## Content

<table>
<thead>
<tr>
<th>1</th>
<th>Understanding and analyzing algorithms</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Using graphs and graph algorithms</td>
</tr>
<tr>
<td>3</td>
<td>Using combinatorial reasoning to quantitatively analyze algorithms and systems</td>
</tr>
<tr>
<td>4</td>
<td>Using probability to algorithm analysis</td>
</tr>
</tbody>
</table>

### 4.1 Basics: Probability in Computer Science
- Experiments
- Sample Space
- Events
- Random Variables
- Expected Value
- Probability Distributions (Uniform and Binomial Distribution)

### 4.2 Probability and Counting

### 4.3 Conditional Probabilities

### 4.4 Birthday Paradox, Hashing and Randomized Algorithms
Basics
Probability is important in computer science, because sometimes
- the input is random (Data Mining, analyzing data from experiments),
- the desired output is random (picking a cryptographic key, performing a scientific simulation),
- the algorithm uses randomness (Monte Carlo methods, Search Heuristics, Randomized Hashing, Quicksort).
Probability in Computer Science

Probability is important in computer science, because sometimes

• the input is random
  (Data Mining, analyzing data from experiments),
• the desired output is random
  (picking a cryptographic key, performing a scientific simulation),
• the algorithm uses randomness
  (Monte Carlo methods, Search Heuristics, Randomized Hashing, Quicksort).

In Data Mining and Machine Learning,

algorithms are used to understand information and make predictions.

• These can be for elections, the weather, stock prices, or genetic indicators
  for diseases.
• Much of that **BIG DATA** information comes from some kind of randomized
  sampling: polls, statistics, random probes.
• An understanding of probability is needed to distinguish between valid
  predictions and overfitting to particular data.
Simulations

In simulations, you want to examine “typical” behaviour of a system, so you want to look at random events conditioned on a complex set of constraints. For example, the chart below shows the results of randomized stock price simulations, performed many times.
Randomized Algorithms

Sometimes randomness can be used by algorithms even when the answer we want is deterministic:

- For example, suppose you are trying to find the minimum possible value of a function.
- In the metropolis heuristic, random moves are combined with greedy moves to favor smaller values without getting stuck at local minima.
Basic Definitions and Examples

Experiments
- Toss a coin
- Roll a die
- Penalty
- Shootout
- Sunshine
- today

Sample Space and Events
A subset $E$ of $S$ is called an event, and we define the probability of $E$, by $\text{Prob}[E] = \sum_{s \in E} p_s$.

Random Variables
Formally, a random variable $X = F(s)$ is determined by a function $F : S \to \mathbb{R}$. The distribution for $X$ is $p_v = \text{Prob}[X = v]$ for each possible value $v$.

Probability Distributions
A probability distribution is an assignment of probabilities $0 \leq p_s \leq 1$ to each element of a sample space $S$ so that $\sum_{s \in S} p_s = 1$. 
Basic Definitions and Examples

<table>
<thead>
<tr>
<th>Experiments</th>
<th>Toss a coin</th>
<th>Roll a die</th>
<th>Penalty</th>
<th>Sunshine</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Shootout</td>
<td>today</td>
</tr>
</tbody>
</table>

Sample Space and Events

Random Variables

Probability
Distributions
For example, consider the sample space of all possible outcomes of a six-sided die, and let each have probability $1/6$. We identify the event “the die roll is even,” with the set of outcomes where that is true:

$$\{2, 4, 6\}$$

and the total probability of that event,

$$\text{Prob}[\text{Even}] = 1/6 + 1/6 + 1/6 = 1/2.$$
A particularly natural type of distribution is the *uniform* distribution, where all outcomes are equally likely, i.e.,
\[ p_s = \frac{1}{|S|} \text{ for all } s \in S. \]

