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. Johsonbaugh. *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;

- $\{a_1, ..., a_2\}$ — 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, $\varnothing \triangleq \{\}$. 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, an 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 $\varnothing$, the empty set, is a subset of every set. Using the second definition of subset, we can say that as $x \in \varnothing$ is false, by definition, and anything follows from falsity, whereas in the first definition we argue that all (0) elements of $\varnothing$ 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 follos 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 direcion; $y \in B \Rightarrow Q(y) \Rightarrow P(y) \Rightarrow y \in A$. 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
- $A \backslash B$ (or $A - B$) $\triangleq \{x \in A \mid x \notin B\}$ — set difference
- $A \triangle B \triangleq (A \backslash B) \cup (B \backslash A)$ — symmetric set difference))
- $A \cap B = \varnothing$ — 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 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 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 ($\lightning$), 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 arbitary $x \in (C \cap D)$. 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 $A = (A \backslash B) \cup (A \cap B)$. 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.

- $A \cup A = A$ — indempotence
- $A \cap A = A$ — indempotence
- $A \cup B = B \cup A$ — 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

- $A \cup \varnothing = A$ — empty set
- $A \cap \varnothing = \varnothing$ — empty set
- $A \triangle A = \varnothing$ — 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 indempotence 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;

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

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 $\wp\varnothing = \{\varnothing\}$, 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, $A = \{a_1, a_2, ...a_n\}$, can either be in the powerset or not. Therefore, we can represet 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 cartsian 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 $A = \{a_1, a_2, ..., a_n\}$, and $B = \{b_1, b_2, ..., b_m\}$, 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;

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

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

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

Partitions

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

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

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 $\forall i \in [1, k][|A_k| = 1]$). By definition of a partion, we can form a cover of S, therefore (the last 2 steps are justfied by the requirement of a partiion being pairwise disjoint);

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

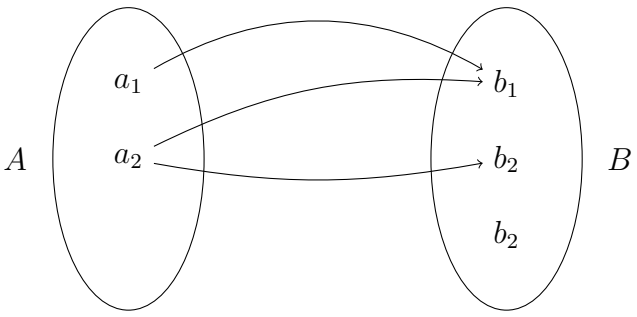
However, given the bounding condition $k < n$, there is no way that $k = n$, and the only assumption is that we made k sets of size 1.

Representing Relations

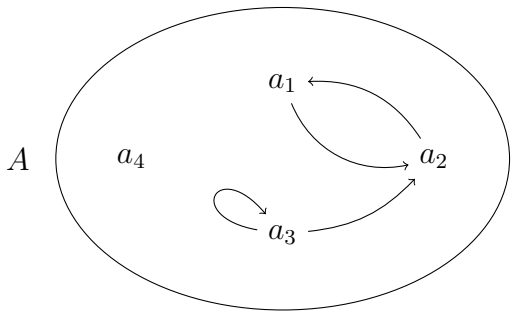
We define a relation between two sets A, and B (from A to B), as a subset of $A \times B$, such that $R \subseteq A \times B$. If we say that $R \subseteq A \times B$, it means that it has type $A \times B$. However, if $R \subseteq A^2$, it is a **binary** relation on A. Instead of writing $\langle a, b \rangle \in \mathbb{R}$, 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 $A = \{a_1, a_1\}$, $B = \{b_1, b_2, b_3\}$, 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 $T \subseteq B \times C$);

- $R \cup S \triangleq \{\langle a, b\rangle \in A \times B \mid \langle a, b\rangle \in A \vee \langle a, b\rangle \in B\}$ — relation union
- $R \cap S \triangleq \{\langle a, b\rangle \in A \times B \mid \langle a, b\rangle \in A \wedge \langle a, b\rangle \in B\}$ — relation intersection
- $\overline{R} \triangleq \{\langle a, b\rangle \in A \times B \mid \langle a, b\rangle \notin A\}$ — 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 grandparentof $\triangleq$ parentof $\circ$ parentof

  therefore x 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 therfore $\langle y, x\rangle \in S^{-1}$. 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 $\triangleq \forall x \in A[\langle x, x\rangle \in R]$
  $\Leftrightarrow \mathrm{id}_A \subseteq R$
- R is symmetric $\triangleq \forall x, y \in A[\langle x, y\rangle \in A \Rightarrow \langle y, x\rangle \in R]$
  $\Leftrightarrow R = R^{-1}$
- 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

Equivlence 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 equivalnce 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 partiion 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 equivalnce 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 equivalnce classes aren't pairwise disjoint, such that $[x] \cap [y] \neq \varnothing$. 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 partion of A.