

CO142 - Discrete Structures

Prelude

The content discussed here is part of CO142 - Discrete Structures (Computing MEng); taught by Steffen van Bakel, in Imperial College London during the academic year 2018/19. The notes are written for my personal use, and have no guarantee of being correct (although I hope it is, for my own sake). This should be used in conjunction with the (extremely detailed) notes.

9th October 2018

Recommended Books

- K.H. Rosen. *Discrete Mathematics and its Applications*
- J.L. Gersting. *Mathematical Structures for Computer Science*
- J.K. Truss. *Discrete Mathematics for Computer Science*
- R. Johnsonbaugh. *Discrete Mathematics*
- C. Schumacher. *Fundamental Notions of Abstract Mathematics*

However, these books don't cover the same content. Learn his notation.

Logical Formula, and Notation

This notation will be shared with **CO140**.

- $A \wedge B$ A and B both hold
- $A \vee B$ A or B holds (or both)
- $\neg A$ A does not hold
- $A \Rightarrow B$ if A holds, then so does B
- $A \Leftrightarrow B$ A holds if and only if B holds
- $\forall x(A)$ the predicate A holds for all x
- $\exists x(A)$ the predicate A holds for some x
- $a \in A$ the object a is in the set A (a is an element of
- A)
- $a \notin A$ the object a is not in the set A
- $=_A$ tests whether two elements of A are the same

Sets

Sets are like data types in Haskell: Haskell data type declaration;

- `data Bool = False | True`
- `{false, true}` set of boolean values
- `[true, false, true, false]` list of boolean values
- `{false, true} = {true, false}` set equality (note that order doesn't matter)

A set is a collection of objects from a pool of objects. Each object is an *element*, or a *member* of the set. A set *contains* its elements. Sets can be defined in the following ways;

- $\{a_1, \dots, a_2\}$ as a collection of n distinct elements
- $\{x \in A \mid P(x)\}$ for all the elements in A, where P holds
- $\{x \mid P(x)\}$ for all elements, where P holds (dangerous - Russel's paradox)

Use of "triangleq"

The use of \triangleq is for "is defined by". Hence the empty set, $\emptyset \triangleq \{\}$. The difference between \triangleq and $=$, is that the former cannot be proven, it is fact, whereas the latter takes work to prove.

Russel's paradox

Not everything we write as $\{x \mid P(x)\}$ is automatically a set. Assume $R = \{X \mid X \notin X\}$ is a set, the set of all sets which don't contain themselves. As R is a set, then $R \in R$, or $R \notin R$ (law of excluded middle), and thus we can do a case by case analysis.

- Assume $R \in R$. By the definition of R , it then follows that $R \notin R$ (if $R \in R$, then it doesn't satisfy the definition of R) - which is a contradiction.
- Assume $R \notin R$. It then follows that $R \in R$, as it follows the definition of R , hence it is another contradiction.

As both assumptions lead to contradictions, it's possible to write sets which aren't defined. We should only select from a set that we know is defined; $\{x \in A \mid P(x)\}$ - where A is a well-defined set.

12th October 2018

Set Comparisons

We can define a set A , as being a subset of another set B if every element in A is an element in B . This can be formally written as; $A \subseteq B \triangleq \forall x \in A (x \in B)$. Note that we can also say $\forall x (x \in A \Rightarrow x \in B)$, and the two hold the same meaning. It's important to clarify in the latter that we're not the domain of x , as we assume there is a universe of possible objects which forms a set. We're also able to define a strict subset such that $A \subset B \triangleq A \subseteq B \wedge A \neq B$.

We can say that any set is a trivial subset of itself, as we'd have $x \in A \Rightarrow x \in A$, which always evaluates to true, from propositional logic. Another trivial example is that \emptyset , the empty set, is a subset of every set. Using the second definition of subset, we can say that as $x \in \emptyset$ is false, by definition, and anything follows from falsity, whereas in the first definition we argue that all (0) elements of \emptyset are in some other set.

We can also define set equality as $A = B \triangleq A \subseteq B \wedge B \subseteq A$. However, we can also consider the set composition notation for a set, such that $A = \{x \in C \mid P(x)\}$, and $B = \{x \in C \mid Q(x)\}$. If we're able to prove that $\forall x (P(x) \Leftrightarrow Q(x))$, it follows that $A = B$. This method can be quite powerful if we're familiar with logic, and equivalences. We can justify this by saying that $y \in A \Rightarrow P(y) \Rightarrow Q(y) \Rightarrow y \in B$, and also in the other direction; $y \in B \Rightarrow Q(y) \Rightarrow P(y) \Rightarrow y \in A$. This however requires both sets to be constructed on top of some known set C .

Set Composition

- $A \cup B \triangleq \{x \mid x \in A \vee x \in B\}$ set union
- $A \cap B \triangleq \{x \in A \mid x \in B\}$ set intersection
- $A \setminus B$ (or $A - B$) $\triangleq \{x \in A \mid x \notin B\}$ set difference
- $A \triangle B \triangleq (A \setminus B) \cup (B \setminus A)$ symmetric set difference))
- $A \cap B = \emptyset$ disjoint set

A Note on Proofs

Instead of writing out the formal definition, where we may lose the intuition, using a natural language (direct) proof is acceptable in this course.

Consider the following proof; $A \subseteq B$, and $B \subseteq C$, then show $A \subseteq C$. Here, we want to show that any element of A , is also an element of C . We can approach this intuitively by taking an arbitrary $a \in A$. By the first assumption, we can say $a \in B$. Then, by the second assumption, $a \in C$. However, we've taken an arbitrary a , therefore this follows $\forall a \in A (a \in C)$, therefore $A \subseteq C$.

The crucial part of the aforementioned proof is the use of some **arbitrary** value. If we were to do a proof on the natural numbers, to show $\forall n \in \mathbb{N} [\text{even}(n)]$, and we proved $\text{even}(2)$, it wouldn't prove it for all natural numbers.

We also want to aim for a direct proof, instead of a proof by contradiction, since we will often do the following; assume $\neg A$, then we somehow get A , which causes a contradiction (\bot), and therefore A . However, we still did all the work to prove A .

