Misc

Misc

- **<u>Dmitry does not like the ∴ and ∵ symbols — use corresponding words instead</u>**
- **When using a big operator, if there is nothing to do (e.g. end index < start index), the result of the operation is the neutral element:**
  - Σ x — 0
  - Π x — 1
  - ⋃ x — ∅
  - ⋀ x — ⊤
  - ⋁ x — F
  - ↔ x — ⊤
- **x|y (x divides y) iff ∃k∈ℤ: kx=y** — looks like bus stop division
- Negating statements can make it more obvious what their truth value is or how they translate from natural language
- **Find x s.t. p for all z that satisfy q translates to find x s.t. ∀z [q →p]** and hence can be achieved by finding x s.t. q is false for all z
- Venn diagrams are useful for probability reasoning but don't constitute proofs
- Truth tables are helpful for logic questions and can constitute proofs

Logic

Propositional logic

What is a proposition

- A proposition is a statement with a determinable truth value (either true or false, not neither and not both)
  - (Assuming the meaning of the symbols used in the statement is known), the truth value of a proposition can be evaluated using only the information in the statement e.g. [$x^2=4$] is not a proposition but [if $x=3$, then $x^2=4$] is a proposition
- $(a+b)^2 \equiv a^2+2ab+b^2$ is determinably true but is not a proposition because it is not a statement (as it is not a "complete" "grammatically correct" logical sentence) — add either if $a \in \mathbb{C} \land b \in \mathbb{C}$, then … or $\forall a,b \in \mathbb{C}$ [...]
  - All variables must be bound (either to a single value, or to a range of values through a quantifier)

Connectives

- Compound propositions are built by chaining atomic propositions together using connectives
- If defining a boolean function ($f: \{T,F\}^n \mapsto \{T,F\}$) by listing all possible cases, listing inputs in alphabetical order (treating each ordered pair as a string) is a good way of ensuring each occurs exactly once
- $\wedge$ is called conjunction — associative and commutative
- $\vee$ is called disjunction — associative and commutative
- **$X \rightarrow Y$ (also denoted $X \Rightarrow Y$) is called material implication**
  - **Natural language forms: If X, then Y; Y is necessary for X; X only if Y**
  - **Is true unless X is true and Y is false — $X \rightarrow Y \equiv \neg(X \wedge \neg Y) \equiv \neg X \vee Y$**
- **$X \leftarrow Y$ (also denoted $X \Leftarrow Y$)**
  - **Natural language forms: Y is sufficient for X; Y only if X; If Y, then X**
  - Is true unless Y is true and X is false — **$X \leftarrow Y \equiv \neg(Y \wedge \neg X) \equiv X \vee \neg Y \equiv Y \rightarrow X$**
- **$X \leftrightarrow Y$ (also denoted $X \Leftrightarrow Y$) is called material equivalence**
  - **Natural language forms: X if and only if Y; X iff Y; X is necessary and sufficient for Y**
  - **True when X and Y have the same truth value —** $X \leftrightarrow Y \equiv \neg(X \oplus Y) \equiv \neg X \wedge \neg Y \vee X \wedge Y$
- **Tautology = a compound proposition that is true for all values of the atomic propositions**
- **Contradiction = a compound proposition that is false for all values of the atomic propositions**
- **P=Q if $P \Leftrightarrow Q$ is a tautology** (if they always have the same truth value as each other)

Laws of logic

- De Morgan: **¬(A ∧ B) ≡ ¬A ∨ ¬B**
- De Morgan: **¬(A ∨ B) ≡ ¬A ∧ ¬B**
- Distributivity: **X ∧ (Y ∨ Z) ≡ (X ∧ Y) ∨ (X ∧ Z)** ≡ X ∧ Y ∨ X ∧ Z
- Distributivity: **X ∨ (Y ∧ Z) ≡ (X ∨ Y) ∧ (X ∨ Z)**
- **Contrapositive: X → Y ≡ ¬Y → ¬X**

Laws of inference

- $((p \rightarrow q) \land p) \rightarrow q$
- $((p \rightarrow q) \land \neg p) \equiv T$
- $((p \rightarrow q) \land q) \equiv T$
- $((p \rightarrow q) \land \neg q) \rightarrow \neg p$
- $((p \rightarrow q) \land (q \rightarrow r)) \rightarrow (p \rightarrow r)$
- $((p \rightarrow q) \land (r \rightarrow s) \land (p \lor r)) \rightarrow (q \lor s)$
- $p \rightarrow q \equiv \neg q \rightarrow \neg p$
- $p \leftrightarrow q \equiv \neg p \leftrightarrow \neg q$

Predicate logic

Working with predicates

- A predicate is a more abstract version of a proposition — it becomes a proposition when the variables used are assigned values
    - Can be thought of as being a function that take in the values of the variables and outputs a (truth value of a) proposition
- $(\exists x \in \mathbb{R}: \forall y \in \mathbb{R}[x<y]) = F$ but $(\forall x \in \mathbb{R}. \exists y \in \mathbb{R}: x<y) = T$
    - : can be omitted and [] can be replaced with a single , or .
        - **Brackets define the scope of the bound variable** in more complex predicates
- Unless specified in the predicate, two variables from the same domain may be equal
- **To evaluate the truth value of a predicate: Working left-to-right, pick a value of the variable at each quantifier trying to force the predicate to be true at existential quantifiers and false at universal quantifiers, once the truth value is not possible to change in the way you would like the current truth value is the correct truth value**
    - This reflects the fact that at existential quantifiers you can chose a convenient value whereas at a universal quantifier the statement has to hold for whatever value the universe throws at you

Properties of quantifiers

- $\forall x \in X.\ P(x) = \forall x[x \in X \rightarrow P(x)]$
- Universal quantifier acts as a $\wedge$ over the specified set
- Existential quantifier acts as a $\vee$ over the specified set
- The below properties follow directly from the previous two properties
- **The universal quantifier distributes over conjunction ($\wedge$) but existential quantifier does not** (distributed being true is sufficient but not necessary for non-distributed being true)
- **The existential quantifier distributes over disjunction ($\vee$) but universal quantifier does not** (distributed being true is necessary but not sufficient for non-distributed being true)
- **When expanding out a negated bracket, all universal quantifiers become existential and vice versa and the propositions are negated as per De Morgan**
- Universal quantifiers are vacuously true and existential quantifiers are vacuously false

