**Tutorial 5**

**For all mathematical workings, please use Microsoft Word** [**Equation**](https://support.microsoft.com/en-us/office/write-an-equation-or-formula-1d01cabc-ceb1-458d-bc70-7f9737722702)**.**

**1 ) What is the formula for r-permutation of n distinct objects?**

A permutation of n distinct objects is an arrangement or ordering of the n objects.

A r-permutation of n distinct objects is an arrangement using r of the n objects.

**2 ) What is the 1-permutation for letter ‘abc’?**

The 1-permutation of letters ‘abc’ are:

a,b,c

**3 ) What is the 2-permutation for letter ‘abc’?**

The 2-permutation of letters ‘abc’ are :

ab, ac, ba, bc, ca, cb

**4 ) How many 3 digit numbers can be made using numbers 1 to 9 if no numbers can be repeated?**

**5 ) What is the formula to compute distinguishable n permutations?**

Distinguishable permutations =

**6 ) How many permutations of ‘aabc’ are there?**

Permutation of aabc are:

aabc, aacb, abac, abca, acab, acba,

aabc, aacb, abac, abca, acab, acba,

baac, baca, caab, caba, bcaa, cbaa

baac, baca, caab, caba, bcaa, cbaa

However, we noted a lot of repeated entries as we cannot tell one ‘a’ apart from the other.

Total permutation of ‘a’ =

Distinguishable permutations of ‘aabc’ =

**7 ) Supposed a coin is tossed 7 times. How many sequences of 4 heads and 3 tails are possible?**

Permutations of HHHHTTT = = 35

**8 ) What is the formula for r combination of n distinct objects?**

With permutation, order is important.

With combination, we are looking at a subset of objects.

A r-combination of n distinct objects is an unordered selection of r of the objects.

**9 ) What are the possible 2 letters combinations for ‘abc”?**

The 2 combinations of ‘abc’ are:

ab,ac,bc

**10) Refer to SIM-CSCI262-DistinguishablePermutationObjects**

**Suppose we have a number of letters:**

**1 W, 3 Os, 2 Ls, 2 Ns, and 2 Gs.**

**How many ways are there to arrange the letters?**

Applying the formula

>>> import math

>>> numerator = math.factorial(10)

>>> denom=math.factorial(3)\*math.factorial(2)\*\*3

>>> numerator/denom

75600.0

11 ) Refer to SIM-CSCI262-Puzzle02(Std).pdf

Read Spring 2016, Part C -Question 2

This explains how client puzzle works.

j is the number of sub puzzle

Client will receive y[j] and L-k bits of the x[j], also known as the pre-image

Client need to find the k missing bits

s is a secret known by the server. As such, client need to bruteforce search, i.e try all permutation of k bits

How difficult the client puzzle is, is dependent on the value k, i.e the number of missing bits

**Refer to SIM-CSCI262-Puzzle.pdf**

You need to understand how m, the number of sub messages and k, the number of puzzle bits, affects Expected number of hash, standard deviation and variance.

Compute the Expected value of the number of hashes required, when m = 1:

Let i be the number of hashes required

Let be the worst case number of hashes required

**12 ) Refer to Client Puzzle Distribution.pptx**

**This explains Week 7 page 45 lecture notes where we compute the distribution of hashes required for the client to solve the puzzle.**

m is the number of sub puzzles

k is the number of bits that are missing from the puzzle

Compute for

m=1,k=4

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| # Hashes | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| Cases m=1, k=4 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |

Columns needed =

m=4,k=2

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| # Hashes | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| Cases m=4, k=2 | 0 | 0 | 0 | 1 | 4 | 10 | 20 | 31 | 40 |  |  |  |  |  |  |  |

Columns needed =

1 to 3 = 0; Given that there is 4 sub puzzle, minimally, 4 hashes are required

4 = 1; All sub puzzle gets it right in the first pass

5 = Combination of {2,1,1,1} = 4C1 \* 3C3 = 4

6 = Combination of {3,1,1,1} or {2,2,1,1} = 4C1\*3C3 + 4C2\*2C2 = 4+6=10

7 = Combination of {4,1,1,1} or {3,2,1,1} or {2,2,2,1}

= 4C1\*3C3 + 4C1\*3C1\*2C2 + 4C3 = 20

8 = Combination of ~~{5,1,1,1}~~ or {4,2,1,1} or {3,3,1,1} or {3,2,2,1} or {2,2,2,2}

However, if k=2, max hashes required , there {5,1,1,1} is invalid.

= 4C1\*3C1\*2C2 + 4C2\*2C2 + 4C1\*3C2\*1C1 + 4C4

= 12 + 6 + 12 + 1 = 31

9 = Combination of ~~{6,1,1,1}~~ or ~~{5,2,1,1}~~ or {4,3,1,1} or {4,2,2,1} or {3,3,2,1} or {3,2,2,2}

= 4C1\*3C1\*2C2 + 4C1\*3C2\*1C1 + 4C2\*2C1 + 4C1\*3C3

= 12+12+12+4 = 40

…

m=2,k=3

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| # Hashes | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| Cases m=2, k=3 | 0 | 1 | 2 | 4 | 4 | 6 | 6 | 8 | 8 |  |  |  |  |  |  |  |

Columns needed =

1=0; Given that there is 2 sub puzzle, minimally, 2 hashes are required.

2 = {1,1} = 1

3 = Combination of {2,1} = 2C1 = 2

4 = Combination of {3,1} or {2,2} = 2C1\* 1C1 + 2C1\*1C1 = 4

5 = Combination of {4,1} or {3,2} = 2C1 + 2C1 = 4

6 = Combination of {5,1} or {4,2} or {3,3} = 2C1 + 2C1 + 2C1 = 6

7 = Combination of {6,1} or {5,2} or {4,3} = 6

8 = Combination of {7,1} or {6,2} or {5,3} or {4,4} = 8

9 = Combination of {8,1} or {7,2} or {6,3} or {5,4} = 8

10 = Combination of ~~{9,1}~~ or {8,2} or {7,3} or {6,4} or {5,5} = …

…

**13 ) Refer to SIM-CSCI262-StatisticalInference**

How to subtract the outcome of one query from another to infer about anonymized values