Consider the proof to show that $C \cap D = D \cap C$. Let us first take some arbitrary $x \in (C \cap D)$. By definition of union, we know that $x \in C$, and $x \in D$. Therefore, it also fits the predicate for $(D \cap C)$. As such, $C \cap D \subseteq D \cap C$. To prove the other direction is trivial, and almost identical to this direction. Since we've proved both directions of \subseteq , we can conclude equality.

Prove that $A = (A \setminus B) \cup (A \cap B)$. I took the approach where we use predicate logic, since I assumed it would be much easier than proving both directions of \subseteq (turns out that the proof is very similar as proving one direction, is proving the other). In order to keep my proof cleaner, let $a \triangleq x \in A$, $b \triangleq x \in B$, and the negations $\neg a \triangleq x \notin A$ (and similar for b). Let us now define $A = \{x \mid P(x)\}$, where $P(x) = a$, and $B = \{x \mid Q(x)\}$, where $Q(x) = (a \wedge \neg b) \vee (a \wedge b)$ - by definitions of set difference, union, and intersection. Since this proves equivalence between the two predicates, we can therefore prove that the sets are equal.

$$\begin{aligned}
 Q(x) &= (a \wedge \neg b) \vee (a \wedge b) \\
 &= [(a \wedge \neg b) \vee a] \wedge [(a \wedge \neg b) \vee b] && (B \wedge C) \vee A \equiv (A \vee B) \wedge (A \vee C) \\
 &= (a \vee a) \wedge (a \vee \neg b) \wedge (a \vee b) \vee (b \vee \neg b) && (B \wedge C) \vee A \equiv (A \vee B) \wedge (A \vee C) \text{ (twice)} \\
 &= a \wedge (a \vee \neg b) \wedge (a \vee b) && A \vee A \equiv A, A \vee \neg A \equiv \top, \text{ and } A \wedge \top \equiv A \\
 &= a && A \wedge (A \vee B) \equiv A \text{ (twice)} \\
 &= P(x)
 \end{aligned}$$

16th October 2018

A Note on the Use of Venn Diagrams

While we can use a Venn diagram to aid in constructing a counter example, the diagram itself is not a counter example. We're also quite limited in the possible uses, as a diagram (in 2d) consisting of ≥ 4 sets doesn't represent all the possible combinations of sets.

Operator Properties

Similar to **CO140**, we have some properties which can be used on arbitrary sets. Note that these are not axioms, and therefore we are able to prove them.

- $A \cup A = A$ idempotence
- $A \cap A = A$ idempotence
- $A \cup B = B \cup A$ commutativity
- $A \cap B = B \cap A$ commutativity
- $A \triangle B = B \triangle A$ commutativity
- $A \cup (B \cup C) = (A \cup B) \cup C$ associativity
- $A \cap (B \cap C) = (A \cap B) \cap C$ associativity

- $A \cup \emptyset = A$ empty set
- $A \cap \emptyset = \emptyset$ empty set
- $A \Delta A = \emptyset$ empty set
- $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ distributivity
- $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ distributivity
- $A \cup (A \cap B) = A$ absorption
- $A \cap (A \cup B) = A$ absorption

Note that we are able to use the properties of logical connectives to aid us in our proofs, since those are fairly easy to prove with truth tables, as they have a finite number of configurations. For example, the proof of idempotence inherently uses the property $p \wedge p \equiv p$, and the same for \vee .

Cardinality

With some finite set A , we can say that the cardinality, $|A|$ is the number of distinct elements in A . Given two finite sets, we can then say that $|A \cup B| = |A| + |B| - |A \cap B|$. With the following set properties (and that for two disjoint finite sets, $|A \cup B| = |A| + |B|$), and knowing the RHSs are disjoint unions;

$$\begin{aligned}
 A &= (A \setminus B) \cup (A \cap B) \\
 B &= (B \setminus A) \cup (A \cap B) \\
 A \cup B &= (A \setminus B) \cup (A \cap B) \cup (B \setminus A) \\
 |A| &= |A \setminus B| + |A \cap B| \\
 |B| &= |B \setminus A| + |A \cap B| \\
 |A \cup B| &= |A \setminus B| + |A \cap B| + |B \setminus A| \\
 &= |A| - |A \cap B| + |A \cap B| + |B| - |A \cap B| \\
 &= |A| + |B| - |A \cap B|
 \end{aligned}$$

19th October 2018

Powerset

Let us define the powerset of A , as $\wp A \triangleq \{x \mid x \subseteq A\}$. It's therefore important to note that $\wp \emptyset = \{\emptyset\}$, hence the powerset of the empty set has size 1. We can prove that $|\wp X| = 2^n$, for some set X , where $|X| = n$. This can be done (fairly) easily with mathematical induction, over natural numbers. Another approach it is to consider that each item in some arbitrary set, $A = \{a_1, a_2, \dots, a_n\}$, can either be in the powerset or not. Therefore, we can represent each subset of A as some n -bit binary number. Therefore, we can have a 2^n possible combinations, hence the size of $|\wp A| = 2^n$.

Products

Let us define some **ordered** pair as $\langle a, b \rangle$, such that generally $\langle a, b \rangle \neq \langle b, a \rangle$.

Let there be some arbitrary sets A , and B . We can then define the cartesian product as follows; $A \times B \triangleq \{\langle a, b \rangle \mid a \in A \wedge b \in B\}$. Since we'll often deal with binary relations, we use the shorthand $A^2 = A \times A$. We can define equality on ordered pairs as $\forall a, b, c, d [\langle a, b \rangle =_{A \times B} \langle c, d \rangle \triangleq a =_A c \wedge b =_B d]$. Note that in general, \times is not a commutative operation.