Proof

Methods of proof

- A proof is an argument that aims to convince the reader that a statement is true — proofs can be subjective
- Proof by cases (exhaustion)
  - □ means end of case or end of sub proof
  - ■ means end of proof
  - Q.E.D means end of significant proof
- Proof by contradiction — ¬P=F ↔ P=T
  - Ending a sentence ?! is a nice way of denoting that it is absurd
- Proof by induction
  - Keegan's trick for inequalities:
    Let f(n) = LHS and g(n) = RHS
    Base case
    Assume true for n=k: …
    Find a function h s.t. f(n+1) = h(f(n)) and f(k)>g(k) → h(f(k)) > h(g(k))
    Show that h(g(k)) > g(k+1) for k: …
    - Works well when g is a polynomial: Look at roots, turning points, derivative etc to sketch and hence find sufficient conditions on inequality
- **Proof by contrapositive: P → Q ≡ ¬Q → ¬P**

Sets

Misc

- **Singleton = a set with cardinality of 1 — this is distinct from the element on its own**
- For the purposes of CS130, $0 \in \mathbb{N}$
- **Set builder notation — $\{x \in A: p(x)\}$** = the set of all x in A such that p(x)=True
  - Can use | or : to denote such that — prefer :
  - Desugars to $\{x: x \in A \land p(x)\}$
- **Subset: $A \subseteq B$ iff $\forall x \in A\ [x \in B]$**
  - *Alternatively $\exists\ Y: A \cup Y = B$*
  - Is associative
  - **Proper subset: $A \subset B$ (also denoted $A \subsetneq B$) iff $A \subseteq B \land \neg(B \subseteq A)$** iff $\forall x \in A\ [x \in B] \land \exists y \in B: y \notin A$
- **$\varnothing$ is a subset of every set** as the condition is vacuously true
- **$A = B$ iff $A \subseteq B \land B \subseteq A$ iff $\forall x[x \in A \leftrightarrow x \in B]$**
- Sets don't have order or repetition, *bags (aka multisets) have repetition but not order,* n-tuples have order and repetition

Set operations

- **Union: $A \cup B = \{x: x \in A \vee x \in B\}$**
  - Ensure $\cup$ and $\vee$ can be distinguished when handwriting either symbol
  - $C \subseteq A \vee C \subseteq B$ is sufficient but not necessary for $C \subseteq A \cup B$
- **Intersection: $A \cap B = \{x: x \in A \wedge x \in B\}$**
- **Union distributes over intersection and vice versa**
- Union and intersection are each: associative, commutative, and idempotent (A * A = A for operator * and all A)
- **Set difference: $A \backslash B = \{x: x \in A \wedge \neg(x \in B)\}$**
- **Symmetric difference: $A \Delta B = A \backslash B \cup B \backslash A$** $= (A \cup B) \backslash (A \cap B) = \{x: x \in A \veebar x \in B\}$
  - The non-bold definitions are easier to reason with but the bold one is the one that should be used in proofs etc
- Methods for set identity proofs
  - Write in set builder and show are equivalent — truth table may help
  - Show each side is a subset of the other

Proof that definitions of symmetric difference are identical

Let $S = A \setminus B \cup B \setminus A$ and $T = (A \cup B) \setminus (A \cap B)$
Need to show that $S \subseteq T$ and that $S \supseteq T$
Pick an arbitrary $x \in S$. Then, $x \in A \setminus B \vee x \in B \setminus A$
$x \in T$ iff $x \in A \cup B \wedge x \notin A \cap B$
Case $x \in A \setminus B$: Then, $x \in A \wedge x \notin B$
    Hence, $x \in A \cup B \wedge x \notin A \cap B$
Case $x \in B \setminus A$: Then, $x \in B \wedge x \notin A$
    Hence, $x \in A \cup B \wedge x \notin A \cap B$
Hence, all elements of S are elements of T, $S \subseteq T$ □

Pick an arbitrary $x \in T$. Then, $x \in A \cup B \wedge x \notin A \cap B$
$x \in S$ iff $x \in (A \setminus B) \vee x \in (B \setminus A)$
Case $x \in A$: As $x \notin A \cap B$, $x \notin B$
    Therefore, $x \in A \setminus B$
Case $x \in B$: As $x \notin A \cap B$, $x \notin A$
    Therefore, $x \in B \setminus A$
Therefore, $x \in A \setminus B \vee x \in B \setminus A$. Hence, all elements of T are elements of S, $S \supseteq T$ ■

Sequences and the cartesian product

- **Cartesian product: $A \times B = \{(a,b): a \in A \land b \in B\}$** — this is not commutative
- Cartesian product is not associative:
  - $A \times B \times C$ has elements of the form (a, b, c)
  - $(A \times B) \times C$ has elements of the form ((a, b), c)
  - $A \times (B \times C)$ has elements of the form (a, (b, c))
- For $n \in \mathbb{N}_{\geq 1}$, X^n is the set of all ordered n-tuples (sequences of length n) of elements of X
  - $\mathbf{X^n=\{(x_1,x_2,...,x_n): \{x_1,x_2,...,x_n\} \subseteq X\}}$ = cartesian product of X with itself n times
- When denoting $a<x<b$, use (a;b) instead of (a,b) to avoid confusion with the ordered pair (a,b)
- The brackets and commas in sequences can be omitted where it does not introduce ambiguity
- For finite sets, $\mathbf{|X^n|=|X|^n}$

Set operations and cardinality

- **Power set: $2^A = \{x: x \subseteq A\}$**
  - *Contains |A|Ck elements with cardinality k*
- **For finite sets, $|2^A|=2^{|A|}$**
- *Inclusion–exclusion principle: $|A \cup B| = |A| + |B| - |A \cap B|$, $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$, etc (signs continue to alternate)*

  Proof for first case (for shorter proof of first case see probability):
  $A \cup B = A \setminus B \cup B \setminus A \cup (A \cap B)$
  $A = A \setminus B \cup (A \cap B)$
  $B = B \setminus A \cup (A \cap B)$
  Hence, by sum rule, $|A \cup B| = (|A| - |A \cap B|) + (|B| - |A \cap B|) + |A \cap B| = |A| + |B| - |A \cap B|$
- *Sum rule: For disjoint, finite sets A and B, $|A \cup B| = |A| + |B|$*
- Product rule: **For finite sets A and B, $|A \times B| = |A||B|$**