This distribution, where the sample space is \{0 heads, 1 head, ..., n heads\}, is called the *binomial distribution*, because the probabilities are proportional to the binomial coefficients.
Binomial Distribution

\[ n=5 \text{ (Shots on the goal)} \]
\[ \pi=70\% \quad \text{(Prob. for Goal)} \]
\[ (1-\pi)=30\% \quad \text{(Prob. for No-Goal)} \]

\[ P(X=5)= P(GGGGG)=0.7^5=16.81\% \]
\[ P(X=0)= P(NNNNN)=0.3^5=0.24\% \]
\[ P(X=4)= P(GGGGN)+ P(GGGNG)+ P(GGGGG)+ P(GGNGG)+ P(GNGGG)+ P(NGGGG) = 5 \times 0.7^4 \times 0.3^1 = 36.02\% \]
\[ P(X=1)= P(GNNNN)+ P(NGNNN)+ P(NNGNN)+ P(NNNNG)+ P(NNNNG)+ P(NNNNG)+ P(NGGGG)= 5 \times 0.7^1 \times 0.3^4 = 2.84\% \]
\[ P(X=2)= P(GGNNN)+ P(GGNNN)+ P(NGNNN)+ P(NNGNN)+ P(NNGGN)+ P(NNNGN)+ P(NGNGN)+ P(NGNNG)+ P(NNNGN)+ P(NNGGN)+ P(NGGGG)= 10 \times 0.7^2 \times 0.3^3 = 13.23\% \]
\[ P(X=3)= P(GGNNN)+ P(GGNNN)+ P(NGNNN)+ P(NNGNN)+ P(NNGGN)+ P(NNNGN)+ P(NGNGN)+ P(NGNNG)+ P(NNNGN)+ P(NNGGN)+ P(NNGNN)+ P(NGGGG)= 10 \times 0.7^3 \times 0.3^2 = 30.87\% \]
Expected Value of a Random Variable

We often want to look at the average or expected value of a random variable.

The expectation of $X$, written $E[X]$, is defined to be

$$E[X] = \sum_v v \cdot \text{Prob}[X = v]$$

where the sum is over all possible outcomes $v$ of the variable $X$.

<table>
<thead>
<tr>
<th>Penalty Shootout</th>
<th>Roll a die</th>
<th>Toss a coin</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0,24% 0,00</td>
<td>0 50,00% 0,00</td>
</tr>
<tr>
<td>1</td>
<td>2,84% 0,03</td>
<td>1 50,00% 0,50</td>
</tr>
<tr>
<td>2</td>
<td>13,23% 0,26</td>
<td>0,50 Exp.Value</td>
</tr>
<tr>
<td>3</td>
<td>30,87% 0,93</td>
<td>4 16,67% 0,67</td>
</tr>
<tr>
<td>4</td>
<td>36,02% 1,44</td>
<td>5 16,67% 0,83</td>
</tr>
<tr>
<td>5</td>
<td>16,81% 0,84</td>
<td>6 16,67% 1,00</td>
</tr>
<tr>
<td></td>
<td>100,01% 3,50 Exp.Value</td>
<td>100,00% 3,50 Exp.Value</td>
</tr>
</tbody>
</table>
Example

20% of all notebooks must be repaired during the first two years. What is the probability that out of 5 notebooks

a) 0
b) exactly 1
c) 1 or more

have to be repaired in the first two years?
Hypothesis testing

When hypotheses are tested for statistical signficancy, the probability for an error that one decides that the hypothesis is true although the hypothesis is false is often set to $\alpha=5\%$. That is, in 5\% of all cases one decides that a hypothesis is true although it is false.

What is the probability that in 10 independent tests of a hypothesis this hypothesis is

a) never
b) exactly one time
c) at most two times

assumed to be true although it is false?
Probability and Counting
Computing probabilities is very connected to counting. If we start with the uniform distribution on a set \( S \), and look at the probability of an event \( E (E \subseteq S) \), then

\[
\text{Prob}[E] = \frac{|E|}{|S|}.
\]

To generalize the distribution before, if we flip \( n \) fair coins (i.e., the uniform distribution on sequences of length \( n \)), what will the probability of getting exactly \( k \) heads be?

**Caution:** You must have each outcome equally likely to use this reasoning.
Example

Suppose 5-card hands are dealt at random from a standard deck of 52. What is the probability that your hand contains exactly two Aces?
Example

Suppose 5-card hands are dealt at random from a standard deck of 52. What is the probability that your hand contains exactly two Aces?

Solution:

\[
\binom{4}{2} \quad \text{2 aces out of 4 possible aces}
\]
\[
\binom{48}{3} \quad \text{3 cards out of 48 (no aces)}
\]
\[
\binom{52}{5} \quad \text{5 cards out of 52}
\]
Example

Suppose 5-card hands are dealt at random from a standard deck of 52. What is the probability that your hand contains exactly two Aces?

