Contents

Why Learn to Count?

- Probability is "the likelihood of something happening" - OED
    - Perform an experiment several times
    - We need to be able to count the number of times the outcome we're interested in happens
    - Divide this by the number of experiments to get the frequency ("probability") with which it occurs

Aside: What about events that can only happen once? We'll come back to this later.

Example: In a family of two children, where the oldest child is a girl, what is the probability that both are girls?

- Toss a coin twice. What is the probability of two heads?
    - Possible outcomes are TT, TH, HT, HH. So expect two heads seen 1 time in 4
    - What about the probability of one head and one tail?
- Now toss a coin 10 times...what is the prbability of two heads now?
- Instead of tossing coins, think of errors in packets transmitting over a wireless link
- Or hash table collisions
- Or chance of guessing a well chosen password

Sum Rule of Counting

- Suppose we have a set `A` of `n` outcomes and a set `B` of `m` outcomes
- Suppose no outcome in `A` is in `B` and vice versa

- Suppose an experiment is performed by drawing one outcome from *either* `A` or `B`
- For the experiments together there are `m+n` possible outputs
- Just enumerate the possible outcomes of the experiment: `1, 2, ..., n, n+1, ..., n+m`
- In set notation, number of outcomes it `|A|+|B|`

Example:

- Suppose we have two sets of servers, one in Dublin and one in London, with 100 servers in Dublin and 50 server in London
- A web request arrives and must be routed to one of the servers. How large is the set of servers that is may get routed to?
- Request can be sent to either of the two location, none of the machines in either location is the same. So sum rules applies and the request could potentially be routed to any of the 150 (= 100+50) servers

Generalised Sum Rule of Counting for 2 Sets

Some examples:

- Suppose we have a set `A` of `n` outcomes and a set `B` or `m` outcomes
- Some outcomes in `A` may also be in `B`, and vice versa
- Suppose an experiment is performed by drawing one outcome from *either* `A` or `B`
- For the experiments togethere there are `|A|+|B|-|A∩B|` possible outputs
- When `|A∩B|` is the empty set we have the basic sum rule of counting
- This is also called the **inclusion-exclusion principle*

Example:

- An 8 bit string is sent over a network. The valid set of strings recognised by the receiver must start 01 or end with 10. How many valid strings are there?
- Set `A` is the set of possible strings that begin with 01. `|A|=64` since of the 8 bits 2 are fixed while the remaining 6 bits can take on binary values, so there are 2^6=64 such strings
- Set `B` is the set of possible strings that end with 10. `|B|=64` since of the 8 bits 2 are fixed
- `|A∩B|` is the set of possible strings that begin with 01 and end with 10. Since there are 4 bits fixed only 4 out of the 8 can very so there are 2^4=16 such srings, i.e. `|A∩B|=16`
- By the generalised sum rule, there are `112=|A|+|A|-|A∩B|=64+64-16` such strings

Product Rule of Counting

- Suppose two experiments are performed
- Experiment 1 can result in any one of `m` possible outcomes
- Experiment 2 can result in any one of `n` possible outcomes
- For the two experiments together there are `mn` possible outputs
- Just enumerate the possible outcomes for the pair of experiments: `(1, 1)`, `(1, 2)`, `...` `(1, n)`, `(2, 1)`, `(2, 2)`, `...` `(m, 1)`, `(m, 2)`, `...` `(m, n)`

Example:

- A byte consists of 8 bits. Each bit takes the value 0 or 1. How many different bytes are there?
- The first bit takes one of 2 possible values. The second bit takes one of 2 possible values, and so on.
- So the total number of potential byte values is $2 \times 2 \times 2 \times 2 ... \times 2 = 2^8 = 256$

Example:

- Consider a hash table with 100 buckets. Two arbitrary strings are independently hashed and added to the table. How many possible ways are there for the strings to be stored in the table?
- Each string can be hashed to one of 100 buckets. Since the results of hashing the first string do not affect the second, there are $100 \times 100 = 10,000$ ways that the two strings may be stored in the hash table

Generalised Product Rule of Counting

- Suppose `r` experiments are performed
- Experiment 1 can result in any one of n_1 possible outcomes
- Experiment 2 can result in any one of n_2 possible outcomes
- And so on...
- For the `r` experiments together, there are $n_1 \times n_2 \times ... \times n_r$ possible outcomes

Example:

- Suppose I choose a password of length 4 using letters a-z
- Number of possible passwords in $26 \times 26 \times 26 \times 26 = 456,976$
- Now suppose I use letters a-z and A-Z
- Number of possible passwords is not $52 \times 52 \times 52 \times 52 = 7,311,616$
- Letters a-z, A-Z and numbers 0-9
- Number of possible passwords is now $62 \times 62 \times 62 \times 62 = 14,776,336$
- Suppose its a length of 6. Number of wasswords is $62^6 = 5 \times 10^{10}$