Suppose that there are two finite sets $A = \{a_1, a_2, \dots, a_n\}$, and $B = \{b_1, b_2, \dots, b_m\}$, with sizes n , and m respectively - then it follows that $|A \times B| = |A| \cdot |B|$. We can justify this by constructing such a matrix R , of dimension $(A \times B)^{n,m}$ - thus having $n \cdot m$ elements;

$$R = \begin{array}{cccc} \langle a_1, b_1 \rangle & \langle a_1, b_2 \rangle & \cdots & \langle a_1, b_m \rangle \\ \langle a_2, b_1 \rangle & \langle a_2, b_2 \rangle & \cdots & \langle a_2, b_m \rangle \\ \vdots & \vdots & \ddots & \vdots \\ \langle a_n, b_1 \rangle & \langle a_n, b_2 \rangle & \cdots & \langle a_n, b_m \rangle \end{array}$$

We can also have an n -ary product, to construct an n -tuple $\langle a_1, a_2, \dots, a_n \rangle$, when $n \geq 1$. Let there be some arbitrary sets, A_1, A_2, \dots, A_n .

This is written as $A_1 \times \dots \times A_n = \prod_{i=1}^n A_i$, and is defined as $\{\langle a_1, a_2, \dots, a_n \rangle \mid \forall i \in [1, n][a_i \in A_i]\}$.

Partitions

Given some set S , we can define a **partition** of S to be a family of subsets $\{A_1, A_2, \dots, A_n\}$ such that;

- none of them are empty (therefore $\forall i \in [1, n][A_i \neq \emptyset]$)
- the subsets cover S (therefore $S = \bigcup_{i=1}^n A_i$)
- they are pairwise disjoint (therefore $\forall i, j \in [1, n][i \neq j \Rightarrow A_i \cap A_j = \emptyset]$)

A partition of S is a set of non-empty subsets that are pairwise disjoint, and cover S .

Pigeonhole Principle

Given a set S of size n , partitioned into k sets such that $0 < k < n$, then at least one of the subsets must have at least 2 elements. We can prove this by contradiction (one of the few times we actually do this, in DS). Assume that there are k subsets, each of size 1 (therefore $\forall i \in [1, k][|A_i| = 1]$). By definition of a partition, we can form a cover of S , therefore (the last 2 steps are justified by the requirement of a partition being pairwise disjoint);

$$n = |S| = \left| \bigcup_{i=1}^k A_i \right| = \sum_{i=1}^k |A_i| = \sum_{i=1}^k 1 = k$$

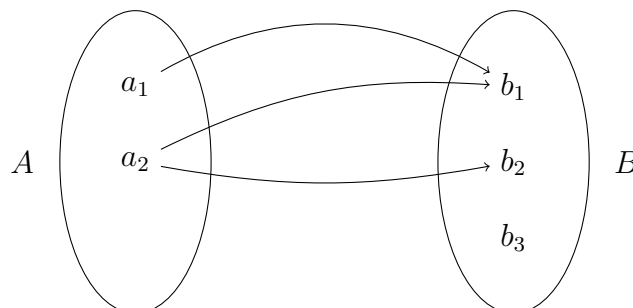
However, given the bounding condition $k < n$, there is no way that $k = n$, and the only assumption is that we made k sets of size 1.

Representing Relations

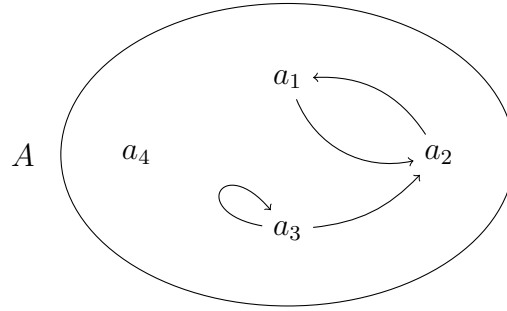
We define a relation between two sets A , and B (from A to B), as a subset of $A \times B$, such that $R \subseteq A \times B$. If we say that $R \subseteq A \times B$, it means that it has type $A \times B$. However, if $R \subseteq A^2$, it is a **binary** relation on A . Instead of writing $\langle a, b \rangle \in R$, we will often shorten it to $a R b$.

A relation does not have to be meaningful; for a set of size $n = 2$, let it be $A = \{a, b\}$, it can have 16 (2^{n^2}) possible binary relations. For any set A , the possible binary relations can be generated by taking $\wp A^2$. A predicate over A is a 1-ary relation, which is just a subset of A . We also can say something along the lines of $\{\langle x, y, z \rangle \in \mathbb{R}^3 \mid x^2 + y^2 + z^2 = 1\}$, as a ternary relation on the reals which covers the surface of a unit sphere at the origin.

Generally, writing out all pairs can become tedious, therefore there are numerous other ways of representing it. We can construct a diagram (a bipartite graph) for the following relation $A = \{a_1, a_2\}$, $B = \{b_1, b_2, b_3\}$, and $R = \{\langle a_1, b_1 \rangle, \langle a_2, b_1 \rangle, \langle a_2, b_2 \rangle\}$;



However, we might also want to represent a binary relation in a similar way, in which case we can draw a regular directed graph. Here we have $A = \{a_1, a_2, a_3, a_4\}$, and $R = \{\langle a_1, a_2 \rangle, \langle a_2, a_1 \rangle, \langle a_3, a_2 \rangle, \langle a_3, a_3 \rangle\}$;



It can also be represented as a matrix, such that we have

$$M_{i,j} = \begin{cases} \text{True} & \text{if } a_i R b_j \\ \text{False} & \text{otherwise} \end{cases}$$

Constructing Relations

Just like in sets, we can construct relations quite easily. Except, we now have a known set in they exist in (by the subset definition), hence (these examples use $R, S \subseteq A \times B$, and $T \subseteq B \times C$);

- $R \cup S \triangleq \{\langle a, b \rangle \in A \times B \mid \langle a, b \rangle \in R \vee \langle a, b \rangle \in S\}$ relation union
- $R \cap S \triangleq \{\langle a, b \rangle \in A \times B \mid \langle a, b \rangle \in R \wedge \langle a, b \rangle \in S\}$ relation intersection
- $\overline{R} \triangleq \{\langle a, b \rangle \in A \times B \mid \langle a, b \rangle \notin R\}$ relation complement
- $R^{-1} \triangleq \{\langle b, a \rangle \in B \times A \mid a R b\}$ inverse relation
- $\text{id}_A \triangleq \{\langle x, y \rangle \in A^2 \mid x =_A y\}$ identity relation
- $R \circ T \triangleq \{\langle a, c \rangle \in A \times C \mid \exists b \in B [a R b \wedge b T c]\}$ relation composition

this is only defined when the types are matching

we can define $\text{grandparentof} \triangleq \text{parentof} \circ \text{parentof}$

therefore $x \text{ gpo } y \triangleq \exists z (x \text{ po } z \wedge z \text{ po } y)$