(Binary) Relations

Misc

- **A relation between A and B is a subset of A × B that is defined by a rule that all members of the relation follow**
  - **A relation on A is the subset of A^2 …**
- **Similar to functions, what the relation is a subset of should be specified before stating the rule**
- Equality of integers can be defined by the relation $R \subseteq \mathbb{Z}^2$ $R=\{(x,x) \in \mathbb{Z}^2\}$
- If R is a relation between A and B, then R^{-1} is a relation from B to A
  - **$R^{-1} = \{(b,a) \in B \times A: (a,b) \in R\}$**
- **If $R \subseteq A \times B$ and $Q \subseteq B \times C$, then $R \circ Q \subseteq A \times C$**
  - **$R \circ Q = \{(a, c) \in A \times C: \exists b: (a,b) \in R \wedge (b,c) \in Q\}$**
- $(a,b) \in R$ can be abbreviated as aRb
- *A relation can be interpreted as a graph where the nodes are the members of A and B and for all nodes a and b in A and B there is an edge (a, b) iff aRb*

Types of relation

Let R be a relation on S

- **R is reflexive iff $\forall a \in S.\ aRa$**
- **R is symmetric iff $\forall a,b \in S.\ aRb \rightarrow bRa$**
- **R is antisymmetric iff $\forall a,b \in S.\ (aRb \wedge bRa) \rightarrow a=b$**
  - This is not the same being not symmetric e.g. = is symmetric and antisymmetric
- **R is transitive iff $\forall a,b,c \in S.\ (aRb \wedge bRc) \rightarrow aRc$**
- **R is an equivalence relation iff it is reflexive, symmetric, and transitive**
- **R is a partial order iff it is reflexive, antisymmetric, and transitive**

Equivalence relations

- **$[a]_R$ = the equivalence class generated by a under R = {x ∈ S: aRx}**
  - Subscript may be omitted where doing so does not harm clarity
  - a is called the representative of the equivalence class — **any member of the equivalence class can be substituted for a and the notation will still refer to the same set** (theorem 0)
- Lemma 1: xRy iff [x]=[y]
  - This follows trivially from theorem 0 as $\forall y(xRy \leftrightarrow y \in [x])$ by definition of an equivalence class
- Theorem 1: $[x] \neq [y]$ iff [x] and [y] are disjoint ($[x] \cap [y] = \varnothing$)
- Fundamental **Theorem** of Equivalence Relations: Let R be an equivalence relation on S. Then, **the equivalence classes of R are non-empty and pairwise-disjoint and their union is equal to S**
  - R partitions S — it groups S so that every element of S is in exactly one group and no group is empty
- **S/R = the quotient set of S under R = the set of all equivalence classes of R = $\{[a]_R: a \in S\}$**
  - As equivalence classes are sets, this is a set of sets
  - <u>Don't confuse with \ for set difference!</u>
  - Under the graph interpretation each equivalence class is a connected component
- $R = \bigcup_{x \in S/R} x^2$

Equivalence relations: Proof of theorem 0

We wish to show that $\forall a \in S.\ \forall b \in [a].\ [b]=[a]$
It suffices to show that $\forall a \in S.\ \forall b \in [a].\ \forall y\ y \in [b] \leftrightarrow y \in [a]$

Chose some arbitrary $a \in S$ and $b \in [a]$
As $b \in [a]$, aRb
Chose some arbitrary y
$y \in [b]$ iff bRy
iff aRb $\wedge$ bRy (aRb is known to be true)
iff aRy (equivalence relations are transitive)
iff $y \in [a]$ as required

Equivalence relations: Proof of theorem 1

$[a]\neq[b]\rightarrow[a]\cap[b]=\varnothing$:

AFTSOC that $\exists\, a,b:\ \exists\, c\in[a]\cap[b] \wedge [a]\neq[b]$

Then, aRc and bRc

As R is an equivalence relation it is symmetric so aRc and cRb and is transitive so aRb

Hence $b\in[a]$. So, by theorem 0, $[a]=[b]$?!

$[a]\neq[b]\leftarrow[a]\cap[b]=\varnothing$:

AFTOSC that $\exists\, a,b: [a]\cap[b]=\varnothing \wedge [a]=[b]$

As $[a]=[b]$, $[a]\cap[b]=[a]=[b]$

Hence, $[a]=[b]=\varnothing$?! (**equivalence classes are non-empty as they contain their representative due to reflexivity**)

Proof of fundamental theorem on equivalence relations

Non-empty

As equivalence relations are reflexive, $\forall a \in S.\ a \in [a]$

Pairwise-disjoint

See theorem 1

Union = S

For every $a \in S$, [a] is a subset of S by the definition of an equivalence class. Hence union $\subseteq S$

For every $x \in S$, there exists [x] and $x \in [x]$ by reflexivity. Hence, every element belongs to at least one equivalence class. Hence union $\supseteq S$

Hence, union = S

Partial orders

- **A relation is a partial order iff it is reflexive, transitive, and antisymmetric**
- **A relation R on X is a total order iff it is a partial order and $\forall a,b \in X\ [(a,b) \in R \vee (b,a) \in R]$**
  - E.g. subset relation is a partial order but not a total order
- A poset is a set equipped with a partial order relation
- In the same way that = is the quintessential equivalence relation, ≤ is the quintessential partial (and total) order — they can both be used to denote any relation of that type
- $a<b$ if $a \leq b \wedge a \neq b$
- $a>b$ if $b \leq a \wedge a \neq b$
- $a \lessdot b$ if $a<b \wedge \neg[\exists z: a<z \wedge z<b]$
  - Drawing edges where $a \lessdot b$ instead of where $a \leq b$ is standard if drawing a graph of a partial order (a Hasse Diagram) (hides edges implied by reflexivity and transitivity)

