Z. Abel, B. Chapman, E. Demaine
revised Wednesday 24th January, 2024

# Lecture 15: Relations and Counting

Fair warning: lots of terms and definitions today. I'm sorry.

## 1 Relations

**Definition 1.** *A **relation** $R \subseteq A \times B$ consists of*

- *a **domain** $A$ (can be any set),*
- *a **codomain** $B$ (can be any set),*
- *and a subset $R \subseteq A \times B$ of ordered pairs*

Generalizes idea of a function from $A$ to $B$. Some stereotypical examples:

Reveal diagrams:

Students: $\{Luke, Geralt, Quentin, Willow\}$. Classes: $\{Chem, Sports, Lit, 6.1200\}$. Professors: $\{Galadriel, Zelda, Eda, Strange\}$.

Students learning in classes: $L \subseteq S \times C$,

$$L = \{(Lu, C), (Lu, Lit), (Ge, C), (Ge, S), (G, Lit), (Q, S), (Q, Lit), (W, Lit)\}.$$

Classes taught by professors: $T \subseteq C \times P$, $T = \{(C, E), (Sp, St), (Lit, Ga), (6, Z)\}$.

For notation, we often write $a\,R\,b$ to mean that $(a, b) \in R$, to mimic other infix relations like $a \in X$, $p = q$, $s \leq t$, etc. Can also think of $R$ as a predicate, and write $R(a, b)$ to mean $(a, b) \in R$. When $(a, b) \in R$, we'll say that $a$ ***relates to*** $b$ in $R$, but be careful because direction matters. That's why we're drawing $(a, b) \in R$ as a directed arrow from $a \in A$ to $b \in B$.

By the way, ***binary relation*** is the same "relation" as in ***relational databases***! It's just pairs of data. Some pairs are present, some aren't. (Relational databases might have more than 2 columns, but we're focused only on binary relations today.)

Functions are an important example:

**Definition 2.** *A relation $R \subseteq A \times B$ is a **function** iff every $a \in A$ relates to at most one $b \in B$. In this case we write $R : A \to B$. "$\leq 1$ arrow out" of each $a \in A$.*

When $R$ is a function, we can write $R(a)$ for that unique element $b$ it relates to, if there is one.

Example: $T$ but not $L$.

Example: $f : \mathbb{R} \to \mathbb{R}$ where $f(x) = 1/x^2$. How does this relate to initial definition? $f \subseteq R \times R$ is really a set of pairs:

$$f = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y = 1/x^2\} = \{(x, 1/x^2) \mid x \in \mathbb{R} \setminus \{0\}\}.$$

There are infinitely many pairs, but that's fine! Note that $f(0)$ is not defined, but that's also fine! Don't need all inputs to have outputs, as long as no input has multiple outputs.

**Definition 3.** *A relation $R \subseteq A \times B$ is* ***total*** *if every $a \in A$ relates to* at least *one element $b \in B$: "$\geq 1$ arrows out" of each $a \in A$.*

Often go together: a ***total function*** $f$ has *exactly one arrow* out of each $a \in A$. So $f(a)$ definitely exists for all inputs, with no ambiguity.

Example: $f(x) = 1/x^2$ is not total as a function $\mathbb{R} \to \mathbb{R}$, but it *is* total if we consider it as $f : A \to A$, where $A = \mathbb{R}^{\neq 0}$. Observe that these have exactly the same set of $(x, y)$ pairs! Need to know what the domain and codomain are before we can answer these properties.

Similar terms for arrows *in*:

**Definition 4.** *A relation $R \subseteq A \times B$ is* ***injective*** *iff every $b \in B$ has* at most 1 *element $a$ satisfying $a\,R\,b$. "$\leq 1$ arrow in" to every $b \in B$.*

*$R$ is* ***surjective*** *iff every $b \in B$ has* at least 1 *element $a$ satisfying $a\,R\,b$. "$\geq 1$ arrow in" to every $b \in B$.*

These properties are useful for comparing the sizes of sets:

**Theorem 1.** *If $A$ and $B$ are finite sets, and $R \subseteq A \times B$ is a total injection, then $|A| \leq |B|$.*

Every $a \in A$ has at least one arrow coming out, and every $B$ has at most one arrow coming in, so $|A| \leq \#$ edges $\leq |B|$. Similarly:

**Theorem 2.** *If $A$ and $B$ are finite sets, and $R \subseteq A \times B$ is a surjective function, then $|A| \geq |B|$.*

By our powers combined,

**Definition 5.** *A* ***total function*** *that is both* ***injective*** *and* ***surjective*** *is known as a* ***bijection****.*

**Theorem 3.** *If $A$ and $B$ are finite sets, and $R \subseteq A \times B$ is a bijection, then $|A| = |B|$.*

We'll get a lot of mileage out of that in a bit.