Solution:

\[ \begin{align*}
\text{C}(4, 2) & \quad 2 \text{ aces out of 4 possible aces} \\
\text{C}(48, 3) & \quad 3 \text{ cards out of 48 (no aces)} \\
\text{C}(52, 5) & \quad 5 \text{ cards out of 52} \\
\end{align*} \]

\[ \frac{\text{C}(4, 2) \times \text{C}(48, 3)}{\text{C}(52, 5)} = \frac{(47 \times 46 \times 4 \times 3 \times 10)}{(52 \times 51 \times 50 \times 49)} = 3.99\% \]
Example

A rise in a permutation of the numbers \{1,\ldots,n\} occurs when a larger number immediately follows a smaller one. For example, if n=5, the permutation 1\ 3\ 2\ 4\ 5 has three rises. What is the expected number of rises in a permutation of size n?
Example

A rise in a permutation of the numbers \(\{1, \ldots, n\}\) occurs when a larger number immediately follows a smaller one. For example, if \(n=5\), the permutation 1 3 2 4 5 has three rises. What is the expected number of rises in a permutation of size \(n\)?

Solution:
The expected number of rises from position \(i\) to \(i+1\) is \(1/2\) ("linearity of expectations").
We have \(n-1\) instances of this, therefore the expected number of rises in a permutation of size \(n\) is \((1/2) \times (n-1)\).
Example

A rise in a permutation of the numbers \{1,\ldots,n\} occurs when a larger number immediately follows a smaller one. For example, if n=5, the permutation 1\ 3\ 2\ 4\ 5 has three rises. What is the expected number of rises in a permutation of size n?

Solution:
The expected number of rises from position i to i+1 is 1/2 ("linearity of expectations").

We have n-1 instances of this, therefore the expected number of rises in a permutation of size n is \(\frac{1}{2} \times (n-1)\).

Example (n=3):  
\[
\begin{array}{c|c}
\text{123} & 2 \\
\text{132} & 1 \\
\text{213} & 1 \\
\text{231} & 1 \\
\text{312} & 1 \\
\text{321} & 0 \\
\end{array}
\]
Conditional Probabilities
Conditional Probabilities

If we initially have a certain probability distribution on outcomes, but then learn something about the actual outcome, this changes our thinking according to the Conditional Probability Law.

The conditional probability of an outcome $s$, given an event $E$, written $\text{Prob}[s|E]$ is

- 0 if $s \not\in E$, and
- $\frac{p_s}{\text{Prob}[E]}$ otherwise.

So if I roll a die, and I don’t look at it, my initial probability distribution is that each of 6 outcomes has probability $1/6$. But if you tell me the result is even, my new probability distribution is that each of 2, 4 and 6 have probability $1/3$. 
Conditional Probability Law

More generally, the Conditional Probability Law says how to update probabilities of one event $B$ if we discover that another event $A$ has taken place:

**Theorem (Conditional Probability Law)**

For any events $A, B$,

$$
Prob[B \mid A] = \frac{Prob[A \land B]}{Prob[A]}. 
$$

Often, we use this in the other direction:

**Theorem (Conditional Probability Law)**

For any events $A, B$,

$$
Prob[A \land B] = Prob[A]Prob[B \mid A].
$$
Problem

Here's a puzzle that stumps many people, although it's just a simple calculation. Assume that initially boys and girls are equally likely.

1. Ms. X has two children. If you know the oldest is a girl:
   What is the probability that both are girls? Answer: 50%

2. Mr. Y has two children. If you know that one of them is a boy:
   What is the probability that both are boys? Answer: 33%

What is the sample space?
bb, bg, gb, gg

What is our initial distribution on the sample space?
Each element of the sample space has probability 1/4 (the uniform distribution).
Problem

We know Ms. X's oldest child is a girl. So if we list the children in age order, we are conditioning on the event \( A = \{gb, gg\} \).

The event we want the probability for is \( B = \{gg\} \).

\[
\begin{align*}
Prob[B|A] &= \frac{Prob[A \land B]}{Prob[A]} \\
&= \frac{1/4}{1/2} \\
&= 1/2.
\end{align*}
\]

We know one of Mr. Y's children is a boy. So if we list the children in age order, we are conditioning on the event \( A = \{bb, gb, bg\} \).