Partial orders: Special elements

- **If $\forall y \in P\ x \leq y$, then x is <u>the</u> least element** — all elements are "greater than or equal to" x
  - By antisymmetry, least element is unique
- **If $\forall y \in P\ y \leq x$, then x is <u>the</u> greatest element** — all elements are "less than or equal to" x
  - By antisymmetry, greatest element is unique
- **If $\forall y \in P\ [\neg(y<x)]$, then x is <u>a</u> minimal element** — there does not exist an element "less than" x
  - **Equivalently, $\forall y \in P\ [y \leq x \rightarrow y=x]$**
- **If $\forall y \in P\ [\neg(x<y)]$, then x is <u>a</u> maximal element** — there does not exist an element "greater than" x
  - **Equivalently, $\forall y \in P\ [x \leq y \rightarrow y=x]$**
- **<u>Least/greatest requires every element to be related to it whereas minimal/maximal don't</u>**

Partial orders: Lattices

- *If $S \subseteq P$ and $\forall y \in P\ [(y \leq x)]$, then x is a upper bound of S*
- *If $S \subseteq P$ and $\forall y \in P\ [(x \leq y)]$, then x is a lower bound of S*
- *The least upper bound of S is the least element of the set of all upper bounds of S under the partial order*
- *The greatest upper bound of S is the greatest element of the set of all lower bounds of S under the partial order*
- *A poset is a lattice if every subset of P with cardinality 2 has a least upper bound and a greatest upper bound*

Functions

Misc

- **Whenever a function is defined the domain and codomain must both be specified**
- **If there exists a rule that unambiguously assigns to each $x \in X$ a single $y \in Y$, then there exists a function from X to Y (there exists $f: X \mapsto Y$)** — each x is assigned 1 y no more no less
- **A relation R between A and B is a function with domain A and codomain B iff for all $x \in A$ there exists exactly one $y \in B$ s.t. xRy**
  - $\forall x \in A\ [\exists y \in B: [(x, y) \in R \land \forall z \in B\ [(x, z) \in R \rightarrow z=y]]]$
- The function $y=f(x)$ is $\{(x, y) \in X \times Y: (x, y) \in f\}$ where f is the underlying relation
- **For a set S, $f(S)=\{y : (x, y) \in f \land x \in S\}$**
  - **range = f(X) where X is the domain**
  - **range $\subseteq$ codomain but $\neg$(range$\equiv$codomain)**
    - Codomain can contain values the function can never output

Function composition

- <u>For C130, **(f ∘ g) (x) ≡ g(f(x))** — apply the functions in the order they are written</u>
  - This matches the way relations are composed
  - *In most other contexts (f ∘ g) (x) ≡ f(g(x)) — operator does not affect order functions are written on RHS*
- Theorem: If f is a function from A to B and g is a function from B to C, then the relation (f ∘ g) is a function from A to C
  Proof:
  Let H be the relation (f ∘ g). Then, H = {(a,c)| ∃ b: (a, b) ∈ f ∧ (b, c) ∈ g}
  We wish to show that for all a in A, there exists exactly one c in C such that aHc.

  At least one: Pick an arbitrary a ∈ A. Then, there exists b ∈ B such that f(a)=b. Then, there exists c ∈ C such that g(b)=c and so (a, c) ∈ h.

  No more than one: Assume for the sake of contradiction that there exists a ∈ A for which there exists c_1, c_2 such that (a, c_1) ∈ h and (a, c_2) ∈ h and $c_1 \neq c_2$
  Then, there exists b_1, b_2 ∈ B such that f(a)=b_1 and g(b_1) = c_1 and f(a) = b_2 and g(b_2)=c_2. Because f is a function, a is only mapped to one value. Hence, b_1=b_2. So, as g is a function, c_1=c_2?!

Images

- f(x) is called the image of x under f
- $f^{-1}(x)$ is called the complete preimage of x under f — f^{-1} is a relation but may not be a function (hence, f^{-1} of a single value may be a set instead of a single value)
  - **f(x) = y iff x is <u>a</u> preimage of y**
  - $f^{-1}(y)$ = **<u>complete</u> preimage of y = {x ∈ X: f(x) = y}**
  - $f^{-1}(Y)$ = <u>complete</u> preimage of a set Y = {x ∈ X: f(x) ∈ y}

Types of function

- **A function is an injection iff $\forall a,b \in X\ [f(a)=f(b) \rightarrow a=b]$** — is one-to-one — no member of the codomain is mapped to by more than one member of the domain
- **A function is a surjection iff $(\forall y \in Y\ [\exists x \in X: f(x)=y)$** — codomain = range — no member of the codomain is mapped to by less than one member of the domain
- A function is a bijection iff it is surjective and injective — every member of the codomain is mapped to by exactly one member of the domain
- **$f|_S$ is the restriction (of the domain) of f to S where S is a subset of the domain of f**
  - **$f|_S = \{(x, y): (x, y) \in f \wedge x \in S\}$**
- If f is an injection $X \mapsto Y$ and $S \subseteq f(X)$, then $f|_S$ is a bijection

Inverse functions

- **$f^{-1}(y) = \{(y,x): y=f(x)\}$**
- **Theorem: f^{-1} is a (bijective) function iff f is a bijection**
  Sketch proof: Surjectivity means that f^{-1} is defined for all $y \in Y$. Injectivity means f is one-to-one, and hence f^{-1} will also be one-to-one

  Proof:
  f^{-1} is a function iff $\forall y \in Y [\exists x \in X: (y, x) \in f^{-1} \wedge \forall x_1,x_2 \in X[(y, x_1) \in f^{-1} \wedge (y, x_2) \in f^{-1}) \rightarrow x_1=x_2]]$

  f is a bijection iff $\forall y \in Y [\exists x \in X: (x, y) \in f \wedge \forall x_1,x_2 \in X[(x_1, y) \in f \wedge (x_2, y) \in f) \rightarrow x_1=x_2]]$
  Because $\forall x \in X. \forall y \in Y. (y, x) \in f^{-1}$ iff $(x, y) \in f$, f is a bijection iff $\forall y \in Y [\exists x \in X: (y, x) \in f^{-1} \wedge \forall x_1,x_2 \in X[(y, x_1) \in f^{-1} \wedge (y, x_2) \in f^{-1}) \rightarrow x_1=x_2]]$ iff f^{-1} is a function

  By the same logic it can be shown that a function f^{-1} is bijective iff a relation f is a function