23rd October 2018

To be honest, this lecture was basically just a tutorial. Some solutions are listed here;

Associativity of \circ

For arbitrary relations, $R \subseteq A \times B$, $S \subseteq B \times C$, and $T \subseteq C \times D$, show that $R \circ (S \circ T) = (R \circ S) \circ T$

Take some arbitrary $\langle x, y \rangle \in R \circ (S \circ T)$;

$$\begin{aligned} x R \circ (S \circ T) y &\triangleq \exists z [x R z \wedge z (S \circ T) y] \\ &\triangleq \exists z [x R z \wedge \exists w [z S w \wedge w T y]] \\ &\Leftrightarrow \exists w, z [x R z \wedge z S w \wedge w T y] \\ &\Leftrightarrow \exists w [x (R \circ S) w \wedge w T y] \\ &\triangleq x (R \circ S) \circ T y \end{aligned}$$

The key point to take from this proof is how we can use our knowledge of propositional logic, and apply it to sets. Since propositional logic is far easier to prove than an arbitrary set, we can reduce the work we do significantly.

Subsets of Inverse Relations

Given two binary relations $R, S \subseteq A^2$, prove that $R \subseteq S \Rightarrow R^{-1} \subseteq S^{-1}$

Take some arbitrary $\langle y, x \rangle \in R^{-1}$. In order to show the RHS, we want to show that this is also in S^{-1} . Let us also make the assumption (the LHS) that $R \subseteq S$, such that $k \in R \Rightarrow k \in S$, where k is any tuple. As we have some $\langle y, x \rangle \in R^{-1}$, it follows that there is a corresponding $\langle x, y \rangle \in R$. Because of our assumption, we can say that $\langle x, y \rangle \in S$, and therefore $\langle y, x \rangle \in S^{-1}$. Therefore, any arbitrary element of R^{-1} is also in S^{-1} , hence $R^{-1} \subseteq S^{-1}$ (given our assumption holds) - so $R \subseteq S \Rightarrow R^{-1} \subseteq S^{-1}$.

26th October 2018

The first part is just some stuff about how you should be doing proofs in natural language, as mathematics (and symbols) is just formalised human thinking. This then goes into (basically) natural deduction - so check **CO140** for techniques you can apply in proofs. Once again, we went through more questions in this lecture.

Relation Properties

Let there be $R \subseteq A^2$, such that R is a binary relation on A ;

- R is reflexive $\triangleq \forall x \in A[\langle x, x \rangle \in R]$
 $\Leftrightarrow \text{id}_A \subseteq R$
- R is symmetric $\triangleq \forall x, y \in A[\langle x, y \rangle \in R \Rightarrow \langle y, x \rangle \in R]$
 $\Leftrightarrow R = R^{-1}$
- R is transitive $\triangleq \forall x, z \in A[\exists y \in A[\langle x, y \rangle \in R \wedge \langle y, z \rangle \in R] \Rightarrow \langle x, z \rangle \in R]$
 $\Leftrightarrow R \circ R \subseteq R$
- R is an equivalence relation if it is reflexive, symmetric, and transitive

We consider something to be an equivalence if it has a weak equality, such that $a R b$ means that a is indistinguishable from b in some sense. We can write this as $a \sim_R b$.

30th October 2018

Equivalence Classes

Given $n \neq 0$, and $n \in \mathbb{N}$, the binary relation R_n on \mathbb{Z} is defined by $a R_n b$ when n divides into $(b - a)$ is defined as; $R_n \triangleq \{\langle a, b \rangle \in \mathbb{Z}^2 \mid \exists q \in \mathbb{Z}[q \cdot n = (b - a)]\}$. This means that two numbers are in the same equivalence class given that they are an integer multiple of n apart. As such, they have the same result under modulo n .

Suppose we have some R , which is an equivalence relation on A . For any $a \in A$, we can define the equivalence class of a with respect to R as follows; $[a]_R \triangleq \{b \in A \mid a \sim_R b\}$. For brevity, we can omit the $_R$ when it's clear what equivalence relation we're referring to from the context. The set of equivalence classes is referred to as the **quotient set**; $\frac{A}{R}$; therefore with the example above, the set $\frac{\mathbb{Z}}{R_n}$ is the quotient set which represents integers which have modulo n .

Let us propose that the set of all equivalence classes, $\{[a] \mid a \in A\}$, forms a partition of A . This means that the equivalence classes aren't empty, they form a cover of A , and that they are pairwise disjoint.

We need to first show that no equivalence class is empty. First, let's take some arbitrary $x \in A$. By the reflexive nature of equivalences, we know that $x \sim_R x$, hence $x \in [x]$. As we took an arbitrary element of A , it's satisfied for all A , therefore none of the equivalence classes are empty.

Next we need to prove that it forms a cover of A , such that $A = \bigcup_{a \in A} [a]$; done by proving that $A \subseteq \bigcup_{a \in A} [a]$, and also $\bigcup_{a \in A} [a] \subseteq A$.

Doing the former, let us take some arbitrary $x \in A$. Now, it follows that it's in its own equivalence class $[x]$, under the same justification we gave for the first part of the proof ($x \sim_R x$ by reflexivity). Trivially, we can say that $[x] \subseteq \bigcup_{a \in A} [a]$. Hence $x \in \bigcup_{a \in A} [a]$, and as we took arbitrary x ; $A \subseteq \bigcup_{a \in A} [a]$.

To prove the other direction, take some arbitrary equivalence class $[x] \in \bigcup_{a \in A} [a]$, and arbitrary $y \in [x]$. This then means we've taken arbitrary $y \in \bigcup_{a \in A} [a]$.

By our definition of an equivalence class, for $y \in [x]$, it must therefore mean $x \sim_R y$, and also that $y \in A$. Hence we get $\bigcup_{a \in A} [a] \subseteq A$. As we have both directions of \subseteq , we conclude the two sets are equal.

