$f : [n] \longrightarrow [k]$

$\boxed{B^A} = \{ f : A \longrightarrow B \}$

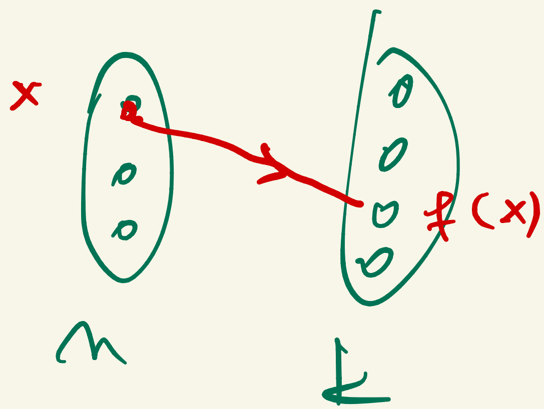
NOTATION

$\left| [k]^{[n]} \right| = k^n$

$\mathrm{dom}(f) = A$

$\mathrm{codom}(f) = B$

$|A| = n \qquad |B| = k$



$$0 \le |\mathrm{coll}(f)| \le \binom{n}{2} = \frac{n(n-1)}{2}$$

collision for f : $\{x, y\} \subseteq \mathrm{dom}(f)$ $\quad x \neq y$

s.t. $\quad f(x) = f(y)$

$$\mathrm{coll}(f) = \{ \{x, y\} \mid x, y \in \mathrm{dom}(f), x \neq y, f(x) = f(y) \}$$

$f : [n] \to [k]$

$$0 \le |\mathrm{coll}(f)| \le \binom{n}{2} = \frac{n(n-1)}{2}$$

$\uparrow$

<u>tight</u> for every n and k

except ...

meaning: $(\exists f)\left(|\mathrm{coll}(f)| = \binom{n}{2}\right)$

demonstrated by [WHAT FUNCTION f?]

the <u>constant</u> functions, for example

$$(\forall x \in \mathrm{dom})(f(x) = 1)$$

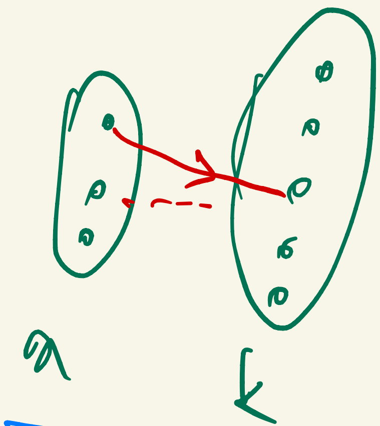
except: $k=0$ codom $= \emptyset$ not tight: $\nexists f$ to demonstrate tightness

except when also $\cancel{\binom{n}{2} = 0}$ i.e. $n = 0$ ~~or 1~~ $\leftarrow$ $\boxed{\text{error in class}}$

$\hookrightarrow n = 0$

DEF f is an <u>injection</u> if $\mathrm{coll}(f) = 0$

$$\left|\{f : [n] \to [k] \text{ injection}\}\right| = \underbrace{k(k-1)\cdots(k-n+1)}_{\#\text{terms} \,=\, n}$$



NAIVE PROBABILITY

$$P\left(\text{random function } f \text{ is an injection}\right) = \frac{\#\text{injections}}{\#\text{functions}} = \frac{k(k-1)\cdots(k-n+1)}{k^n}$$

Birthday paradox crossover point $n \approx \sqrt{k}$

FINITE PROBABILITY SPACES

(Ω, P)

Ω : non-empty finite set ← for this course

Sample space

elements of Ω: "elementary events"

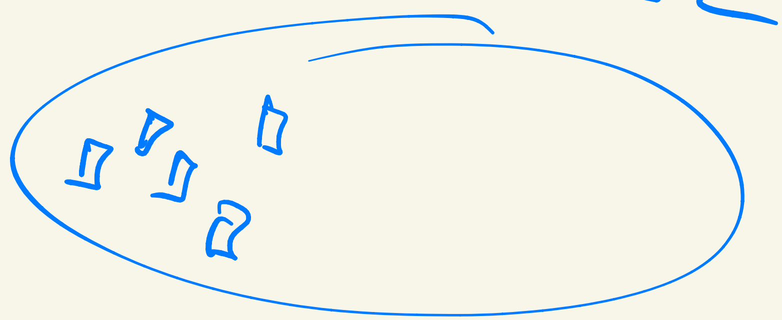
$P : \Omega \to \mathbb{R}$

probability distribution

for $a \in \Omega$ we say:

$P(a)$ is the probability of the elementary event $\underline{a}$

Ω



Axioms:

$$(\forall a \in \Omega)(P(a) \geq 0)$$

$$\sum_{a \in \Omega} P(a) = 1$$

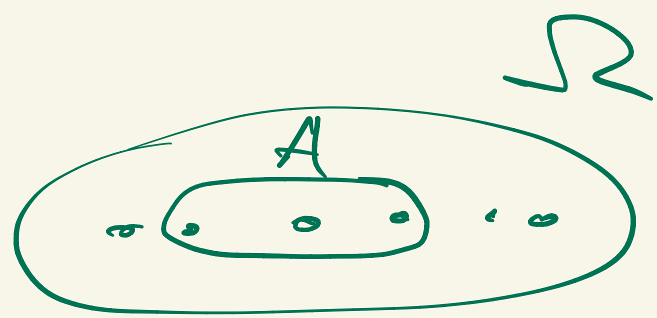
p5

Event $A \subseteq \Omega$

DEF
$$\boxed{P(A) = \sum_{a \in A} P(a)}$$

HW study standard deck of 52 cards

If $|\Omega| = n$ then
#events $= 2^n$



HW Can all these 2^n events have different probabilities?

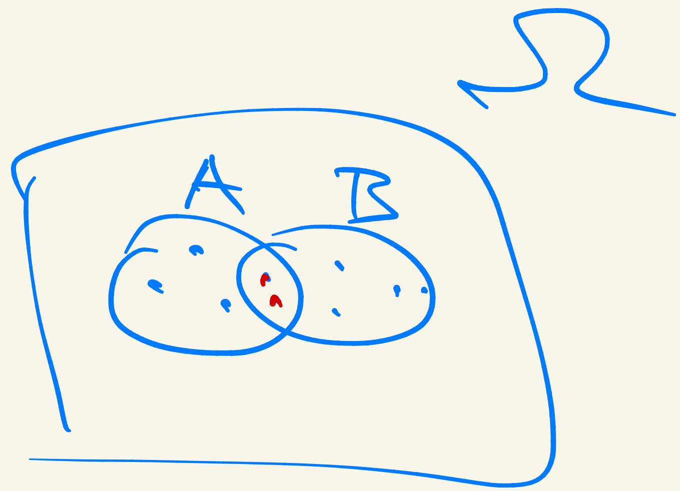
(for all n)

$$P(\{a\}) = P(a)$$

$$A, B \subseteq \Omega$$

HW $\quad P(A \cup B) \le P(A) + P(B)$

thm
$$\boxed{P\left(\bigcup_{i=1}^{t} A_i\right) \le \sum_{i=1}^{t} P(A_i)}$$



UNION BOUND

$$P(\emptyset) = 0$$

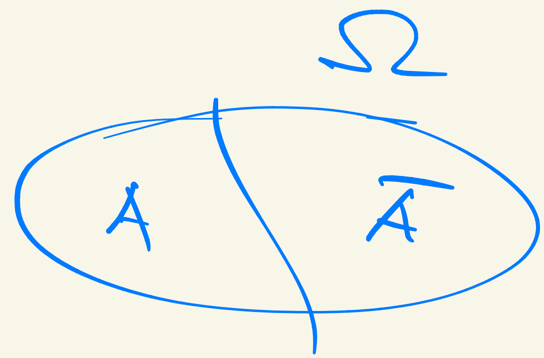
$$P(\Omega) = 1$$

which events have prob = 0 ?

$$P(A) = 0 \iff (\forall a \in A)(P(a) = 0)$$

Complement $\bar{A} = \Omega \setminus A$

$$\boxed{P(\bar{A}) = 1 - P(A)}$$



DEF P is the <u>uniform</u> distribution if

$$(\forall a \in \Omega)\left(P(a) = \frac{1}{n}\right) \qquad n = |\Omega|$$

in this case $\quad A \subseteq \Omega$

$$P(A) = \frac{|A|}{|\Omega|}$$

← NAIVE PROBABILITY

flipping n coins : outcome

$$\begin{array}{ccccccc} 1-p & & p & p & (1-p) & & \\ \downarrow & & \downarrow & \downarrow & \downarrow & & \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 \end{array}$$

$$|\Omega| = 2^n$$

1 : heads

0 : tails

fair coin: $P(\text{heads}) = \frac{1}{2}$

$$\boxed{P(\#\text{heads} = k) = \frac{\binom{n}{k}}{2^n}}$$

biased coin: $P(\text{heads}) = p$

$$\boxed{P(\#\text{heads} = k) = \binom{n}{k} \cdot p^k (1-p)^{n-k}}$$

from intuitive notion of independence to be clarified later

$$P(\underset{\text{with } k \text{ heads}}{\text{outcome is a given } (0,1)\text{-sequence}}) = p^k (1-p)^{n-k}$$