Set countability

Definitions

- **Sets A and B are equinumerous (have the same cardinality) iff there exists a bijection between them**
- Let F_i = the set containing the first i naturals = $\{x \in \mathbb{N}: x < i\}$ and S be a set
  - S if finite iff $\exists n \in \mathbb{N}$: S is equinumerous with F_n
  - S is countably infinite iff S is equinumerous with $\mathbb{N}$
  - S is countable iff it is finite or countably infinite
  - S is uncountable iff it is not countable

Proofs using pseudocode

To show that $\mathbb{Z}$ is countably infinite, we must find a bijective f: $\mathbb{N} \mapsto \mathbb{Z}$
We will define f using code for simplicity

```
c := 0
print (c,0)
for i:= 1,2,3,...
    c := c+1
    print (c,i)

    c := c+1

    print(c, -i)
```

This gives:

(0,0), (1, 1), (2, −1), (3, 2), (4, −2),…

- := is used for assignment to avoid ambiguity
- print is a statement, not a function
- Must provide sample output
- **Any arbitrary pair must be output in finite time**

Proof that the rationals are countable

Lemma: If A and B are countable sets, then A×B is countable. Moreover, if A and B are not both not finite then neither is A×B

Proof: Case A and B are both finite: Then |A×B|=|A||B|

Case A and B are both countably infinite: Then, there exists bijections f: $\mathbb{N} \mapsto$ A and g: $\mathbb{N} \mapsto$ B

```
c := 0
for s:= 0,1,2,3,...
    for i := 0 to s
        a := f(s-i)
        b := g(i)
        print (c, (a, b))
        c := c+1
```

Sample output: $(0, (a_0,b_0)), ((1, (a_1,b_0)), ((2, (a_0,b_1)), ((3, (a_2,b_0)), ((4, (a_1,b_1)), ((5, (a_0,b_2))$

This corresponds to traversing the <u>trailing</u> diagonals of

(a_0, b_0) (a_1, b_0) (a_2, b_0)
(a_0, b_1) (a_1, b_1) (a_2, b_1) etc

(a_0, b_2) (a_1, b_2) (a_2, b_2)

etc

Case one of A and B is countably infinite: Use similar logic to previous case

$\mathbb{Q} \subset \mathbb{Z}\times\mathbb{N}$ and $\mathbb{N}$ is the quintessential countably infinite set and we have shown previously that $\mathbb{Z}$ is countably infinite

Cantor's theorem

Cantor's Theorem: For all sets A, A is not equinumerous with 2^A

Proof:

Assume for the sake of contradiction that there exists a set S s.t. there exists a bijective $f: S \mapsto 2^S$

Consider **$A = \{x \in S: x \notin f(x)\}$**

A is clearly a subset of S, hence $A \in 2^S$

As we have assumed f is bijective it is surjective, so **$\exists y \in S: f(y) = A$ (because $A \in 2^S$)**

Case $y \in f(y)$: By the definition of A, $y \notin A$?!

Case $y \notin f(y)$: By the definition of A, $y \in A$?!

Hence, f is not surjective and so there does not exist a bijection between S and 2^S

Uncountability of the reals by diagonalization

Let I=[0, 1). Deduce that I ⊆ ℝ and thus if I is uncountable then ℝ is uncountable.
Let B = set of all binary strings (infinite sequences formed from {0,1}). (Note that this includes sequences with an infinite tail of zeros)

By using fixed point representation with the binary string from I starting immediately after the binary point, every member of I is represented by exactly one member of B and every member of B represents exactly one member of I. Hence, B and I are in bijection and so are equinumerous. Thus, if B is uncountable then I is uncountable and so ℝ is uncountable.

Assume for the sake of contradiction that B is countable.
B is "obviously" not finite, so B must be countably infinite and thus there exists a bijection f: ℕ ↦ B

Let x[i] denote the ith element (starting at i=0) in a sequence x
Let g: ℕ ↦ {0, 1}, g(i) = f(i)[i]
Let k: {0, 1} ↦ {0, 1}, k(i)=(i − 1)^2 i.e. the binary digit i after a bit flip
Let h: ℕ ↦ {0, 1}, h(i)=k(g(i)) i.e. the binary digit g(i) after a bit flip

Let b = (h(0), h(1), … for all naturals). Deduce that b ∈ B.
As f is a bijection there exists n such that f(n)=b
Note that b[n] = f(n)[n] = g(n) and b[n] = h(n) = k(g(n)) and thus deduce that g(n) = k(g(n))
Case g(n)=0: Then h(n)=k(0)=1. Hence, 0=1?!
Case g(n)=1: Then h(n)=k(1)=0. Hence, 1=0?!
Hence, B is not countable (as f is not actually surjective) and so B is uncountable. Hence, ℝ is uncountable

Graphs

Definitions

- Graph = an ordered pair (V, E) where V is the (finite, non-empty) vertex set and E is a collection of edges
- If the graph does not contain parallel edges, E is a set
  - *If the graph does, E can still be a set if it is equipped with a function that maps each edge to the number of times it occurs*
- In a directed graph, each edge is an ordered pair
- In an undirected graph, each edge is a set
- Simple graph = a graph that contains neither self-loops nor parallel edges — E is a set of sets
  - Unless stated otherwise, all graphs are simple
  - *Every simple graph defines an irreflexive relation*
- *Every undirected graph defines a symmetric relation*
- u and v are adjacent iff $(u, v) \in E \vee (v, u) \in E$
- **A graph H = (V′, E′) is a subgraph of G = (V, E) iff $V' \subseteq V$ and $E' \subseteq E$**

Degree

- **Degree of v = number of edges incident on v, self-loops count as 2**
- **Indegree of v = number of edges in which v is the destination**
- **Outdegree of v = number of edges in which v is the source**
- **Degree of v = indegree of v + outdegree of v**
- **Handshaking lemma: For any graph, $\Sigma_{v \in V} deg(v) = 2|E|$**
  Proof: LHS = number of endpoints of edges. Every edge has two endpoints.
  - **Hence, every graph contains an even number of nodes with odd degree**, as the total degree is even and k*even + m*odd = even for any integer k but only for even integers m