The last one can be done by proving two equivalence classes are equal, if they aren't pairwise disjoint. Suppose two arbitrary classes in the set of equivalence classes aren't pairwise disjoint, such that $[x] \cap [y] \neq \emptyset$. Therefore, this means that $w \in ([x] \cap [y])$, by definition of set union, we can then say that $w \in [x]$, and also $w \in [y]$. This then leads to $x \sim_R w$, and also $y \sim_R w$, by definition. However, by symmetry, we can rewrite the former as $w \sim_R x$. To establish equality, we need to show that they are subsets of each other (will only do one, since it's trivial to do the other way around). Take some arbitrary $v \in [x]$, then it follows that $x \sim_R v$. By transitivity, we can now say $w \sim_R v$, and therefore also $y \sim_R v$. It then follows that $v \in [y]$. As we took arbitrary $v \in [x]$, it follows that $[x] \subseteq [y]$. Hence the only way two items aren't disjoint in a set of equivalence classes, is when they are equal. Thus, the family of equivalence classes is pairwise disjoint, and is a partition of A .

Transitive Closure

Strange that I'm revising this **after** doing Warshall's algorithm in **CO150**. It's probably a better idea to learn the pre-requisites for a module, before doing it.

Suppose we have a binary relation R on A . We define the transitive closure of R^+ , such that it's the smallest transitive relation that contains R . Defining R^k is required;

$$\begin{aligned} R^1 &\triangleq R \\ R^2 &\triangleq R \circ R \\ R^3 &\triangleq R \circ R \circ R = R \circ (R^2) \\ &\dots \\ R^k &\triangleq R \circ R \circ \dots \circ R \quad (k \text{ times}) \end{aligned}$$

We can then define $R^+ \triangleq \bigcup_{i \geq 1} R^i$, and thus we get $a R^+ b \Leftrightarrow \exists i \geq 1 [a R^i b]$.

Let R be some finite binary relation on A . If R is already transitive, then there is no more work we need to do. However, in the case that it's not transitive, it must mean that there is some $a, b, c \in A$ such that we have $a R b$, and also $b R c$, but not $a R c$. We then add the pair $\langle a, c \rangle$ to the relation. This is then repeated until we reach a point where the relation is transitive, and we are done.

Since every step was a requirement of transitivity, we have obtained the smallest possible relation containing R . In our proofs, we are allowed to create an infinite construction, but **not** an infinite step proof.

Consider some relation $<_1 \triangleq \{\langle m, n \rangle \in \mathbb{N}^2 \mid m = n + 1\}$ over \mathbb{N} . This relation represents a difference of 1. Now, we can construct $<_2 = <_1 \circ <_1$ (fairly trivial to prove, since we know it covers the naturals, we can almost approach it inductively, however there is an easier solution where we use the properties of natural numbers (hint - if $n \in \mathbb{N}$, then $n + 1 \in \mathbb{N}$)). The transitive closure on $<_1$, $<_1^+$, is therefore $<$.

Note that I won't include most of the exercises, because it's surprisingly laborious to typeset them on L^AT_EX, especially when I'm sleep deprived. The ones included are ones that have specific techniques that we should remember for the exam.

2nd November 2018

Peano Arithmetic

Peano defined a set of **axioms** for the naturals, such that for the set \mathbb{N} , it must satisfy the properties;

1. $0 \in \mathbb{N}$
2. if $n \in \mathbb{N}$, then $\text{Succ}(n) \in \mathbb{N}$
3. for all $n \in \mathbb{N}$, $\text{Succ}(n) \neq 0$
4. for all $n, m \in \mathbb{N}$, if $\text{Succ}(n) = \text{Succ}(m)$, then $n = m$
5. suppose there is a set V , such that $0 \in V$, and for all $n \in \mathbb{N}$, if $n \in V$ then $\text{Succ}(n) \in V$, then $\mathbb{N} \subseteq V$

Note that the 5th point is the principle of induction. Let us also define arithmetic as follows, on the successor function (will use $S(n)$ to represent $\text{Succ}(n)$, $A(m, n)$ to represent $\text{Add}(m, n)$, and $M(m, n)$ to represent $\text{Mult}(m, n)$;

- $A(0, n) = n$
- $A(S(m), 0) = S(A(m))$
- $M(0, n) = 0$
- $M(S(m), n) = A(M(m, n), n)$

Let us prove that $\forall n \in \mathbb{N}[A(n, S(0)) = S(n)]$. By the principle of induction, let us define some set $V \triangleq \{n \mid A(n, S(0)) = S(n)\}$. First, we have to show $0 \in V$, which means showing that $A(0, S(0)) = S(0)$. By the first case for addition, we can show the predicate holds trivially, hence $0 \in V$.

Now, let us make the assumption that some arbitrary $k \in \mathbb{N}$, $n \in V$, such that we are given $A(k, S(0)) = S(k)$. Our goal here is to prove that $S(k) \in V$, by showing $A(S(k), S(0)) = S(S(k))$. By the second case of addition, we can say that $A(S(k), S(0)) = S(A(k, S(0)))$. However, by our assumption, we can substitute the value for $S(k)$, therefore $S(S(k))$. Therefore, by our assumption, we can say $k \in V \Rightarrow S(k) \in V$. By the principle of induction, it follows that $\mathbb{N} \subseteq V$, hence $\forall n \in \mathbb{N}[A(n, S(0)) = S(n)]$.

While the idea of an infinite proof seems acceptable to us, intuitively, we cannot do an infinite proof. We are allowed to do infinite constructions, but not a proof with infinite steps, hence we must use induction.

