The Product Principle Revisited

Formalising the Count of Valid Passwords

Prof Hans Georg Schaathun

Høgskolen i Ålesund

Autumn 2013 – Part 1/Session 3/Video 1B
Recorded: July 7, 2014

Passwords

A password (for some computer system) is between four and eight characters long (inclusive), and composed of lowercase and/or uppercase letters (26-letter alphabet).

1. *How many passwords are possible?*
2. *What counting principle(s) do you use?*
3. *What percentage of valid passwords have exactly four letters?*

paraphrased from Stein et al. Section 1.2

HØGSKOLEN I ÅLESUND
Aalesund University College

Formalising notation

- The password (x_1, x_2, x_3, x_4) is a tuple (or list) of four elements from A
- The set of four-letter passwords is often written

$$P_4 = A \times A \times A \times A = A^4$$

- The product principle implies that

$$\left|A^4\right| = |A|^4$$

- In general,

$$P_i = A \times A \times \ldots \times A = A^i$$

- and

$$\left|A^i\right| = |A|^i$$

Definition

The notation $A \times B$ for sets A and B is known as a Cartesian product.

Product Principle

Version 2

If a set S of lists of length m has the properties that

1. there are i_1 choices for the first element in the lists, and
2. for each $j > 1$, and each choice of the first $j-1$ elements in the list, there are i_j choices for position j,

then

$$|S| = i_1 i_2 \cdots i_m = \prod_{k=1}^{m} i_k.$$

- The big letter Π is called Product Notation
- Analogous to the *Sum Notation* Σ
- Read $\prod_{k=a}^{b} x_k$ as the 'product of x_k from a to b'.

HØGSKOLEN I ÅLESUND
Aalesund University College

Exercise

For security reasons, we often want to make the password space (set of valid passwords) as large as possible.

Still considering passwords of four to eight characters, how much larger does the password space become if we allow digits as well as the 52 upper and lower case letters?

Give the answer as a factor. E.g. the new password space is x times larger than the old one.

HØGSKOLEN I ÅLESUND
Aalesund University College