Isomorphism

- **Simple graphs $G_1=(V_1, E_1)$ and $G_2=(V_2, E_2)$ are isomorphic iff there exists a bijection $f: V_1 \mapsto V_2$ s.t. $[\forall u, v \in V_1. (u, v) \in E_1$ iff $(f(u), f(v)) \in E_2]$**
  - Informally: It is possible to relabel vertices so that the graphs are the same
- K_n = the complete graph with n vertices **= the simple undirected graph with n vertices and nC2 edges**
  - Up to isomorphism, there exists only one such graph for each n
- The following are necessary but not sufficient for isomorphism (and hence their negation is sufficient for non-isomorphism)
  - Same number of connected components with each size (and hence overall)
  - Same number of nodes with each degree
  - Same number of cycles with each length
  - These follow from the fact that **because f preserves edges and their absence, f(u) is reachable from f(v) iff u is reachable from v**
- If f is an isomorphism from G to H, then for any vertex v of G $\deg_G(v) = \deg_H(f(v))$
- *If all nodes have the same degree in G and H, and there exist cycles in both of them that visit every vertex at least once, then matching up vertices that are visited at the same time forms an isomorphism?*

Walks, paths, and cycles

- **A walk is a finite sequence of alternating vertices and edges that starts and ends with a vertex** e.g. v_0, (v_0, v_1), v_1, …, v_{n-1}, (v_{n-1}, v_n), v_n
  - **Length = number of edges** = n in the above example
- **A path is a walk that repeats no edge**
  - **A simple path is a path that repeats no vertex** (equivalently a walk that repeats no vertex)
- **A tour is a walk where the first and last vertex are the same**
- **A cycle is a tour that is a path**
  - **A simple cycle is a cycle in which the only repetition of vertices is the start and end** — this vertex cannot be repeated elsewhere

Reachability

- v is reachable from u iff there exists a walk from u to v
- Proposition: The reachability relation is an equivalence relation on an undirected graph *and a partial order on an acyclic directed graph*
  Proof of first part: Reflexive as any node a can be reached from a by the walk a
  Transitive as if we have a walk w_1 from u to v and a walk w_2 from v to w then appending w_2 to w_1 gives a walk from u to w
  Symmetric if undirected as for all u, v if there exists an edge from u to v then there exists an edge from v to u
- **The equivalence classes of the reachability relation on an undirected graph G are called the connected components of G**
- A graph is connected iff it has exactly one connected component i.e. $\forall$ u, v $\in$ V [v is reachable from u]

Eulerian paths and cycles

- **A tour/cycle is Eulerian iff every edge occurs exactly once**
- **A tour/cycle is Hamiltonian iff every node occurs exactly once**

Euler-Hierholzer Theorem: G has an eulerian cycle iff every vertex has even degree and once isolated vertices (if they exist) are removed G is connected

Proof: Let $C=v_0, \ldots, v_0$ be an eulerian cycle in G
Pick an arbitrary $u \in V$ and let k be the number of times u occurs in C. Note that as C is Eulerian, each occurrence corresponds to the use of different edges to the occurences.
Case u is not present in C (k=0): As the cycle visits every edge, u must not have any incident edges. Hence, deg(u)=0
Case $u \neq v_0$ and u is present in C: Every time u is visited then left immediately. So, deg(u)=2k
Case $u=v_0$ (then u is present in C): u is left at start and visited at end and if it occurs anywhere else there is visited and immediately left. So, deg(u)=1+1+2(k−2)=2(k-1)
Hence, eulerian cycle → all nodes have even degree

Let G' = (V', E) be G after the removal of isolated vertices. Deduce that C is also an Eulerian cycle in G' and every member of V' occurs in C.
Pick arbitrary u and v in V'. WLOG assume that u precedes v in C.
The portion of C from u to v is a path from u to v and hence u is reachable from v. As G is undirected and u is reachable from v, v is reachable from u. Hence, as u and v are both arbitrary and are reachable from each other, G is connected.

Hence, eulerian cycle → all nodes have even degree and after removal of isolated vertices G is connected

Lemma 0

Lemma: **If there is a walk from u to v in G, then there is a simple path from u to v in G**

Proof: Let l be the length of the walk. We will use induction.

Base case l=0: The walk is a simple path as there are no edges to be repeated

Base case l=1: The walk is a simple path as it only contains one edge

Assume that the lemma holds for walks with $l \leq k$

Consider a walk w with l=k+1

Case no vertex is repeated in w: Then w is a simple path

Case a vertex is repeated in w: Let x_i be the first occurrence of this vertex in the walk and x_j be the final occurrence of this vertex. Remove the portion of w from x_{i+1} to x_j (obtaining $u,\ldots,x_i,(x_j,x_{j+1}),x_{i+1},\ldots,v$). This is a walk from u to v (as, because $x_i=x_j$, $(x_j, x_{j+1})=(x_i,x_{j+1})$) with length $\leq k$, hence there exists a simple path from u to v

Proof of other direction of Euler-Hierholzer Theorem

- I find this proof confusing but just about believe it

We wish to show that all nodes have even degree and after removal of isolated vertices G is connected → eulerian cycle

We will use induction on the number of edges
Base case $|E|=0$: Vacuously true as all vertices are isolated
Assume true for graphs with $|E|\leq k$
Consider a graph G with $|E|=k+1$
Pick an arbitrary v_0, v_k from V and construct an arbitrary path P from v_0 to v_k by walking and applying lemma 0
Let E_P = edges present in P and $G'=(V, E\backslash E_P)$

Lemma 1: If P is not a cycle ($v_k\neq v_0$), $\deg(v_k)$ is odd in G'. If P is a cycle ($v_0=v_k$), every node has even degree in G'
Proof: Case not a cycle: Let t=number of times P visits v_k, then number of members of E_P which are incident on $v_k=2(t-1)+1=2t-1$ as visits every time but does not leave after final visit. So, $\deg(v_k)$ in G' = even − (2t−1) = odd
Case is a cycle: Let t=number of times P visits v_k, then number of members of E_P which are incident on $v_k=2(t-2)+2=2(t-1)$ as visits and leaves immediately t−2 times, leaves at start, and visits at end. So, $\deg(v_k)$ in G' = even − 2(t−1) = even
Let u be an arbitrary node in G' that is not v_0. Let y=number of times P visits u, then number of members of E_P which are incident on u=2t as visits and leaves immediately every time. So, $\deg(v_k)$ in G' = even − 2t = even

By lemma 1, if $v_k\neq v_0$ we can keep on walking (as every node has even degree in G but v_0 has odd degree in G' so there is at least one edge we have not yet taken) until we have $v_k=v_0$. Let P'=P with the added steps (if there are any) required to form a cycle added.
Let G''=G' with the edges that were added to P to form P' removed and isolated nodes removed. As G'' is connected (and every node has even degree using L1), we can use inductive hypothesis. Take the Eulerian cycle in G'' and insert (details left as an exercise to the reader) it into P (an Eulerian cycle in G\G'') to obtain an Eulerian cycle in G.