The event we want the probability for is \( B = \{bb\} \).

\[
\begin{align*}
Prob[B|A] &= \frac{Prob[A \land B]}{Prob[A]} \\
&= \frac{1/4}{3/4} \\
&= 1/3.
\end{align*}
\]
Example

A bitstring of length 4 is generated randomly one bit at a time. So far, you can see that the first bit is a 1. What is the probability that the string will have at least two consecutive 0's?
Example

A bitstring of length 4 is generated randomly one bit at a time. So far, you can see that the first bit is a 1. What is the probability that the string will have at least two consecutive 0's?

Solution:
We are conditioning on the event $A=\{\text{first bit is a } 1\}$. The event we want the probability for is $B=\{\text{at least two consecutive } 0\text{'s}\}$. 
Example

A bitstring of length 4 is generated randomly one bit at a time. So far, you can see that the first bit is a 1. What is the probability that the string will have at least two consecutive 0's?

Solution:
We are conditioning on the event $A=\{\text{first bit is a 1}\}$.
The event we want the probability for is $B=\{\text{at least two consecutive 0's}\}$.

$P(A) = 1/2$
$P(A \text{ and } B) = 3/16$ (last 3 bits must be 000 or 001 or 100)
$P(B|A) = P(A \text{ and } B) / P(A) = 3/16 \div 1/2 = 3/8$
Simpson’s Paradox (1/2)

In the early 1970's, UC Berkeley was sued under the Equal Opportunity Act. The plaintiffs showed that only 35% of women who applied to graduate school were accepted in 1973, compared to 45% of men who applied. The University countered by showing that, in every department, the percentage of women who were accepted was at least as large as the percentage of men who were accepted.

How are both of these possible at the same time?

We have three events for random applicants: Male, Female, Accepted. We know

\[
\text{Prob}[\text{Accepted}|\text{Male}] > \text{Prob}[\text{Accepted}|\text{Female}].
\]

But for each department,

\[
\text{Prob}[\text{Accepted}|\text{Male, Department}] \leq \text{Prob}[\text{Accepted}|\text{Female, Department}].
\]

Is this possible?
We can show this phenomenon is possible by giving a situation where it occurs.

<table>
<thead>
<tr>
<th>Math Department</th>
<th>English Department</th>
</tr>
</thead>
<tbody>
<tr>
<td>60% of females accepted</td>
<td>20% of females accepted</td>
</tr>
<tr>
<td>50% of males accepted</td>
<td>10% of males accepted</td>
</tr>
</tbody>
</table>

300 females apply for Math, and 700 for English. 700 males apply for Math, and 300 for English.
Birthday Paradox, Hashing and Randomized Algorithms
Birthday TODAY

Find the smallest number of people you need to choose at random so that the probability that at least one of them has a birthday today exceeds 1/2.
Birthday TODAY

Find the smallest number of people you need to choose at random so that the probability that at least one of them has a birthday today exceeds 1/2.

Solution:
Assuming a year has 365 days, the probability of someone not having a birthday today is 364/365.
Given n people, the probability of them having a birthday today is (364/365)^n.
Birthday TODAY

Find the smallest number of people you need to choose at random so that the probability that at least one of them has a birthday today exceeds 1/2.

Solution:
Assuming a year has 365 days, the probability of someone not having a birthday today is 364/365.
Given n people, the probability of them having a birthday today is (364/365)^n.
So we need 1 – (364/365)^n >= 1/2, or n >= log_(364/365) 1/2, so n >= 253.
Birthday Paradox

What is the minimum number of people who need to be in a room so that the probability that at least two of them have the same birthday is greater than 50%?

We make the following assumptions: The birthdays of the people in the room are independent, each birthday is equally likely, there are 366 days in the year.
Birthday Paradox

What is the minimum number of people who need to be in a room so that the probability that at least two of them have the same birthday is greater than 50%?