Defining Natural Numbers with Sets

Assuming that our notion of sets is real, we can recursively define natural numbers as follows;

$$\begin{aligned} 0 &\triangleq \emptyset \\ n &\triangleq n-1 \cup \{n-1\} \\ &= n-2 \cup \{n-2\} \cup \{n-1\} \\ &= \dots \\ &= \{1, 2, 3, \dots, n-2, n-1\} \\ 0 &= \emptyset \\ 1 &= \emptyset \cup \{\emptyset\} \\ &= \{\emptyset\} \\ 2 &= \{\emptyset\} \cup \{\{\emptyset\}\} \\ &= \{\emptyset, \{\emptyset\}\} \end{aligned}$$

Defining Integers, and Rational Numbers

We can define the integers, \mathbb{Z} , as $\mathbb{Z} \triangleq \mathbb{N} \cup \{-n \mid n \in \mathbb{N}\}$. We can also define equality on the integers, $=_{\mathbb{Z}}$, as $=_{\mathbb{Z}} \triangleq \langle -0, 0 \rangle \cup \{\langle n, m \rangle \mid n =_{\mathbb{N}} m\} \cup \{\langle -n, -m \rangle \mid n =_{\mathbb{N}} m\}$, which covers all the cases (note the specific inclusion of ± 0). By these definitions, we can see that $\mathbb{N} \subseteq \mathbb{Z}$.

With this, we're also able to define the rational numbers, \mathbb{Q} , as $\mathbb{Q} \triangleq \mathbb{Z} \times \mathbb{N}$, and we can define equality over the natural numbers, $=_{\mathbb{Q}}$, as $=_{\mathbb{Q}} \triangleq \{\langle \langle n_1, m_1 \rangle, \langle n_2, m_2 \rangle \rangle \in (\mathbb{Z} \times \mathbb{N})^2 \mid n_1 \cdot m_2 =_{\mathbb{Z}} n_2 \cdot m_1\}$. Note that the slides use $=_{\mathbb{N}}$, which is incorrect, as we have no guarantee that the product of a natural, and an integer is a natural, but we can guarantee it is an integer by the closure of multiplication on integers.

Defining $=_{\mathbb{R}}$ takes much more work. It's also established that every sequence of rational (\mathbb{Q}) numbers, e.g. $\{3, 3.1, 3.14, 3.141, 3.145, \dots\}$ has an upper limit in \mathbb{R} .

6th November 2018

Functions

We define a function f , from A (the function domain) to B (the function co-domain) as $f : A \mapsto B$ (should I be using \mapsto , or \rightarrow here?). **Every** element of A must map to a **unique** (exactly 1) element in B . We can formally write this as follows, where both conditions must hold;

1. $\forall a \in A \forall b_1, b_2 \in B [\langle a, b_1 \rangle \in f \wedge \langle a, b_2 \rangle \in f \Rightarrow b_1 = b_2]$
2. $\forall a \in A \exists b \in B [\langle a, b \rangle \in f]$

The set of all functions from A , to B is denoted as B^A , such that $B^A \subseteq \wp(A \times B)$. For brevity, we can use the following shorthands;

- $f : A \mapsto B$ is short for $f \subseteq B^A$
- $\exists f : A \mapsto B[\dots]$ is short for $\exists f \in B^A[\dots]$
- $\forall f : A \mapsto B[\dots]$ is short for $\forall f \in B^A[\dots]$
- suppose that A is an n -ary product $A_1 \times \dots \times A_n$, we can write $f(a_1, \dots, a_n)$ instead of $f(\langle a_1, \dots, a_n \rangle)$

We define equality on two functions $f, g : A \mapsto B$, as $f =_{A \times B} g \triangleq \forall x \in A [f(x) =_B g(x)]$.

For any subset of A , $X \subseteq A$, the image of X under f is denoted $f[X] \triangleq \{f(x) \mid x \in X\}$. We can define the image set of A , as $f[A]$. For example, let there be sets $A = \{1, 2, 3\}$, $B = \{a, b, c\}$, and the function $f = \{\langle 1, a \rangle, \langle 2, b \rangle, \langle 3, a \rangle\}$. The image set of A , $f[A]$, is $\{a, b\}$, and the image set $f[\{1, 3\}] = \{a\}$.

These are some examples of functions;

- $f : \mathbb{N}^2 \mapsto \mathbb{N}$ $f(x, y) = x + y$
- $f : \mathbb{N} \mapsto \mathbb{N}$ $f(x) = x^2$
- $f : \mathbb{R} \mapsto \mathbb{R}$ $f(x) = x + 3$

However, the **relation** $R \triangleq \{\langle x, y \rangle \in \mathbb{R}^2 \mid x = y^2\}$ is not a function, as we can easily prove a one-to-many relationship, thus violating the first condition. For example; both $\langle 1, -1 \rangle$, and $\langle 1, 1 \rangle$ are in R , but clearly $-1 \neq_{\mathbb{R}} 1$. In order to verify a function is actually a function, we must prove that the LHS has 1 unique mapping.

Cardinality of Function Space

Let B^A represent the function space of all functions mapping from A to B , where both A , and B are finite sets, such that $|A| = m$, and $|B| = n$. For something to be a function, every item in A , must map to an item in B . For any item in A , there are n independent options to which it can map to. Hence it follows that there are n^m unique options; thus $|B^A| = n^m$.

Characteristic Function

Suppose we have a set A , and the characteristic function of $B \subseteq A$ is defined as $\chi_B : A \mapsto \{0, 1\}$, and for some n -ary relation R , such that $R \subseteq A_1 \times \dots \times A_n$, we can define $\chi_R : A_1 \times \dots \times A_n \mapsto \{0, 1\}$;

$$\chi_B(a) = \begin{cases} 1 & \text{if } a \in B \\ 0 & \text{if } a \in A \setminus B \end{cases}$$
$$\chi_R(a_1, \dots, a_n) = \begin{cases} 1 & \text{if } \langle a_1, \dots, a_n \rangle \in R \\ 0 & \text{if } \langle a_1, \dots, a_n \rangle \notin R \end{cases}$$

Partial Functions

A partial function is a function **without** the second condition, therefore not all elements in A , must have a corresponding element in B . We denote an undefined value as \perp , therefore we can create a "function" from a partial function by saying $f : A \mapsto (B \cup \{\perp\})$. If you are asked to give a function in an exam, **do not give a partial function**.

Properties of Functions

We will be working on some function $f : A \mapsto B$.

