From last time

Prove that √2 is irrational by giving a proof by contradiction.

(Hint: if a number is rational, it can be represented by a/b where a and b are integers and have no common terms).

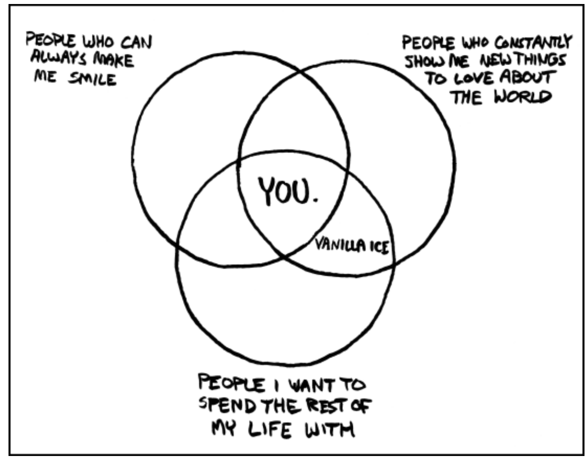


Figure 1: Comic from XKCD

Sets (sections 2.1 and 2.2)

Everyone knows what a set is, right?

- A **set** is an unordered collection of objects.
- Two sets are **equal** if they contain the same elements.
  - {P, Q, 7} = {Q, 7, P} = {7, 7, P, Q, Q, P}

What we are going to need to do now is walk through a *massive* number of definitions. Hold on tight.

Specification

- We can specify a set by **enumeration**:
  - e.g. { 3, 4, 8 }
- Can specify a set by a **rule**:
  - **S** = { $s \in$ Students | s is taking EECS 203}.

Size

- A set can be finite or infinite.
  - The **cardinality** |S| of a finite set S is the number of distinct elements in S.

Sets with special names

- There are a number of sets with special names. A list of the more common ones is on the right.

- $\phi = \{\ \}$ — the empty set
- $\mathbf{N} = \mathbb{N} = \{0,1,2,3, \dots\}$ — natural numbers
- $\mathbf{Z}^+ = \mathbb{Z}^+ = \{1,2,3,4, \dots\}$ — positive integers
- $\mathbf{Z} = \mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ — integers
- $\mathbf{Q} = \mathbb{Q} = \{p/q \mid p, q \in \mathbb{Z} \text{ and } q \neq 0\}$ — rationals
- $\mathbf{R} = \mathbb{R}$ — the set of real numbers
- $\mathbf{R}^+ = \mathbb{R}^+$ — the set of positive real numbers
- $\mathbf{C} = \mathbb{C}$ — the set of complex numbers

Sets can contain anything. Including sets.

- { {1, 3, 5, 7, 9}, {2, 4, 6, 8, 10} } is a set.
  - What is the cardinality of that set? __________
- Just to be annoying, let's consider this set: S = $\{\phi, \{\phi\}, \{\phi,\{\phi\}\}, \{\phi,\{\phi\},\{\phi,\{\phi\}\}\}\}$
  - What is |S|? __________

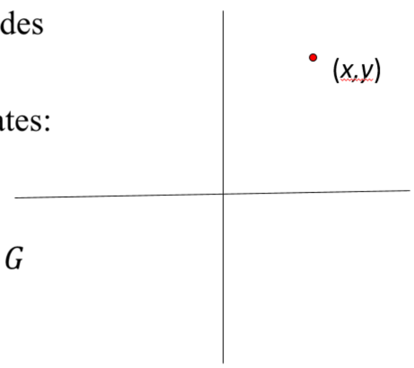
Set relations and other terms and notation

We've already defined equality. What else is there?

- **Element** of
  - x ∈ A means that x is an element of A.
  - If S={ {1, 3, 5, 7, 9}, {2, 4, 6, 8, 10} }, is 2 ∈ S? ___________

- **Subset**
  - A $\subseteq$ B means that every element of A is also in B.
    - Write that as a proposition: $\forall$x (x $\in$ A __________________)
- **Superset**
  - A $\supseteq$ B means that every element of B is also in A.
- **Proper subset/superset**
  - A $\subset$ B means that A is a subset of B and A≠B.
    - Very similar to the way > and ≥ work with numbers…
- **Power Set**
  - This one is weird. The power set of the set S, P(S), is all the subsets of S including the empty set.
    - P(S) = { A | A $\subseteq$ S }
  - What is the cardinality of P({1,2})? _______________
  - What is the cardinality of P({1,2,3})? _______________
- **Cartesian Product of Sets**
  - Another odd one. This is basically a set that contains all pairs from both sets.
  - This idea shows up in a lot places, including databases (all pair of two lists…)
  - That last line is there to make it clear that I can take the Cartesian product of many sets.

