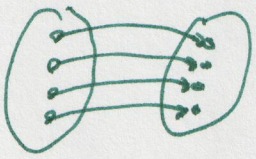
A.

$f: A \to B$ is a bijection if it is one-to-one and onto.
(injective) (surjective)

- one-to-one: for each $y \in B$ there is at most one $x \in A$ s.t. $f(x) = y$.
- onto: for each $y \in B$ there is at least one $x \in A$ s.t. $f(x) = y$.



Bijection Rule: If there exists a bijection $f: A \to B$ then $|A| = |B|$

Product Rule:

A = "the set of possible executions of a procedure P"

B = "the set we want to know the size of"

X = "an n-element set"

P(X) = the set of all subsets of X

$X = \{a, b, c\}$.

$P(X) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a,b\}, \{a,c\}, \{b,c\}, \{a,b,c\}\}$.

Theorem: For any n-element set X, $|P(X)| = 2^n$.

Proof: Let $X = \{x_1 \ldots x_n\}$.

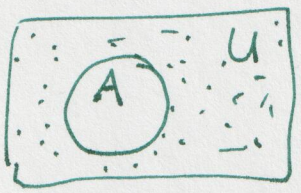
For any $S \subseteq X$, define the bitstring ~~$b_1 \ldots b_n$ where~~

$f(S) = b_1 \ldots b_n$ where $b_i = \begin{cases} 0 & \text{if } x_i \notin S \\ 1 & \text{if } x_i \in S. \end{cases}$

Then f is a bijection from P(X) onto binary strings of length n.

Can also prove using product Rule.

Complement Rule: If $A \subseteq U$ then $|A| = |U| - |U \setminus A|$



Example: Password is a string of 8 characters over the alphabet $\Sigma = \{a, b, \ldots, 0, 1, 2, \ldots 9\}$. that contains at least one digit.

S: "the set of all passwords"

U = "all 8-character strings over Σ"

$|\Sigma| = 36$

$|U| = 36^8$ · (Product Rule).

$U \setminus S$ = "all 8 character strings with no digits."
= "8 character strings over $\{a, b, c, \ldots z\}$."

$|U \setminus S| = 26^8$

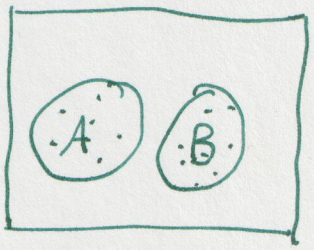
$\therefore |S| = |U| - |U \setminus S| = 36^8 - 26^8 = 2,612,282,842,880$

Not resistant to brute force.

The Sum Rule.

If A and B are disjoint, then $|A \cup B| = |A| + |B|$

If $A_1 \dots A_n$ are pairwise disjoint then $|A_1 \cup \dots \cup A_n| = |A_1| + |A_2| + \dots + |A_n|$.



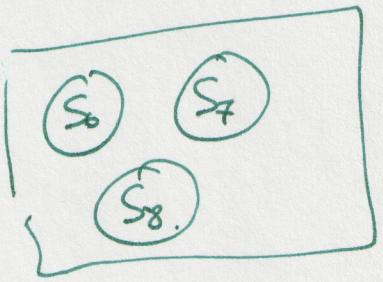
Example: A valid password is any string of length 6, 7, or 8 over the alphabet $\Sigma = \{a, \dots z, 0, \dots 9\}$ ~~where~~ that contains at least one character.

For each $n \in \{6, 7, 8\}$, let S_n be the set of valid passwords of length n.

$S = S_6 \cup S_7 \cup S_8$ so $|S| = |S_6 \cup S_7 \cup S_8| = |S_6| + |S_7| + |S_8|$

$= 36^6 - 26^6 + 36^7 - 26^7 + 36^8 - 26^8$

$= 2,684,483,063,360.$



P. I-E (3 sets).

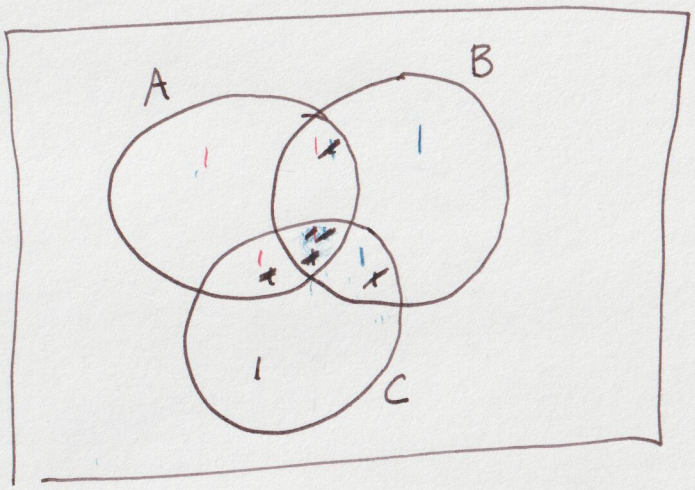
For any sets A, B, and C $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$.

- same problem (bitstrings).

C = length-17 bitstrings with 01 at positions 6 & 7.

$|C| = 2^{15}$.

C = ⊔⊔⊔⊔⊔01⊔⊔⊔⊔⊔⊔⊔⊔⊔⊔ (5, 10).



$|A \cup B \cup C| = 2^{14} + 2^{15} + 2^{15} - 2^{12} - 2^{12} - 2^{13} + 2^{10} = 66,560$.

$|A \cap C| = 2^{12}$ = 111⊔⊔01⊔⊔⊔⊔⊔⊔⊔⊔ (2, 10)

$|B \cap C| = 2^{13}$ = ⊔⊔⊔⊔⊔01⊔⊔⊔⊔⊔⊔⊔⊔00 (5, 8)

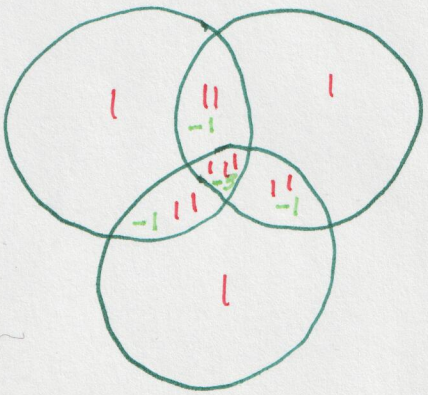
$|A \cap B \cap C| = 2^{10}$ = 111⊔⊔01⊔⊔⊔⊔⊔⊔⊔⊔00 (2, 8)

Principle Inc-Exc For 3 sets.

For any 3-sets A, B, C

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$

General formula for n-terms has $2^n - 1$ terms.



Example: ~~Bit~~ Length-17 bitstrings again or have 1's at positions ~~6~~, 7, 8.

$|A| = 2^{14}$

$|B| = 2^{15}$

$|C| = 2^{15}$

$|A \cap B| = 2^{12}$

$|B \cap C| = 2^{13}$

$|A \cap C| = 2^{12}$

$|A \cap B \cap C| = 2^{10}$.

$$|A \cup B \cup C| = 2^{14} + 2^{15} + 2^{15} - 2^{12} - 2^{13} - 2^{12} + 2^{10}$$

$$= 66,560.$$