Dr. J's Guide to Permutations with replacement

Fundamental Rule of Counting

Definition

The Fundamental Rule of Counting states that if there are a ways of doing something **and** b ways of doing something else, then there are $a \times b$ ways of doing those two things.

Examples:

- If you roll a 6-sided die and flip a coin, there are $6 \times 2 = 12$ ways for the die and coin to appear.
- If there are 12 ice cream flavors, 5 ice cream toppings, and 3 ice cream cones, there are $12 \times 5 \times 3 = 180$ different combinations of flavors, toppings, and cones.

Intuition behind the formula for permutations with replacement

Definition

A permutation with replacement is an ordered set of k elements taken from a set of n elements where elements can be repeated.

How many choices do we have for the

- first item? n
- second item? n
- $\vdots$
- kth item? n

By the Fundamental Rule of Counting, we have

$$\underbrace{n \times n \times \cdots \times n}_{k \text{ times}} = n^k$$

of ways to choose these items.

Simple passwords

fecghtsfwa

How many passwords of length 10 using lowercase English letters are there?

- Initial set: $n = 26$ because there are 26 English letters.
- Final set: $k = 10$ because the password has 10 digits.

Thus there are

$$26^{10} \approx 10^{14}$$

unique passwords.

More complex passwords

Passwords can be made more complex by

- increasing their length and
- increasing the digits that can be used.

A 20-digit, lowercase-only password has

$$26^{20} \approx 10^{28}$$

possible passwords.

A 10-digit, lowercase and uppercase password has

$$(26 + 26)^{10} \approx 10^{17}$$

possible passwords.

More complex passwords

Most password policies

- allow password lengths in a range and
- letters, numbers, and symbols.

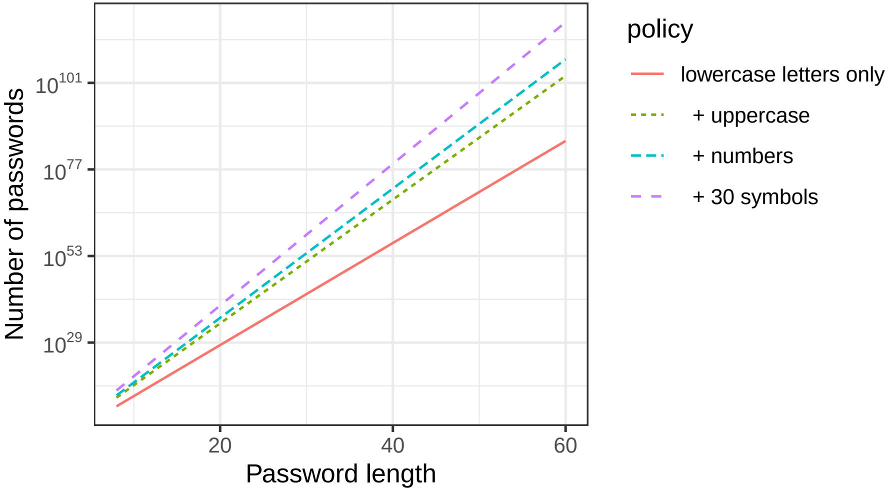
A password policy that allows letters (both uppercase and lowercase), numbers, and these 30 symbols (!@#$%^&*()_+-=[]\{}|;':",./<>?) and allows 8-20 digits has

$$
\begin{aligned}
& 92^{8} + 92^{9} + \cdots + +92^{19} + 92^{20} \\
& \approx 10^{16} + 10^{18} + \cdots + 10^{37} + 10^{39} \\
& \approx 10^{39}
\end{aligned}
$$

possible passwords.

Complex passwords

Number of passwords as a function of password length



Summary

- Fundamental Rule of Counting
- Intuition behind permutation with replacement formula: n^k
- Applied the formula to determine number of passwords under various policies: