System Security Group | Lancaster University

Fundamentals of Statistics

System Security Group | Lancaster University

Why Statistics

- Statistics is essential for describing/measuring/quantifying things in cybersecurity risk management

- Refer to Chapters 2 and 3 of the book

  How to Measure Anything in Cybersecurity Risk

https://ebookcentral.proquest.com/lib/lancaster/detail.action?docID=4585272&pq-origsite=primo

Describing the Centre

- The central tendency
- Where is the middle of the data
- Arithmetic Mean
- Median
- Mode

An Arithmetic Mean Example

System Security Group | Lancaster University

- Our population is composted of 11 computers and we are measuring the number of applications installed on each
  - 1,2,6,2,1,1,4,7,3,20,8
  - The arithmetic mean is the sum of the data points divided by the number of data points
  - $\frac{1+2+6+2+1+1+4+7+3+20+8}{11} = \frac{55}{11} = 5$

System Security Group | Lancaster University

A Median Example

- Using our example from before we have the following numbers of applications installed
  - 1,2,6,2,1,1,4,7,3,20,8
- The median is found by ordering the population and then taking the mid point.
  - 1,1,1,2,2,3,4,6,7,8,20
  - The median is therefore 3
  - If we had only 10 samples we would take the arithmetic mean of the two middle numbers

A Mode Example

- The mode is the most common number.
- In our sample of
  - 1,2,6,2,1,1,4,7,3,20,8
- In this case the most frequent number is 1
  - The mode is 1

Measuring the Spread

- How close are all the data points around out measure of central tendency?
- Median – Interquartile range
- Mean – Variance or standard deviation

Interquartile range

- We want to know the range from
  - the mid way point between the first number and the median
  - The mid way point between the median and the last number
- 1,1,1,2,2,3,4,6,7,8,20
- 1,1,1,2,2,3,4,6,7,8,20
- IQR is 1 to 7 = 6

The Variance

- The average of the square distances of the population data points from the population mean
  - 1,2,6,2,1,1,4,7,3,20,8 mean of 5

$$\frac{(1-5)^2+(2-5)^2+(6-5)^2+(2-5)^2+(1-5)^2+(1-5)^2+(4-5)^2+(7-5)^2+(3-5)^2+(20-5)^2+(8-5)^2}{11}$$

  - The variance is approx. 28.08 = σ^2
  - The standard deviation is the $\sqrt{Variation} = \sigma$

Questions?

System Security Group | Lancaster University

Fundamentals of Probability

Sets

- A **set** is a collection of objects called **elements** or **members**
  - Sets normally capital letters
  - Elements of a set normally lower case
- Membership is denoted by:
  - $a \in S$ a is a member of Set S (S normally means the complete sample space
  - $a \notin S$ a is not a member of Set S

System Security Group | Lancaster University

Set Membership

- Memberships can be defined as a grouping or by properties
- Grouping $S=\{a,b,c,d,e\}$
- Property $S=\{x:x \text{ } has \text{ } property \text{ } P\}$
  - $S=\{N:N\in Z,\ N\leq 500\}$
  - where Z $=Set \text{ } of \text{ } all \text{ } integer \text{ } Numbers$
- If every element in set A is in set B and every element in set B is in set A then $A=B$
  - Otherwise $A\neq B$

Sub or Super?

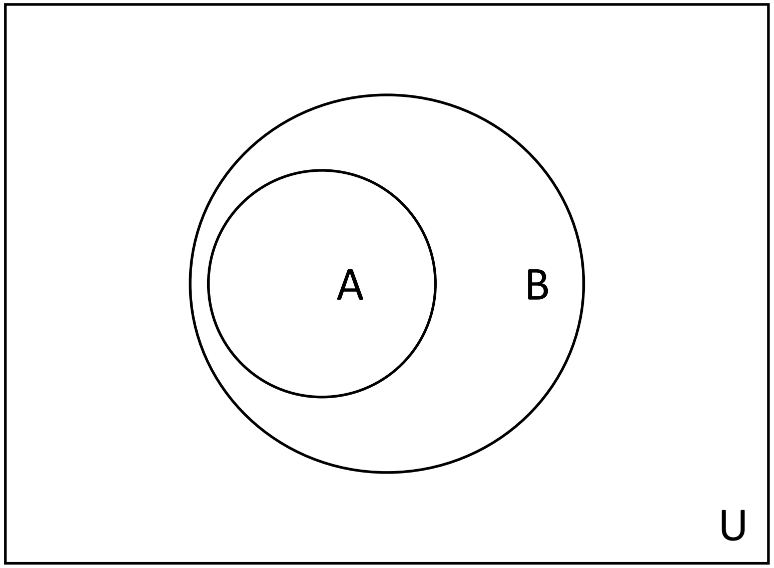
- If every element of A is an element of B then A is a subset of B, $A \subseteq B$
  - Also B is a superset of A, $B \supseteq A$
- If every element of A is an element of B but sets A and B are not equal then A is a proper subset of B, $A \subset B$
  - Also B is a proper superset of A, $B \supset A$
- Not a sub or super set then use:
  - $\not\subset$, $\not\supset$, $\nsubseteq$, $\nsupseteq$

Complements and Empties

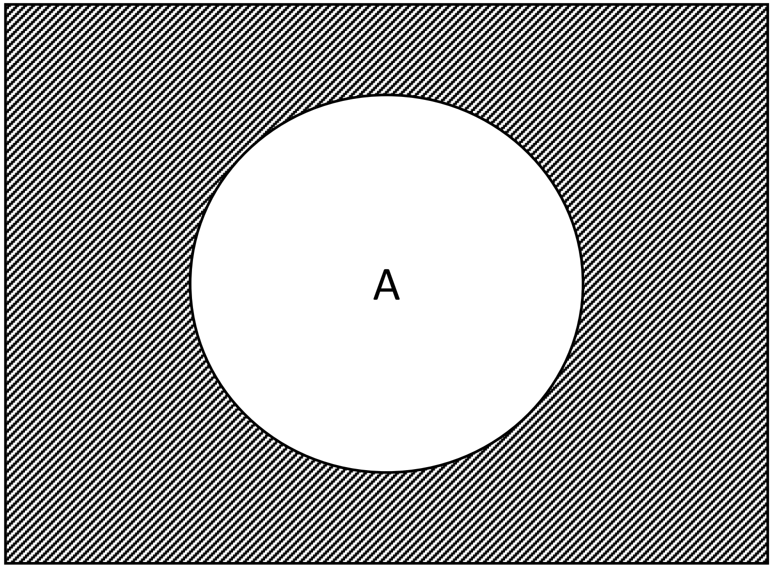
- An empty set is denoted by:
  - $A = \emptyset$
- The complement of a set A is everything that is not in A but still in the universal set U
  - $\bar{A} = \{x : x \in U, x \notin A\}$

Venn Diagrams

- These are really useful to understanding the relationships between sets:



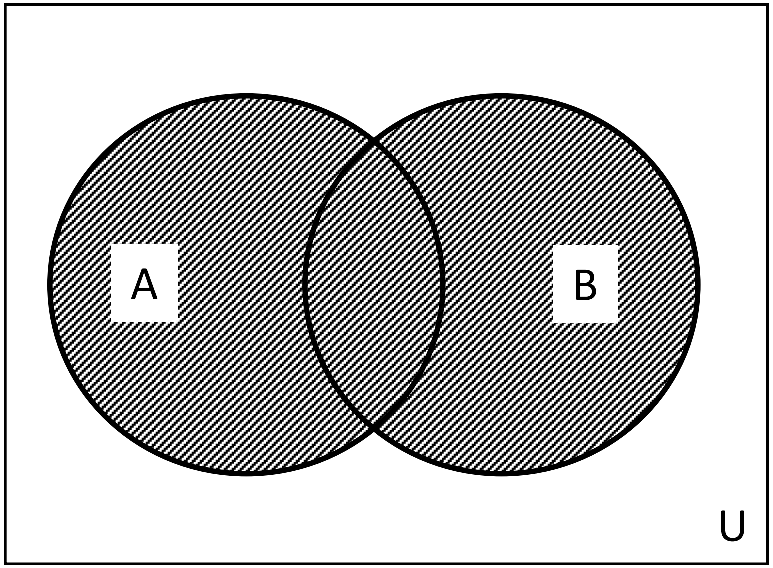
$A \subset B$



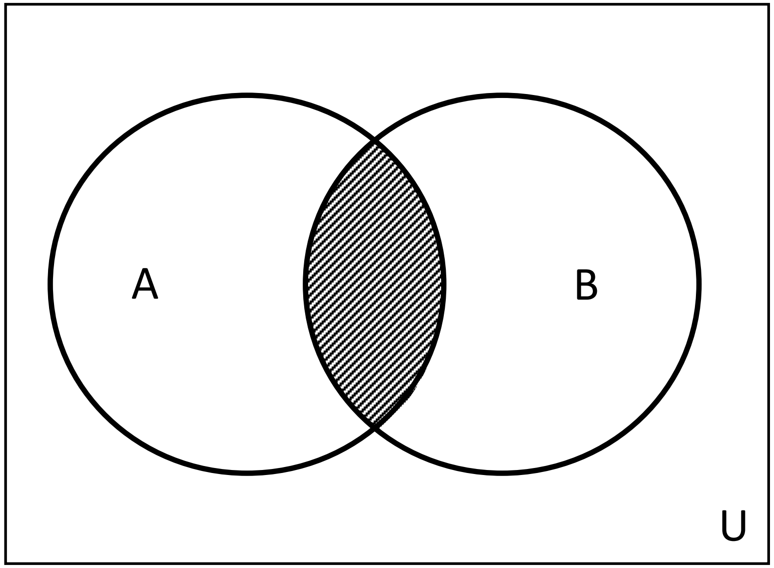
$\bar{A}$ $(shaded)$

Union and Intersection

- Sets can be combined in two different ways **if they relate to the same universal set U**
  - Union: A or B
  - Intersection: A and B

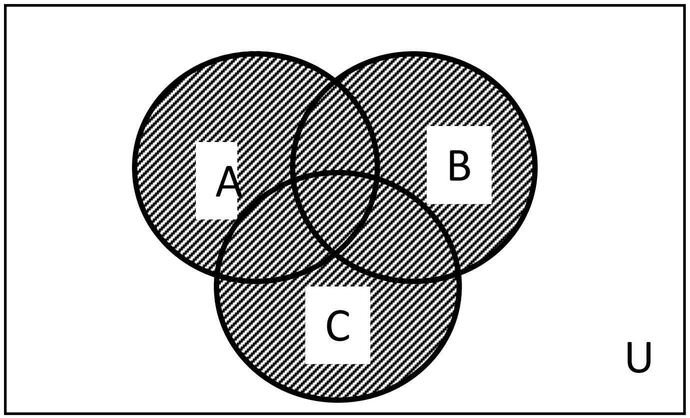


$$A \cup B = B \cup A$$

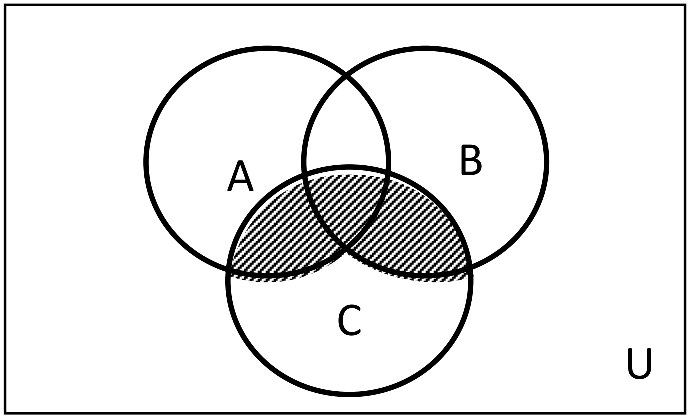


$$A \cap B = B \cap A$$

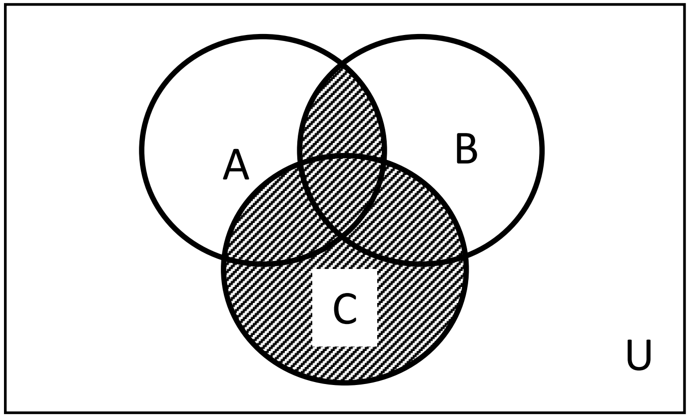
Algebra of Sets



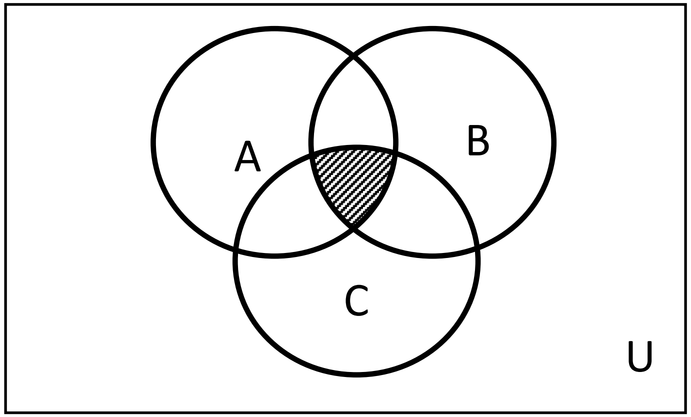
$C \cup (A \cup B)$



$C \cap (A \cup B)$



$C \cup (A \cap B)$



$C \cap (A \cap B)$

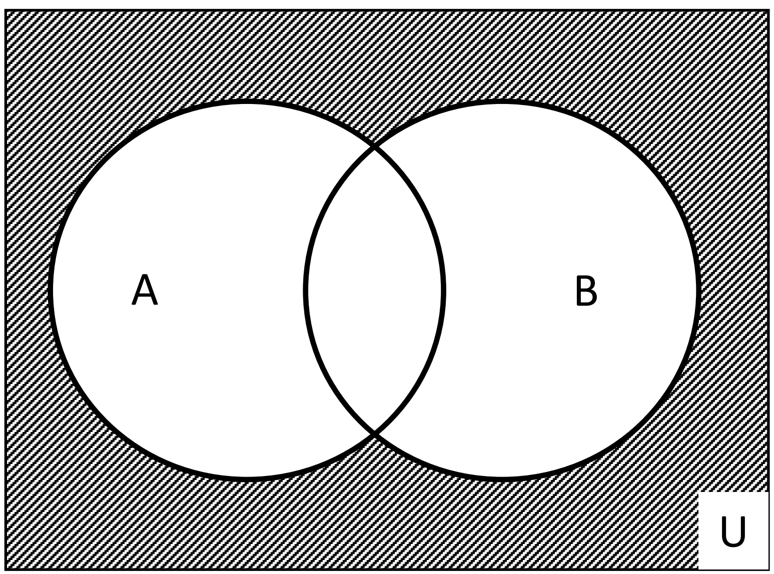
Algebra of Sets

- Commutative Laws
  - $A \cup B = B \cup A$
  - $A \cap B = B \cap A$
- Identity Laws
  - $A \cup \phi = A$
  - $A \cap U = A$
- Associative Laws
  - $A \cup (\mathrm{B} \cup C) = (A \cup B) \cup C$
  - $A \cap (\mathrm{B} \cap C) = (A \cap B) \cap C$
- Idempotent Laws
  - $A \cup A = A$
  - $A \cap A = A$
- Complementary Laws
  - $A \cup \bar{A} = U$
  - $A \cap \bar{A} = \emptyset$
- Distributive Laws
  - $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
  - $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

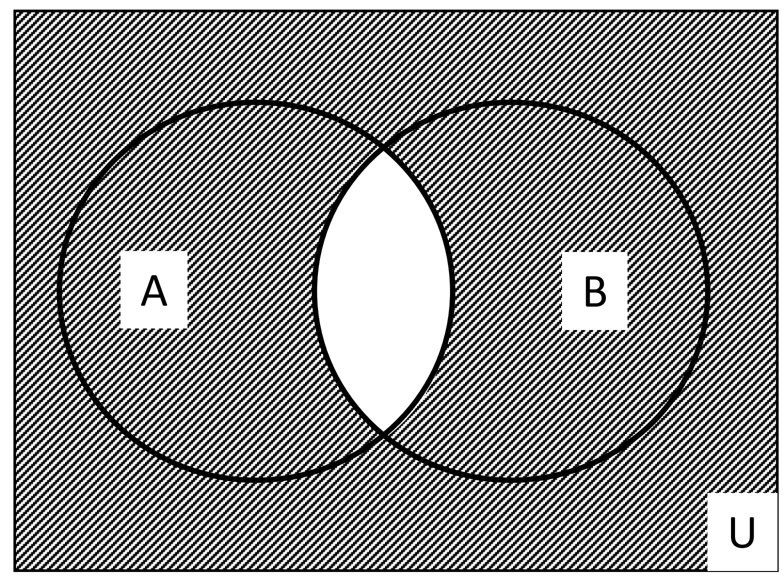
System Security Group | Lancaster University

De Morgan Laws

- We can use the $\cap, \cup, (\overline{\ \ })$ operators to simplify expressions. These are called De Morgan laws.



$$\overline{A \cup B} = \bar{A} \cap \bar{B}$$



$$\overline{A \cap B} = \bar{A} \cup \bar{B}$$

Questions?