
- Assumption : *equiprobable*
- Event:

•

- Outcomes : Sequences of L/R with length n
- 2^n outcomes
- Probability space
- Assumption : *equiprobable*
- Event: $\#R \in [0.4n, 0.6n]$

Galton Board Revisited

- Outcomes : Sequences of L/R with length n
- 2^n outcomes
- Probability space
- Assumption : *equiprobable*
- Event: $\#R \in [0.4n, 0.6n]$
- probability = (#favourable)/(#total)

•

- Outcomes : Sequences of L/R with length n
- 2^n outcomes
- Probability space
- Assumption : *equiprobable*
- Event: $\#R \in [0.4n, 0.6n]$
- probability = (#favourable)/(#total)

$$\sum_{k \in [0.4n, 0.6n]} \binom{n}{k} / 2^n$$

- Outcomes : Sequences of L/R with length n
- 2^n outcomes
- Probability space
- Assumption : *equiprobable*
- Event: $\#R \in [0.4n, 0.6n]$
- probability = (#favourable)/(#total)

Introduction to Discrete Math

What is Probability

Probability Theory = Combinatronics?

Not completely true

Introduction to Discrete Math

What is Probability

- Not completely true
- Only the mathematical part

- Not completely true
- Only the mathematical part
- Independence

- Not completely true
- Only the mathematical part
- Independence
- Non-uniform distributions

- Not completely true
- Only the mathematical part
- Independence
- Non-uniform distributions
- Unknown distributions

- Not completely true
- Only the mathematical part
- Independence
- Non-uniform distributions
- Unknown distributions
- Continuous distributions

Thank you.