- f is onto (surjective) when every element of B is in the image of A
 $\forall b \in B \exists a \in A [f(a) =_B b]$
also $f[A] = B$ (?)
- f is one-to-one (injective) when every element of B has **at most one** $a \in A$ with $f(a) = b$
 $\forall a_1, a_2 \in A [f(a_1) =_B f(a_2) \Rightarrow a_1 =_A a_2]$
- f is bijective, if it is both surjective (onto), and injective (one-to-one)

The (Dual) Cantor-Bernstein Theorem states that if there exists $f : A \mapsto B$, and $g : B \mapsto A$, where they are both surjective, or both injective, then it follows that there is a bijection $h : A \mapsto B$. This theorem is extremely helpful when we want to prove that two infinite sets have the same cardinality.

These are some example functions, and their properties;

- $f : \mathbb{N}^2 \mapsto \mathbb{N}$ $f(x, y) = x + y$
we can prove it is surjective by taking some arbitrary $n \in \mathbb{N}$, and proving that $f(n, 0) = n + 0 = n$
we can prove it is not injective by finding a counter example, such as $f(0, 1) = 1 = f(1, 0)$, but $\langle 0, 1 \rangle \neq \langle 1, 0 \rangle$
- $f : \mathbb{N} \mapsto \mathbb{N}$ $f(x) = x^2$
we can prove it is not surjective by finding a counter example; such as $f(x) = 3$, as there is no $x \in \mathbb{N}$ such that $x^2 = 3$
- $f : \mathbb{R} \mapsto \mathbb{R}$ $f(x) = 4x + 3$
this is bijective

Some Proof on Function Image?

No idea what this should actually be titled. But let there be a finite set A , a function $f : A \mapsto B$, and $X \subseteq A$. We want to prove that $|f[X]| \leq |X|$.

By contradiction, let us assume that $|f[X]| > |X|$. Define a function p , such that $p : f[X] \mapsto X$. Suppose we pick an arbitrary $b \in f[X]$, and some $a \in X$ (we know this exists by definition of image), such that we have $f(a) = b$, and define $p(b) = a$.

We take y , from $f[X]$, and place it into a pigeonhole labeled x , where $x \in X$, if $p(y) = x$. By the pigeonhole principle, there exists some $c \in X$, such that $d, d' \in f[X]$ (because the image set is larger). Hence, it follows that $p(d) = p(d') = c$. But, by definition of p , we have $f(c) = d$, and also $f(c) = d'$. Therefore, f isn't a function, hence we have a contradiction.

9th November 2018

An Improvement on Last Lecture's Proof

Using the same introduction as last lecture's proof, construct sets for all $x \in X$, $V_x \subseteq f[X]$. If for some $a \in X$, $f(a) = b$, then $b \in f[X]$ (by definition of the image), and $b \in V_a$ (by our definition). By making our assumption (which we want to be able to derive a contradiction from) $|f[X]| > |X|$. Therefore, $\exists c \in X[|V_c| > 1]$. So, we're able to say that there are distinct $d, d' \in V_c$. But by our definition of V_c , it follows that $f(c) = d$, and also $f(c) = d'$. This is not possible, as we defined f as a function, hence we have a contradiction. The main issue with last week's proof was assuming we had an inverse function, p .

Proposition on the Property of Functions

Given two **finite** sets (these do not always apply to infinite sets) A , and B , and a function $f : A \mapsto B$, we can say that if...

- f is onto (surjective), then $|A| \geq |B|$
 note that if it is injective, then $f[A] = B$, therefore $|f[A]| = |B|$
 we can use what we just proved, that $|f[A]| \leq |A|$, so $|A| \geq |B|$
- f is one-to-one (injective), then $|A| \leq |B|$
 contraposition of the pigeonhole principle, or something
- f is bijective, then $|A| = |B|$
 this follows from the first two, trivially

Function Composition

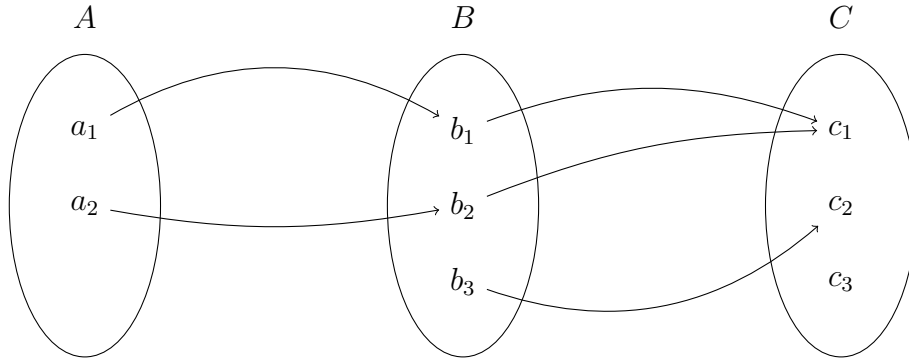
Suppose we have arbitrary sets, A , B , C , and let there be two functions $f : A \mapsto B$, and $g : B \mapsto C$. We can define the composition of f with g (meaning g applied to the image of f), as $\langle a, c \rangle \in (g \circ f) \triangleq \exists b \in B[\langle a, b \rangle \in f \wedge \langle b, c \rangle \in g]$ where $(g \circ f) : A \mapsto C$. It's important to note that the order of the arguments is flipped, compared to relation composition. The crucial requirement is that the co-domain of f matches the domain of g .

We can prove that function composition is associative quite trivially. Recall that two functions i, j (let them both be functions from A to B) are equal if $\forall a \in A[i(a) =_B j(a)]$. We want to prove that $h \circ (g \circ f) = (h \circ g) \circ f$, and we are using the same definitions mentioned previously, plus a new set D , and $h : C \mapsto D$. We first take an arbitrary $a \in A$;

$$\begin{aligned} (h \circ (g \circ f))(a) &= h((g \circ f)(a)) \\ &= h(g(f(a))) \\ &= (h \circ g)(f(a)) \\ &= ((h \circ g) \circ f)(a) \end{aligned}$$

As we have taken arbitrary $a \in A$, it follows that the two are equal.