We make the following assumptions: The birthdays of the people in the room are independent, each birthday is equally likely, there are 366 days in the year.

\[ X = \text{“at least two out of } n \text{ people in a room have the same birthday“} \]
\[ P(X) = 1 - P(Y) \]
\[ Y = \text{“all } n \text{ people in the room have different birthdays“} \]
\[ P(Y) = \frac{365}{366} \times \frac{364}{366} \times \frac{363}{366} \times \ldots \times \frac{367-n}{366} \]
# Birthday Paradox

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1,000</td>
<td>0,000</td>
</tr>
<tr>
<td>2</td>
<td>0,997</td>
<td>0,003</td>
</tr>
<tr>
<td>3</td>
<td>0,995</td>
<td>0,008</td>
</tr>
<tr>
<td>4</td>
<td>0,992</td>
<td>0,016</td>
</tr>
<tr>
<td>5</td>
<td>0,989</td>
<td>0,027</td>
</tr>
<tr>
<td>6</td>
<td>0,986</td>
<td>0,040</td>
</tr>
<tr>
<td>7</td>
<td>0,984</td>
<td>0,056</td>
</tr>
<tr>
<td>8</td>
<td>0,981</td>
<td>0,074</td>
</tr>
<tr>
<td>9</td>
<td>0,978</td>
<td>0,094</td>
</tr>
<tr>
<td>10</td>
<td>0,975</td>
<td>0,117</td>
</tr>
<tr>
<td>11</td>
<td>0,973</td>
<td>0,141</td>
</tr>
<tr>
<td>12</td>
<td>0,970</td>
<td>0,167</td>
</tr>
<tr>
<td>13</td>
<td>0,967</td>
<td>0,194</td>
</tr>
<tr>
<td>14</td>
<td>0,964</td>
<td>0,223</td>
</tr>
<tr>
<td>15</td>
<td>0,962</td>
<td>0,252</td>
</tr>
<tr>
<td>16</td>
<td>0,959</td>
<td>0,283</td>
</tr>
<tr>
<td>17</td>
<td>0,956</td>
<td>0,314</td>
</tr>
<tr>
<td>18</td>
<td>0,954</td>
<td>0,346</td>
</tr>
<tr>
<td>19</td>
<td>0,951</td>
<td>0,378</td>
</tr>
<tr>
<td>20</td>
<td>0,948</td>
<td>0,411</td>
</tr>
<tr>
<td>21</td>
<td>0,945</td>
<td>0,443</td>
</tr>
<tr>
<td>22</td>
<td>0,943</td>
<td>0,475</td>
</tr>
<tr>
<td>23</td>
<td>0,940</td>
<td>0,506</td>
</tr>
<tr>
<td>24</td>
<td>0,937</td>
<td>0,537</td>
</tr>
<tr>
<td>25</td>
<td>0,934</td>
<td>0,568</td>
</tr>
<tr>
<td>26</td>
<td>0,932</td>
<td>0,597</td>
</tr>
<tr>
<td>27</td>
<td>0,929</td>
<td>0,626</td>
</tr>
<tr>
<td>28</td>
<td>0,926</td>
<td>0,653</td>
</tr>
<tr>
<td>29</td>
<td>0,923</td>
<td>0,680</td>
</tr>
<tr>
<td>30</td>
<td>0,921</td>
<td>0,705</td>
</tr>
<tr>
<td>31</td>
<td>0,918</td>
<td>0,729</td>
</tr>
<tr>
<td>32</td>
<td>0,915</td>
<td>0,752</td>
</tr>
<tr>
<td>33</td>
<td>0,913</td>
<td>0,774</td>
</tr>
<tr>
<td>34</td>
<td>0,910</td>
<td>0,794</td>
</tr>
<tr>
<td>35</td>
<td>0,907</td>
<td>0,813</td>
</tr>
<tr>
<td>36</td>
<td>0,904</td>
<td>0,831</td>
</tr>
<tr>
<td>37</td>
<td>0,902</td>
<td>0,848</td>
</tr>
<tr>
<td>38</td>
<td>0,899</td>
<td>0,863</td>
</tr>
<tr>
<td>39</td>
<td>0,896</td>
<td>0,877</td>
</tr>
<tr>
<td>40</td>
<td>0,893</td>
<td>0,891</td>
</tr>
<tr>
<td>41</td>
<td>0,891</td>
<td>0,903</td>
</tr>
<tr>
<td>42</td>
<td>0,888</td>
<td>0,913</td>
</tr>
<tr>
<td>43</td>
<td>0,885</td>
<td>0,923</td>
</tr>
<tr>
<td>44</td>
<td>0,883</td>
<td>0,932</td>
</tr>
<tr>
<td>45</td>
<td>0,880</td>
<td>0,940</td>
</tr>
<tr>
<td>46</td>
<td>0,877</td>
<td>0,948</td>
</tr>
<tr>
<td>47</td>
<td>0,874</td>
<td>0,954</td>
</tr>
<tr>
<td>48</td>
<td>0,872</td>
<td>0,960</td>
</tr>
<tr>
<td>49</td>
<td>0,869</td>
<td>0,965</td>
</tr>
<tr>
<td>50</td>
<td>0,866</td>
<td>0,970</td>
</tr>
</tbody>
</table>
Birthday Paradox

What is the minimum number of people who need to be in a room so that the probability that at least two of them have the same birthday is greater than 50%?