# 2 Relations on a Single Set

We never said $A$ and $B$ have to be disjoint, or even distinct! Many useful examples come from the case where $A = B$. A relation $R \subseteq A \times A$ is known as a binary relation ***on*** $A$.

Now, the defn is literally identical to the defn of directed graph. $a\,R\,b$ means the graph has directed edge $(a, b)$. So all of our digraph examples apply. Another exaple I like is the digraph of who likes whom—not necessarily romantically, just as a person. Lots of fun chaotic structure. E.g., not symmetric: if I like you, you don't necessarily like me (especially when there's a tough pset!). Sometimes I don't even like myself, so my note wouldn't have a self-loop that day! Not in a cry-for-help kind of way, but occasionally we can be a little down on ourselves, and that's ok! (If it happens too often, though, please seek help and support.)

Funny story, I gave this same example a few years ago, and then someone posted it without context on MIT Confessions! Over the next few days I had Facebook friends messaging me, "Zach are you ok? We haven't caught up in a while, but I'm here to listen, and I'd love to catch up!". I felt very loved :)

Anyway, back to relations. There are many familiar examples that we don't necessarily think of as graphs: $a = b$, $a \equiv b \bmod 10$, $a \leq b$, $A \subseteq B$, $a \mid b$.

If $G$ is a digraph, we looked at its ***walk relation*** aka ***reachability relation*** $G^*$, where $a\ G^*\ b$ iff there exists a walk from $a$ to $b$. Also the strong connectivity relation $S$, where $a\ S\ b$ iff $a\ G^*\ b$ AND $b\ G^*\ a$. Careful: we can think of these relations as digraphs in their own right, and these relations-as-graphs are in general *different* from the graph $G$ they're defined from.

Let's look at two common, useful kinds:

## 2.1 Equivalence Relations

Want to capture what it means to *behave like* "=", to represent "sameness" or "equivalence". We've seen multiple examples: $a \equiv b \bmod 10$ means they have the *same remainder*. $a$ is connected to $b$ in a simple graph means $a$ and $b$ belong to the same *connected component*.

Turns out, this is captured by three properties:

**Definition 6.** *Let $R \subseteq A \times A$ be a relation on $A$.*

*$R$ is **reflexive** means $a\,R\,a$ for all $a \in A$. "Everything is equivalent to itself."*

*$R$ is **symmetric** means $a\,R\,b$ IFF $b\,R\,a$ for all $a, b \in A$. "Order doesn't matter."*

*$R$ is **transitive** means $a\,R\,b$ AND $b\,R\,c$ IMPLIES $a\,R\,c$ for all $a, b, c \in A$. "If $a$ and $b$ are equivalent, and $b$ and $c$ are equivalent, then $a$ and $c$ are equivalent."*

*$R$ is a **equivalence relation** means that $R$ is reflexive, symmetric, and transitive.*

**Theorem 4.** *If $R$ is an equivalence relation on $A$, then $R$ partitions $A$ into subsets called **equivalence classes**, where each $a \in A$ belongs to exactly one equivalence class, and $a\,R\,b$ is true precisely when $a$ and $b$ belong to the same equivalence class.*

Skipping the proof, but the result is important. Just these three rules are enough!

## 2.2 Weak Partial Orders

Want to capture what it means to *behave like* "$\leq$", to represent "ordering". We know multiple other examples: $A \subseteq B$, $a \mid b$, "$a$ is a prerequisite for $b$" ie reachability in a DAG.

Two properties are the same: reflexive and transitive. $a \leq a$ is true, and $a \leq b$ AND $b \leq c$ IMPLIES $a \leq c$ are both true, so we want to keep these. Only symmetry needs changing:

**Definition 7.** *Let $R \subseteq A \times A$ be a relation on $A$.*

*$R$ is **antisymmetric** means that for all $a, b \in A$, if $a\,R\,b$ and $b\,R\,a$ are both true, then $a = b$. "can't be both greater and less, unless you're exactly the same."*

*$R$ is a **weak partial order** means that $R$ is reflexive, **anti**symmetric, and transitive.*

**Theorem 5.** *If $G$ is a digraph, then the walk relation on $G$ is a WPO iff $G$ is a DAG.*

Notice that these examples are a bit more permissive: they don't require that *every* pair of items be ordered, e.g., Left-Sock and Right-Sock can go in either order. But the ones that do have definite orderings, need to behave like we would expect. If we need *every* pair to have a definite ordering, we get:

**Definition 8.** *For a WPO $R \subset A \times A$, two elements $a, b$ are called **comparable** when $a\,R\,b$ or $b\,R\,a$.*

*A WPO is called a **linear ordering** aka **total ordering** if every pair of elements are comparable. (This is just putting all items in order left to right.)*

$a \leq b$ is a total ordering, but $a \mid b$ and $A \subseteq B$ are not.

