Lemma. A function $f: A \to B$ has

(i) a left inverse iff f is one-to-one

(ii) a right inverse iff f is onto

Proof of (i):

($\Rightarrow$) Suppose that g is left-inverse of f.

Consider a_1, a_2 s.t. $f(a_1) = f(a_2)$

$$a_1 = 1_A(a_1) = (g \circ f)(a_1) = g(f(a_1))$$

$$= g(f(a_2)) = 1_A(a_2) = a_2$$

($\Leftarrow$) Suppose f is one-to-one.

Show f has left inverse $g: B \to A$.

Define

$$g(b) = \begin{cases} a & \text{if } f(a) = b \\ a_0 & \text{if } b \text{ is not in the image of } f \end{cases}$$

Here a_0 is any element of A.

g is well-defined because f is one-to-one.

$(g \circ f)(a) = g(f(a)) = a$ for all $a \in A$. $\square$

Proof of (ii) in Asn 1.

Lemma. If $f: A \to B$ has a left inverse g and a right inverse h then $g = h$ and it is the unique inverse function of f.

Proof. Suppose that f has left inverse $g: B \to A$, and, right inverse $h: B \to A$.

Now

$$h = 1_A \circ h = (g \circ f) \circ h =$$

↑ associativity of function composition

$$= g \circ (f \circ h) = g \circ 1_B = g$$

□

Equivalence relations

Consider $R \subseteq A \times A$. R is an equivalence relation if

(i) $I_A \subseteq R$ (reflexive)

(ii) $R^{-1} \subseteq R$ (symmetric)

(iii) $R \circ R \subseteq R$ (transitive)

Example. Congruence modulo n, $n \in \mathbb{N}$

$x \equiv y \mod n$ if n divides $x - y$

Claim. Congruence modulo n is a equivalence relation.

Consider equiv. relation $R \subseteq A \times A$.

Equivalence class of element $a \in A$:

$$[a]_R = \{ b \in A \mid (a,b) \in R \}$$

Lemma. $R \subseteq A \times A$ is equiv. relation.

(i) $a \in [a]_R$

(ii) $[a]_R = [b]_R$ iff $(a,b) \in R$

(iii) $[a]_R \cap [b]_R \neq \emptyset$ iff $(a,b) \in R$

use transitivity

The above implies that equiv. classes of R form a **partition** of the set A.

Partition of A is a collection of disjoint non-empty subsets whose union is A.

Example: $A = \{1, 2, 3, 4, 5, 6, 7\}$

Partition of A: $\{1, 2, 4\}, \{3, 6\}, \{5, 7\}$

Corresponding equiv. relation:

$\{(1,1), (2,2), (4,4), (1,2), (2,1), (1,4),$
$(4,1), (2,4), (4,2), (3,3), (6,6), (3,6),$
$(6,3), (5,7), (7,5), (5,5), (7,7)\}$

Basics of combinatorics:

counting, permutations, combinations

Example. BestBuy has the following brands of laptops:

HP : 5 models

Lenovo : 4 models

Acer : 7 models

Dell : 5 models

Apple : 3 models

- How many choices for a model a customer has? (24)
- A customer buys one model of each brand. How many choices does the customer have?

210 choices

Product rule

- event A has m choices
- event B has n choices
- the two events are independent

Total number of choices: $m \cdot n$

More generally:

$A_1, \ldots, A_k$ are finite sets

$$|A_1 \times \ldots \times A_k| = |A_1| \cdot |A_2| \cdot \ldots \cdot |A_k|$$

Example. How many one-to-one functions $A \to B$ there are when $|A| = m$, $|B| = n$?

(i) $m > n$: 0

(ii) $m \leq n$

mapping first element has n choices

" second " " $n-1$ "

⋮

" m^{th} " " $n-m+1$ "

Product rule:

$n(n-1)(n-2)\cdots(n-m+1)$ choices

Sum rule

If an event can occur either in one of m ways, or in one of n ways where none of the set of m ways is the same as any of the set of n ways, then the event can occur in total in $m+n$ ways.