When we're working with function compositions, especially when we're told to give a specific example, it's useful to draw out diagrams (wish I knew that during the Christmas exam). The example below has $f : A \mapsto B$, such that $f = \{\langle a_1, b_1 \rangle, \langle a_2, b_2 \rangle\}$, and $g : B \mapsto C$, such that $g = \{\langle b_1, c_1 \rangle, \langle b_2, c_1 \rangle, \langle b_3, c_2 \rangle\}$. Thus the composed function $(g \circ f) : A \mapsto C$, is $g \circ f = \{\langle a_1, c_1 \rangle, \langle a_2, c_1 \rangle\}$.



Proofs on Properties of Composed Functions

We want to show that if $g \circ f$ is an injective function, then it follows that f is an injective function.

Take some arbitrary $a_1, a_2 \in A$. Assume that $f(a_1) = f(a_2)$ (otherwise it doesn't help, since falsity implies anything). Now, by the definition of a function, we can say that $g(f(a_1)) = g(f(a_2))$, which means that $(g \circ f)(a_1) = (g \circ f)(a_2)$. However, we're assuming that $g \circ f$ is injective, hence it follows that $a_1 = a_2$. By assuming that $f(a_1) = f(a_2)$, we get $a_1 = a_2$, hence we have proven f is injective.

We want to show that if $g \circ f$ is a surjective function, then it follows that g is a surjective function.

Our goal is to show that $\forall c \in C \exists b \in B [g(b) = c]$. Knowing that $\forall c \in C \exists a \in A [(g \circ f)(a) = c]$, it implies that there exists some $b \in B$, such that $f(a) = b$ (by definition of function composition). Hence, g is surjective.

We want to show that if we have bijections $f : A \mapsto B$, and $g : B \mapsto C$, then $g \circ f$ is a bijection. It is sufficient to show that if f, g are both surjective, then so is $g \circ f$, and if f, g are both injective, then so is $g \circ f$.

The first part can be proven by assuming that they are both surjective. Therefore, it means that $\forall c \in C \exists b \in B [g(b) = c]$, and also $\forall b \in B \exists a \in A [f(a) = b]$. So, suppose that there is an arbitrary $c \in C$, therefore there exists some $b \in B$, such that $g(b) = c$. Now, with that b , we can say that there exists such an $a \in A$ where $f(a) = b$. Therefore, it follows that $\forall c \in C \exists a \in A [(g \circ f)(a) = c]$. Hence, the composed function is surjective.

The second part can be proven similarly, assuming that both functions are injective. Let us take some arbitrary $a_1, a_2 \in A$. We assume that $(g \circ f)(a_1) = (g \circ f)(a_2)$, hence $g(f(a_1)) = g(f(a_2))$. But we know g is injective, therefore $f(a_1) = f(a_2)$, but since f is also injective, it follows that $a_1 = a_2$. Hence, by assuming that $(g \circ f)(a_1) = (g \circ f)(a_2)$, we end up with $a_1 = a_2$, it follows that $g \circ f$ is injective. By proving it's also a surjection, it is therefore a bijective function.

Identity, and Inverse

Suppose we have a set A , the identity function on A , denoted $\text{id}_A : A \mapsto A$, is defined by $\forall a \in A [\text{id}_A(a) = a]$. Let there be some arbitrary function $f : A \mapsto B$, then the inverse of the function, $g : B \mapsto A$ (normally written f^{-1}) has to fulfill the following criteria. $\forall a \in A [g(f(a)) = a] \wedge \forall b \in B [f(g(b)) = b]$. We can also write this, more succinctly, as $g \circ f = \text{id}_A \wedge f \circ g = \text{id}_B$.

Let there be a bijection $f : A \mapsto B$, and its inverse $f^{-1} : B \mapsto A$, defined as $f^{-1}(b) = a$, when $f(a) = b$. Take some arbitrary $b \in B$, we know that there must be a corresponding $a \in A$, since f is surjective. Therefore, we have shown that every item in the domain of f^{-1} maps to something (one of the criteria for a function). Knowing that f is also injective means that for arbitrary b , we have a single unique a that corresponds to it, therefore f^{-1} is a well defined function.

Suppose we have a function $f : A \mapsto B$, with a well defined inverse g . We can prove that f is a bijection, and g is unique. We want to first prove that it is a surjection; take an arbitrary $b \in B$; now we know that $f(g(b)) = b$, by definition of inverse, hence it is onto. Now to prove that f is injective, take arbitrary $a_1, a_2 \in A$. Assume that $f(a_1) = f(a_2)$, then it follows that $g(f(a_1)) = g(f(a_2))$. By

definition of inverse (with the identity), we can then say that $g(f(a_1)) = a_1 = a_2 = g(f(a_2))$, hence $a_1 = a_2$, thus f is injective, and since it is both injective, and surjective, it is a bijection.

Assume that there are two inverses of f ; g, g' . Taking an arbitrary $b \in B$, we can say that $f(g(b)) = b$, and also $f(g'(b)) = b$, once again by using the identity definition. Hence, it follows that $g = g'$, as f is injective.

Cardinality of Sets

Let us define equivalence on sets (not equality), for **any** (they can be infinite) sets A , and B ;
 $A \approx B \triangleq \exists f : A \mapsto B$ (where f is a bijection). Note that the previously mentioned (Dual) Cantor-Bernstein Theorem states that there is a bijection when there are two injective (or two surjective) functions $g : A \mapsto B$, and $h : B \mapsto A$.

We can also prove that it is an equivalence relation, such that it is reflexive, symmetric, and also transitive;

- \approx is reflexive, hence $A \approx A$
 we have the identity relation $\text{id}_A : A \mapsto A$, which is a bijection
- \approx is symmetric, hence if $A \approx B$, then $B \approx A$
 given that there is a bijection $f : A \mapsto B$, there exists an inverse $f^{-1} : B \mapsto A$, which is also a bijection (proven above)
- \approx is transitive, hence if $A \approx B$, and $B \approx C$, then $A \approx C$
 given that there exists two bijections, $f : A \mapsto B$, and $g : B \mapsto C$, the composition $(g \circ f) : A \mapsto C$ is also a bijection (proven above)

We can prove that $\mathbb{N} \approx \mathbb{N}^2$ by arranging the pairs in an infinite grid (remember that we're allowed infinite constructions, just not infinite step proofs). Each pair is visited once, and only once, therefore there exists a bijection.

