Tutorial 1
Passwords

Learning Objectives

> In this tutorial you will be comparing the security of different password systems. The number of possible passwords relates directly to the security of the system - the more passwords there are, the harder it is to find the correct one by brute force.
>
> These problems relate to the following course learning objectives: *Select and justify appropriate tools to analyze a counting problem, analyze a counting problem by proving an exact or approximate enumeration, or a method to compute one efficiently*, and *identify when an exact solution is intractable, and use estimates to describe its approximate size.*

ALPs

The Android Lock Pattern (ALP) is a password system where the user draws a path on a 3×3 grid of points. The path starts at any point, and connects $4 - 9$ points with straight lines. Each point may be used only once, and an unused point cannot be jumped.

Alternatively, a PIN is a string of digits $0 - 9$, with repetition allowed, and is between 4 and 6 digits in length.

1. How may PINs are there of length 4? How many of length 6?
2. Are there more or less ALPs than length 6 PINs?
3. Are there more or less ALPs than length 4 PINs?
4. Computing the exact number of ALPs requires some programming. Suppose someone gave you a list claiming to count the exact number of patterns of each length. Which two lengths should have the same number of patterns?

UTORid

Three years ago, the UTORid password policy changed from requiring exactly 8 characters to requiring 10-32. The allowed symbols come from 4 character sets: 26 lower case letters, 26 upper case letters, 10 numbers, and 24 punctuation marks.

A new password can be "short" (10-15 characters, using at least 3 sets), "intermediate" (16-19, using at least two sets), or "easy to type" (20-32 characters, using at least one set).

5. How many passwords were possible under the old 8 character policy, using any characters from any set? Are there more or fewer passwords if we require at least one character from each set?
6. How many "easy to type" passwords are there using only numbers? Is this more or less than the number of "short" passwords? (Hint: Counting the exact number of short passwords may be difficult until we learn Inclusion-Exclusion).

1. There are 10^4 and 10^6 PINs of those lengths.

2. Encoding the path as a string of digits, we want to estimate the number of strings of length 4 to 9 using 9 characters at most once each. This is

$$\sum_{i=4}^{9} P(9,i) = 985824,$$

which gives an upper bound for the number of lock patterns, so there are more PINs of length 6.

3. Each path has 9 options to start, and from any position, at most half of the remaining points are blocked, so at least half of them can be the next point in the path. This gives a lower bound of

$$9\cdot 4\cdot 4\cdot 3 + 9\cdot 4\cdot 4\cdot 3\cdot 3 + \cdots + 9\cdot 4\cdot 4\cdot 3\cdot 3\cdot 2\cdot 2\cdot 1\cdot 1 = 19872,$$

so there are more lock patterns than PINs of length 4.

4. The number of patterns of length 8 must be equal to the number of length 9, since every pattern of length 8 can be uniquely extended to one of length 9 by adding the remaining point, and every pattern of length 9 comes from a unique pattern of length 8.

5. There are 86^8 possible passwords with no restrictions. Any restriction necessarily lowers the number of possible passwords by making some unacceptable, so there are fewer if we require one character from each set (which they did!)

6. The number of easy to type passwords using only digits is

$$10^{20} + 10^{21} + \cdots + 10^{32} = \frac{10^{33} - 10^{20}}{9}.$$

This number is 13 ones followed by 20 zeros, and is a bit more than 10^{32}. The number of short passwords is bounded above by the number of strings of length $10-15$ using all 86 characters,

$$86^{10} + \cdots + 86^{15} = \frac{86^{16} - 86^{10}}{85} < 10^{30},$$

so there are more easy to type passwords.