If A and B are disjoint finite sets

then $|A \cup B| = |A| + |B|$

If $A_1, \ldots, A_k$ are pairwise disjoints finite sets

$$|A_1 \cup \ldots \cup A_k| = \sum_{i=1}^{k} |A_i|$$

Example. A password is 6–8 characters long. Each character is an upper or a lower case letter or a digit, and the password has at least one digit.
How many possible passwords there are?

P = total number of passwords

P_i = number of passwords of length i, $i = 6, 7, 8$

Sum rule:

$$P = P_6 + P_7 + P_8$$

$$P_6 = 62^6 - 52^6$$

$$P_7 = 62^7 - 52^7$$

$$P_8 = 62^8 - 52^8$$

Example. How many bit strings of length 8 either

(i) begin with 1, or,

(ii) end with 00. (or both.)

A = set of length 8 bit strings that begin with 1

$|A| = 2^7$

B = set of length 8 bit strings that end with 00

$|B| = 2^6$

$|A \cap B| = 2^5$

$|A \cup B| = 2^7 + 2^6 - 2^5 = 128 + 64 - 32$

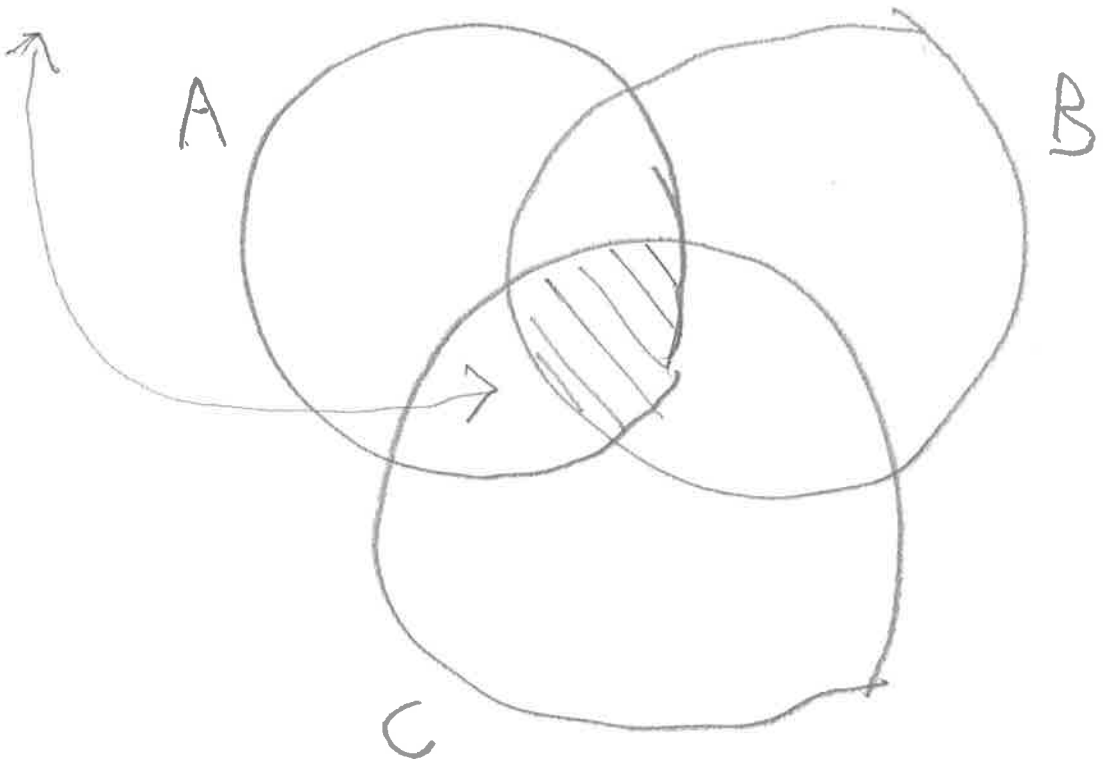
$= 160$

Inclusion-exclusion principle

Size of union of not neccesarily disjoint sets.