# 3 Counting

Counting! Not 1,2,3,..., but as in finding the size of sets. How many shuffled decks of cards are there? Answer: 52!. How many trees are there with nodes $\{1, 2, \ldots, n\}$? Surprising answer: $n^{n-2}$.

Useful when analyzing algorithms; can often use counting techniques to prove runtime bounds. Useful for probability, coming after Quiz 2.

## 3.1 Parable of the Two Shepherds

First shepherd doesn't know how to count. Lets sheep out of their pen every morning, returns them every evening. How do they know all the sheep came back? Put a pebble in pocket every time you let one out. Remove a pebble every time you let one in. Sets up a ***bijection*** between sheep and pebbles, and that guarantees there are the same number of each. This is the key takeaway: we'll usually be counting with ***bijections***.

Second shepherd knows how to count, but has an overeager apprentice. Apprentice says "Master, I got all 40 sheep back in their pen!". Master looks confused: "But my young apprentice, we only have 37 sheep!" Apprentice: "That's OK, I rounded them up." What's the moral? Nothing, I just liked the pun.

## 3.2 Product Rule

For finite sets $A, B$, we have $|A \times B| = |A| \cdot |B|$. Works more generally:

$$|A_1 \times \cdots \times A_n| = |A_1| \cdot \cdots \cdot |A_n|.$$

Example: The number of binary sequences of length $n$ is $2^n$. This set is exactly $B_n := \{0,1\} \times \cdots \times \{0,1\} = \{0,1\}^n$ (new notation!), so its size is $2 \cdot \cdots \cdot 2 = 2^n$.

## 3.3 Bijection Rule

If there is a bijection between $A$ and $B$, then $|A| = |B|$.

Example: the number of subsets of $\{1, 2, \ldots, n\}$ is $2^n$.

$P_n := \{A \mid A \subseteq \{1, 2, \ldots, n\}\}$. We can give a bijection from $P_n$ to $B_n$: $A \in P_n$ maps to the $n$-bit string where the $i$th bit is 1 if $i \in A$, and 0 if $i \notin A$. E.g., $\{1, 2, 5\}$ maps to $11001000 \cdots 0$.

Can verify that this is a bijection, so $|P_n| = |B_n| = 2^n$.

## 3.4 Sum Rule

Sum rule: if $A_1, \ldots, A_n$ are **pairwise disjoint** finite sets, then

$$|A_1 \cup \cdots \cup A_n| = |A_1| + \cdots + |A_n|.$$

Example: how many passwords have length between 6 and 8, start with a capital letter, and the rest of the characters are capital letters, lowercase letters, or digits?

$W$ is the disjoint union of $W_6$, $W_7$, and $W_8$, where $W_k$ counts the number of passwords with length $k$ satisfying these constraints. By the product rule, $W_k = 26 \cdot 62^{k-1}$. So $|W| = |W_6| + |W_7| + |W_8| = 26 \cdot 62^5 + 26 \cdot 62^6 + 26 \cdot 62^7 \approx 5.7$quadrillion.

For both Sum rule and Product rule, we're usually making multiple kinds of choices. If it's the OR of those choices, use sum rule. If it's the AND of those choices, use product rule. If we have 10 shirts and 6 pants, we have 16 articles of clothing because we can choose a shirt OR a pair of pants. But we have 60 outfits, because we have to choose a shirt AND a pair of pants.

## 3.5 Generalized Product Rule

Example first: How many orderings are possible for a shuffled deck of cards? 52 distinct cards in total.

We have 52 choices for the first card. Now that that's selected, we have 51 choices for the second card. Then 50, then 49, and so on. The answer is $52 \cdot 51 \cdot 50 \cdots 1 = 52! \approx 8 \cdot 10^{67}$.

This wasn't the product rule: the set of choices for the second card *changes* depending on what was chosen for the first card! What's important is that the *number* of choices is consistent, no matter what choices were made earlier.

In general, if $A$ is a set of length $k$ sequences $(a_1, \ldots, a_k)$ where there are $n_1$ choices for $a_1$, there are $n_2$ choices for $a_2$ *no matter what value was chosen for* $a_1$, there are $n_3$ choices for $a_3$ *no matter what values were chosen for* $a_1$ *and* $a_2$, and so on up to $n_k$ choices for $a_k$ *no matter what values were picked for* $a_1, \ldots, a_{k-1}$, then $|A| = n_1 \cdot n_2 \cdots n_k$.

One more example: US one dollar bills have an 8 digit serial number, and they frequently have repeated digits! Who has a dollar bill with them? Is some digit used more than once? The number of serial numbers **without** repeated digits is $10 \cdot 9 \cdot 8 \cdots 4 \cdot 3$ by the generalized product rule. Total number of serials is $10^8$ by the standard product rule. Fraction that avoids repeats is $\approx .018$, or 1.8%.

We'll get tons more practice with these ideas next week.