We make the following assumptions: The birthdays of the people in the room are independent, each birthday is equally likely, there are 366 days in the year.

\[ X = \text{“at least two out of n people in a room have the same birthday“} \]
\[ P(X) = 1 - P(Y) \]
\[ Y = \text{“all n people in the room have different birthdays“} \]
\[ P(Y) = \frac{365}{366} \times \frac{364}{366} \times \frac{363}{366} \times \ldots \times \frac{367-n}{366} \]

For \( n=22 \), \( P(X)=0.475 \).
For \( n=23 \), \( P(X)=0.506>50\% \).
For \( n=47 \), \( P(X)>95\% \).
Applications

The Pollard-Rho algorithm for the factorization of integers makes use of the Birthday Paradox.

The Birthday Paradox has also applications in the analysis of randomized algorithms, e.g. Hashing.
Hashing

Why Hashing?

- Hashing-based data structures implement dictionaries (abstract data type that supports insert(x), delete(x), search(x)).
- Hashing is a space-saving Direct Storage.

Direct Storage

Store key x in table A at position A[x] – with the following disadvantages:
- table can become very large
- even if we should be able to get a table, we will waste a lot of storage when we only store a small number of keys compared to the size of the table

Hashing

Use m separate lists instead of one huge list. A „hash function“ transforms every possible key x into a list number h(x) between 0 and m-1:

\[ h(x): U \to \{0, 1, \ldots, m-1\} \]
Collisions

A **collision** occurs when more than one key is assigned to a memory location, i.e. when two keys \( x \) and \( y \in U, x \neq y \), are hashed on the same value of the hashtable: \( h(x) = h(y) \) for \( x, y \in U, x \neq y \).

**Chaining** is one of several approaches to augmenting a hash table to resolve collisions. In chaining, each memory location holds a pointer to a linked list, initialized to be empty. When we hash an input to a location, we add the input to the list in that location. Collisions still hurt us, but only in that we take more time traversing a linked list.
How many Collisions?

In the best case, there are no collisions at all, $h$ is injective (static dictionaries can do that with perfect hashing).

In the worst case, all of the $n$ keys are hashed to the exactly same position in the hash table.

Both possibilities are unlikely. We need the following analysis.

1. **Average-case analysis**
   Choose the keys in a way that the probability for a collision is only $1/m$. („Randomness lies by the user“)

2. **Universal Hashing**
   Choose the hash function randomly so that the algorithm behaves well for all possible key sets. („Randomness lies by the algorithm“)
Average-case analysis

Assumptions:
1. The keys are chosen randomly out of $U$.
2. $h$ distributes the keys evenly to the places of the hash table.

What follows:
The number of keys from $U$ that are hashed to a specific value between 0 and $m-1$ is

$$\frac{|U|}{m}$$

(the keys are hashed in every slot with the same probability).

Therefore:
$$P(h(x)=h(y)) = \frac{\#\text{hits}}{\#\text{possibilities}} = \frac{|U|/m}{|U|} = \frac{1}{m}$$

Costs of an operation: $O(t+n/m)$ - $t$ are the costs to compute $h(x)$
Universal Hashing (Carter/Fredman 1979)

The hash function $h: U \rightarrow \{0, \ldots, m-1\}$ is chosen randomly out of the set $H_0$ of all possible functions from $U$ to $\{0, \ldots, m-1\}$.

What follows:
The number of functions from $H_0$ that yield to a collision between two different keys $x$ and $y \in U$, is

$$|H_0|/m$$

Therefore:
P($h(x)=h(y)$) = #hits / #possibilities = $|H_0|/m / |H_0| = 1/m$

Costs of an operation: $O(t+n/m)$ - $t$ are the costs to compute $h(x)$