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

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



Example. $A = \{1, 2, 3, 5, 8, 13\}$

$B = \{3, 4, 5, 6\}$

$C = \{5, 6, 7 8\}$

$|A \cup B \cup C| = 9$

$|A| = 6, \quad |B| = |C| = 4$

$|A \cap B| = 2 \quad |A \cap C| = 2$

$|B \cap C| = 2$

$= 9$

$|A \cup B \cup C| = 6 + 4 + 4 - 2 - 2 - 2$

$+ 1$

General form of inclusion-exclusion:

$$\left|\bigcup_{i=1}^{m} A_i\right| = \sum_{k=1}^{m} (-1)^{k+1} \left(\sum_{1 \le i_1 < \cdots < i_k \le m} |A_{i_1} \cap \cdots \cap A_{i_k}| \right)$$

$m = 4$:

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

Pigeon-hole principle

- p pigeons live in a coop divided into h holes
- If $p > h$, then more than one pigeon live in the same hole.

Example. $A = \{1, 2, 3, \ldots, 9\}$

What is the smallest number of elements of A we need to select to be sure that two (*) of the selected numbers add up to 10?

(*) the two numbers can be the same

Pairs of numbers that add up to 10:

1, 9
2, 8
3, 7
4, 6
5, 5

Smallest number of elements is 6

Example. Lossless compression of files, i.e., bit strings.

Claim: For each $n \in \mathbb{N}$ there exists a bit string of length n that cannot be compressed.

Proof: Consider an arbitrary compression function comp(·) on bit strings.

The function comp(·) has to be one-to-one.

The number of bit strings of length n: 2^n

The number of bit strings of length less than n:

$$1 + 2 + 2^2 + \dots + 2^{n-1} = \frac{2^n - 1}{2 - 1} = 2^n - 1$$

Pigeonhole: comp(·) cannot be one-to-one.

Geometric series $(r \neq 1)$

$$a + ar + ar^2 + \dots + ar^{n-1} = a\left(\frac{1 - r^n}{1 - r}\right)$$

$a = 1$

$r = 2$

Generalized pigeon-hole principle

If n elements are partitioned into m subsets, then some subset contains $\lceil \frac{n}{m} \rceil$ elements.

Proof. For the sake of contradiction assume that all subsets contain at most $\lceil \frac{n}{m} \rceil - 1$ elements.

Now

$$n \leq m \cdot \left(\left\lceil \frac{n}{m} \right\rceil - 1 \right) < m \cdot \left(\frac{n}{m} + 1 - 1 \right)$$

$$= n$$

This is a contradiction. □

Example. A discrete mathematics class has 13 possible grades A+, A, ..., D−, F

What is the minimum number of students required to guarantee that 5 students receive the same grade?

Smallest value for n s.t.

$$\left\lceil \frac{n}{13} \right\rceil \geq 5$$

$$4 \cdot 13 + 1 = 53 \qquad \left\lceil \frac{53}{13} \right\rceil = 5$$

Example. Consider a group A of six people where each pair of people are either friends or enemies.

Show that A must have 3 people who are all either mutual friends or all mutual enemies.

Fix one person P in the group A.

Pigeon-hole: the set $A - \{P\}$ must have $\lceil \frac{5}{2} \rceil$ elements that are all friends or all enemies of P.

- Assume that P_1, P_2, P_3 are all enemies of P. a) If P_i, P_j, $i \neq j$, are mutual enemies, then P, P_i, P_j are all mutual enemies.
  b) If P_1, P_2, P_3 are all mutual friends, then this is the triple.
- The possibility where P_1, P_2, P_3 are all friends of P is symmetric.