A lemma

Lemma: In a connected graph with vertices all of even degree, removing a single edge leaves the graph connected
Proof: Assume for the sake of contradiction that there exists a choice of edge to remove e that will produce a disconnected graph. Then, the graph is split into two connected components, one containing the source of e and one containing the destination of e. Hence, each connected component contains exactly one node with odd degree. This violates the handshaking lemma?!
Hence, there is no single edge that when removed will disconnect the graph

Trees

- **A tree is a connected acyclic simple undirected graph**
- A leaf = node with degree 1
- **A forest is an acyclic simple undirected graph** (one or more trees)
- The following are equivalent:

  0. G is a tree
  1. G is a simple connected acyclic graph
  2. G is a simple acyclic graph with $|V|=|E|+1$
  3. G is a simple connected graph with $\mathbf{|E|=|V|-1}$ (as adding a new node introduces exactly one new edge and the tree with $|V|=1$ has $|E|=0$)
  4. G is a simple connected undirected graph which is minimally connected (the removal of any one edge would make it disconnected)
  5. G is a simple undirected graph which is minimally acyclic (the addition of any one edge would cause it to cease being acyclic)

  Proof strategy: We wish to show that $0 \leftrightarrow 1 \leftrightarrow 2 \leftrightarrow 3 \leftrightarrow 4 \leftrightarrow 5$
  1 is the standard definition of 0 so we already have $0 \leftrightarrow 1$
  It suffices to show that $1 \rightarrow 2 \rightarrow 3 \rightarrow 4 \rightarrow 5 \rightarrow 1$

Lemma 0

Lemma: **Let G be an acyclic graph. Introducing a new edge that connects nodes in the same connected component creates a cycle. Introducing a new edge that connects nodes in different connected components does not create a cycle.**

Proof: Let e be the additional edge and u and v be the endpoints of e
Case same connected component: As u and v are in the same connected component there must exist a walk (and hence a path) from v to u, adding e to the end of this path forms a cycle

Case different connected components: Let e be the additional edge. AFTOSC that there exists a cycle after the addition of e. Then a walk from u to v can be obtained by removing e from the cycle, hence in the original graph u is reachable from v?!

Lemma 1

Lemma: **Let n=|Connected components of G=(V, E)|. Then, n ≥ |V| − |E| and if G is acyclic n = |V| − |E|**

Proof: Base case |E| = 0: Then, n=|V| and the graph is acyclic. |V|=|V|−0

Asume true for |E|=k
Consider |E|=k+1
Let G'=G with an arbitrary edge e removed, this introduces at most one new connected component.
By inductive hypothesis, $n_{G'} \geq |V|-k$
$0 \leq n_{G'} - n_G \leq 1 \rightarrow n_G \geq n_{G'} - 1 \rightarrow n_G \geq |V|-k-1 \rightarrow n_G \geq |V|-(k+1)$

If G is acyclic, because it is connected but acyclic removing an edge must introduce a new connected component (corollary to lemma 0). By inductive hypothesis, $n_{G'}=|V|-k$.
As $n_{G'}=n_G+1$, $n_G=|V|-k-1=|V|-(k+1)$

Proof of definitions of trees

1. G is a simple connected acyclic graph
2. G is a simple acyclic graph with $|V|=|E|+1$
3. G is a simple connected graph with $|E|=|V|-1$
4. G is a simple connected undirected graph which is minimally connected (the removal of any one edge would make it disconnected)
5. G is a simple undirected graph which is minimally acyclic (the addition of any one edge would cause it to cease being acyclic)

$1 \rightarrow 2$: As G is connected and acyclic, $1=|V|-|E|$

$2 \rightarrow 3$: As graph is acyclic and $|V|=|E|+1$, $n=|V|-|E|=1$, hence connected as required

$3 \rightarrow 4$: As $|V|=|E|+1$, after removing an edge $n \geq (|E|+1)-(|E|-1)=2$, hence disconnected

$4 \rightarrow 5$: As G is connected, adding a new edge would introduce a cycle

$5 \rightarrow 1$: AFTSOC that G is disconnected: Then, an edge could be introduced connecting different connected components, this would not introduce a cycle, hence 5 is false?! Hence, G is connected

Spanning trees

- **A subgraph T=(V', E') of G=(V, E) is a spanning tree of G iff V'=V and T is a tree**
- **Theorem: A simple graph is connected iff it contains a spanning tree**
  Proof:
  Spanning tree → Connected: Trees are connected. As T is a subgraph of G every path in T is also a path in G. Hence, as T and G have the same vertex set, G is connected.
  Connected → Spanning tree:
  Base case |E| = 0: Can only be connected if |V|=1. G is acyclic so is a spanning tree of itself
  IH: Assume true for |E|=k
  IS: Consider G with |E|=k+1
  Case G is acyclic: G is a spanning tree of itself
  Case G contains a cycle: Remove any one edge e from the cycle to form G'. G' will still be connected, hence by inductive hypothesis G' contains a spanning tree. As G' is a subgraph of G and they have the same vertex sets, G contains the same spanning tree

Colouring

- **A proper k-colouring of G=(V, E) is a function f: V ↦ {x ∈ ℕ: 1≤x≤k} s.t. ∀u,v∈V [{u,v}∈E → f(u)≠f(v)]**
- **A graph is k-colorable iff there exists a proper k-colouring of it** — as f does not have to be surjective, if a graph is n-colourable it is k-colourable for all k≥n
- Every graph without self-loops is trivially |V|-colourable
- K_n is not (n−1)-colourable
- Let f(H) = smallest k for which H is k-colourable. f(G) = max({f(C_1), …, f(C_n)}) where C_1, …, C_n are the connected components of G

