Using Sum and Product Principles

Counting valid passwords

Prof Hans Georg Schaathun

Høgskolen i Ålesund

Autumn 2013 – Part 1/Session 3/Video 1
Recorded: August 21, 2013

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

Step 1: Partitioning

Q 1 How many passwords are possible?

- Let P be the set of all valid passwords.

  How do we partition P?

- Let P_i be the set of i-letter passwords.

$$P = P_4 \cup P_5 \cup P_6 \cup P_7 \cup P_8$$

- Treating one subset P_i at a time, we get rid of one variable
  - fixed number of letters to choose

Step 1: Partitioning

Q 1 How many passwords are possible?

- Let P be the set of all valid passwords.

  How do we partition P?

- Let P_i be the set of i-letter passwords.

$$P = P_4 \cup P_5 \cup P_6 \cup P_7 \cup P_8$$

- Treating one subset P_i at a time, we get rid of one variable
  - fixed number of letters to choose

Step 2: Counting the first component

How many four-letter passwords are possible?

$A = \{a, b, \dots z, A, B, \dots Z\}$ $\quad |A| = 52$

- Choose one letter at a time
  - Let A be the case-sensitive alphabet
  - $|A| = 52$

$(x_1 x_2 x_3 x_4)$

$W_{x_1} = \{(x_1, x_2 x_3 x_4) \mid x_2, x_3, x_4 \in A\}$ $\quad \times 52$

$\boxed{W_{x_1 x_2}}$

$W_{x_1} = \bigcup_{x \in A} W_{x_1 x}$

1. Choose first letter $x_1 \in A$; 52 choices.
2. Given x_1, choose second letter from $x_2 \in A_{x_1} = A$; 52 choices
3. Given x_2, choose second letter from $x_3 \in A_{x_1 x_2} = A$; 52 choices
4. Given x_3, choose second letter from $x_4 \in A_{x_1 x_2 x_3} = A$; 52 choices

$W_{x_1 x_2 x_3} = \{(x_1 x_2 x_3 y) \mid y \in A\}$

$W_{x_1 x_2} = \bigcup_{x \in A} W_{x_1 x_2 x}$

$|W_{x_1 x_2 x_3}| = 52$

$|W_{x_1 x_2}| = 52 \cdot 52$

- Applying the product principle, we get

$$|P_4| = 52 \cdot 52 \cdot 52 \cdot 52 = 52^4$$

$|W_{x_1}| = 52 \cdot 52 \cdot 52$

$|P_4| = 52^4$

Step 2: Counting the first component

How many four-letter passwords are possible?

- Choose one letter at a time
  - Let A be the case-sensitive alphabet

$$|A| = 52$$

1. Choose first letter $x_1 \in A$; 52 choices.
2. Given x_1, choose second letter from $x_2 \in A_{x_1} = A$; 52 choices
3. Given x_2, choose second letter from $x_3 \in A_{x_1 x_2} = A$; 52 choices
4. Given x_3, choose second letter from $x_4 \in A_{x_1 x_2 x_3} = A$; 52 choices

- Applying the product principle, we get

$$|P_4| = 52 \cdot 52 \cdot 52 \cdot 52 = 52^4$$

Step 3: Generalising

How many i-letter passwords are possible?

1. 52 choices for one letter
2. Having chosen $i-1$ letters, we have 52 choices for the ith one
3. Thus, by the product principle,

$$
\begin{aligned}
|P_5| &= |P_4| \cdot 52 = 52^5 \\
|P_6| &= |P_5| \cdot 52 = 52^6 \\
|P_7| &= |P_6| \cdot 52 = 52^7 \\
|P_8| &= |P_7| \cdot 52 = 52^8
\end{aligned}
$$

4. In general $|P_i| = |P_{i-1}| \cdot 52 = 52^i$
5. or $|P_i| = 52^i$

We have used a trick known as recursion, which we will discuss formally at a later stage.

HØGSKOLEN I ÅLESUND
Aalesund University College

Step 4: Putting it all together

The sum principle

How many passwords are possible with four to eight letters?

- We have a partitioning

$$P = P_4 \cup P_5 \cup P_6 \cup P_7 \cup P_8$$

- The sum principle applies

$$\begin{aligned} |P| &= |P_4| \cup |P_5| \cup |P_6| \cup |P_7| \cup |P_8| \\ &= 52^4 + 52^5 + 52^6 + 72^5 + 52^8 \\ &= 54\,507\,958\,359\,296 \end{aligned}$$

Step 4: Putting it all together

The sum principle

How many passwords are possible with four to eight letters?

- We have a partitioning

$$\boxed{P = P_4 \cup P_5 \cup P_6 \cup P_7 \cup P_8}$$

- The sum principle applies

$$\begin{aligned}
|P| &= |P_4| \cancel{\cup} + |P_5| \cancel{\cup} + |P_6| \cancel{\cup} + |P_7| \cancel{\cup} + |P_8| \\
&= 52^4 + 52^5 + 52^6 + \cancel{52^5}\, 52^7 + 52^8 \\
&= \underline{54\,507\,958\,359\,296}
\end{aligned}$$

Counting principles

Q 2 What counting principle(s) do you use?

Answer We need both the sum and the product principle.

Percentage of short passwords

Q 3 What is percentage of valid passwords have exactly four letters?

$$\frac{|P_4|}{|P|} = \frac{52^4}{52^4 + 52^5 + 52^6 + 52^7 + 52^8}$$
$$= \frac{7\,311\,616}{54\,507\,958\,359\,296}$$
$$\approx 0.0000134\%.$$

HØGSKOLEN I ÅLESUND Aalesund University College

Percentage of short passwords

Q 3 What is percentage of valid passwords have exactly four letters?

$$\frac{|P_4|}{|P|} = \boxed{\frac{52^4}{52^4 + 52^5 + 52^6 + 52^7 + 52^8}}$$

$$= \frac{7\,311\,616}{54\,507\,958\,359\,296}$$

$$\approx \underline{0.0000134\%}.$$

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.