Bipartite graphs

- **A graph is bipartite iff it is 2-colourable**
- Theorem: All forests (and hence all trees) are bipartite
  Proof: Base case |E|=0: Any function from nodes to {1, 2} is a valid two-colouring
  Inductive hypothesis: Proposition holds for |E|=k
  Consider a forest G with |E|=k+1
  Remove an arbitrary edge to obtain a forest G'. By inductive hypothesis, G' is bipartite. As G is acyclic, the nodes e is incident on are in different connected components. If the nodes incident on e have the same colour in the 2-colouring of G' flip the colours of all nodes in the connected component of one of them in G' to obtain a 2-colouring in G. Otherwise, the 2-colouring in G' is a 2-colouring in G.
- **$K_{m,n}$ is the complete bipartite graph with partitions of size m and n**
  - There are no edges between nodes in the same partition and there is an edge between every node in one partition and every node in the other
  - $V = \{x \in \mathbb{N}: 1 \leq x \leq m+n\}$
  - $E = \{x \in \mathbb{N}: 1 \leq x \leq m\} \times \{m+x: x \in \mathbb{N} \land 1 \leq x \leq n\} \cup \{m+x: x \in \mathbb{N} \land 1 \leq x \leq n\} \times \{x \in \mathbb{N}: 1 \leq x \leq m\}$

Planarity

- **A graph is planar iff it can be drawn in 2D without edges overlapping**
- Kuratowski's Theorem: **A graph is not planar iff it contains a subgraph which is isomorphic to a graph obtained by a series of edge subdivisions on either K_5 or $K_{3,3}$**
  - **Hence, all trees** (and forests) **are planar** *(as K_5 and $K_{3,3}$ both contain cycles but trees (and forests) are acyclic)*
- A simple connected planar graph partitions the plane into $|E| - |V| + 2$ regions (one of which is everything outside the area enclosed by the graph)
- **4-colour theorem: Every planar graph is 4-colourable**

(Discrete) Probability

Foundations

- Modelling assumptions
  - Conditions under which the experiment occurred can be reproduced exactly in order to perform the experiment an arbitrary number of times
  - There exists *finite non-empty* **Ω** (omega) **the set of all elementary (mutually exclusive** (if one occurs in a run, then no other occured in that run) **and collectively exhaustive** (in every run at least one occurs)) **outcomes** — sample space
  - For any event A, $A \subseteq \Omega$ — $A \in 2^{\Omega}$
    - **2^{Ω} is the set of all events** — event space
      - Singleton members are elementary events
  - There exists a probability measure P: $2^{\Omega} \mapsto \mathbb{R}$ — every event has exactly one associated probability
- Lower case letters are used to denote outcomes and capital letters are used to denote events
- **P obeys the following three axioms for all $A \subseteq \Omega$ and $B \subseteq \Omega$:**
  A1: $P(A) \geq 0$
  A2: $P(\Omega) = 1$
  A3: If A and B are mutually exclusive (A and B are disjoint sets), $P(A \cup B) = P(A) + P(B)$
- A probability space is the ordered triple (Ω, 2^{Ω}, P) — (sample space, event space, probability measure)

Using the axioms

For all $A \subseteq \Omega$ and $B \subseteq \Omega$

- $P(A \cup B)$ and $P(A \cap B)$ really do refer to set operations as events are sets (of elementary outcomes)
- **A1: $P(A) \geq 0$**
- **A2: $P(\Omega) = 1$**
- **A3: If $A \cap B = \varnothing$, then $P(A \cup B) = P(A) + P(B)$**
- C1: $P(\varnothing) = 0$ — $P(\Omega) = 1$ [A2] = $P(\Omega \cup \varnothing) = P(\Omega) + P(\varnothing)$ [A3]
- C2: **$P(B \setminus A) = P(B) - P(A \cap B)$** — $P(B) = P((B \setminus A) \cup (A \cap B)) = P(A \cap B) + P(B \setminus A)$ [A3]
- C3: **$P(A \cup B) = P(A) + P(B) - P(A \cap B)$** — $P(A \cup B) = P(A \cup (B \setminus A)) = P(A) + P(B \setminus A)$ [A3] = $P(A) + P(B) - P(A \cap B)$ [C2]
  - Hence, $P(A \cup B) \leq P(A)+P(B)$ [A1]
- C4: $P(A')= 1 - P(A)$ — **$A' = \Omega \setminus A$**. $1 = P(\Omega)$ [A2] = $P(A \cup A') = P(A) + P(A')$ [A3]
- C5: **$P(\{a, b, \ldots\}) = P(\{a\}) + P(\{b\}) + \ldots$** — [A3; {a}, {b}, … are pairwise-disjoint and {a, b, …} = {a} ∪ {b} ∪ …]

Conditional probability

- **Conditional probability: $P(A|B) = P(A \cap B)/P(B)$**
  - Hence, if $A \subseteq B$, then $P(A|B) = P(A)/P(B)$
- **A and B are independent iff** $P(A|B)=P(A) \leftrightarrow$ **$P(A \cap B)=P(A)P(B)$**
- **Total probability theorem: Let events $B_1, \ldots, B_m$ be a partition of Ω** (pairwise disjoint and $B_1 \cup \ldots \cup B_m = \Omega$). For all events $A \subseteq \Omega$, **$P(A) = \sum P(A|B_i)P(B_i)$** $= \sum P(A \cap B_i)$
  Proof: $A = A \cap \Omega = A \cap (B_1 \cup \ldots \cup B_m) = A \cap B_1 \cup \ldots \cup A \cap B_m$
  As $B_1, \ldots, B_m$ are pairwise-disjoint, $A \cap B_1, \ldots, A \cap B_m$ are pairwise-disjoint
  So, $P(A) = P(A \cap B_1) + \ldots + P(A \cap B_m)$ by axiom 3
- **Bayes' theorem: Let events $B_1, \ldots, B_m$ be a partition of Ω.** For all events $A \subseteq \Omega$,
  $P(B_j|A) = P(A|B_j)P(B_j)/P(A)$ $=$ **$P(A|B_j)P(B_j)/\sum P(A|B_i)P(B_i)$**
  Proof: $P(B_i|A) = P(B_i \cap A)/P(A)$ by conditional probability
  $= P(A|B_i)P(B_i)/P(A)$ by conditional probability
  $= P(A|B_i)P(B_i)/\sum P(A|B_i)P(B_i)$ by total probability theorem