- $A \times B = \{(x, y) | x \in A, y \in B\}$
  - uniqnames $\times$ Grades
  - Cartesian coordinates:
    - $(x,y) \in \mathrm{R}^2$
  - $A \times B \times C \times \cdots \times G$



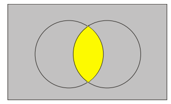
    - If A={1,2} and B={a,b}, what is A × B? _____________________________________

Random questions…

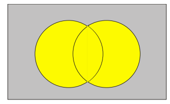
1. Is it ***always / sometimes / never*** the case that S $\in$ P(S)?
2. If A $\supseteq$ B and B $\subset$ A, does A=B?
3. Suppose that A × B = ∅, where A and B are sets. What can you conclude?
4. Translate each of these quantifications into English and determine its truth value.
   a. $\exists x \in$ R $(x^3 = -1)$
   b. $\forall x \in$ N $(x - 1 \in$ N$)$
   c. $\forall x \in$ N $(x + 1 \in$ N$)$

Set Operations

- **Intersection**
  - $A \cap B = \{x \mid x \in A \wedge x \in B\}$



- **Union**
  - $A \cup B = \{x \mid x \in A \vee x \in B\}$



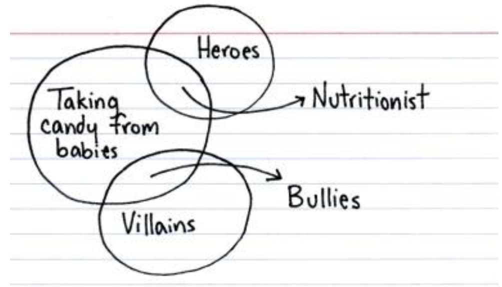
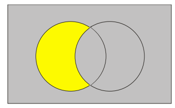
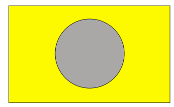


Figure 2:Comic from indexed

- **Difference**
  - $A - B = \{x \mid x \in A \wedge x \notin B\}$

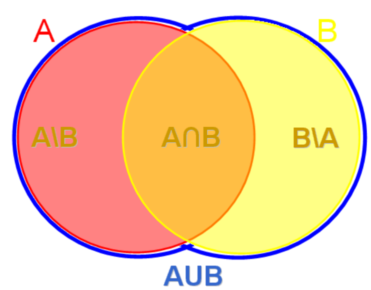


- **Complement**
  - $\bar{A} = \{x \in U \mid x \notin A\}$
  - Note that complement must be defined wrt some Universe.



Set Identities

- **Identity** laws
  $A \cap U = A$
  $A \cup \emptyset = A$
- **Domination** laws
  $A \cup U = U$
  $A \cap \emptyset = \emptyset$
- **Idempotent** laws
  $A \cup A = A$
  $A \cap A = A$
- **Complementation** law
  $\overline{(\overline{A})} = A$
- **Commutative** laws
  $A \cup B = B \cup A$
  $A \cap B = B \cap A$
- **Associative** laws
  $A \cup (B \cup C) = (A \cup B) \cup C$
  $A \cap (B \cap C) = (A \cap B) \cap C$
- **Distributive** laws
  $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
  $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
- **De Morgan's** laws
  $\overline{A \cup B} = \overline{A} \cap \overline{B}$
  $\overline{A \cap B} = \overline{A} \cup \overline{B}$
- **Absorption** laws
  $A \cap (A \cup B) = A$
  $A \cup (A \cap B) = A$
- **Complement** laws
  $A \cup \overline{A} = U$
  $A \cap \overline{A} = \emptyset$



An instructive question

- Let $U = \{ x \in \mathbf{Z} \mid 1 \le x \le 30 \}$
- Let $S_n = \{x \in U \mid x = kn \text{ for some } k \in \mathbb{Z}\}$

- What is $|S_2|$? What is $|S_3|$?
- What is the value of $|S_2 \cup S_3|$?

- The basic principle:

$$|S_2 \cup S_3| = |S_2| + |S_3| - |S_2 \cap S_3|$$
$$|S_2| = 15$$
$$|S_3| = 10$$
$$|S_2 \cap S_3| = |S_6| = 5$$
$$|S_2 \cup S_3| = 15 + 10 - 5 = 20$$

Let's say we have three sets X_1, X_2, and X_3 where $|X_n|=c_n$. One thing we might want to know is the value of $|X_1 \cap X_2 \cap X_3|$ Clearly we don't have enough information, but what can we say about the range of possibilities for $|X_1 \cap X_2 \cap X_3|$?

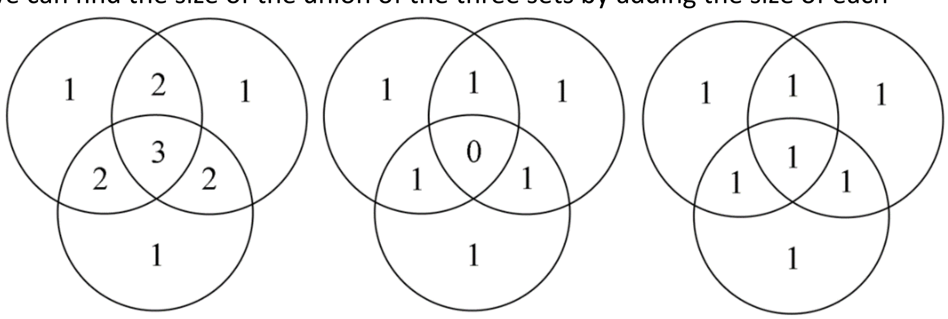
Let's consider a somewhat more specific case. If we know $|X_1| = 4, |X_2| = 8, |X_3| = 5$, what is the largest $|X_1 \cap X_2 \cap X_3|$ could be? The smallest? What if we know that $|X_1 \cap X_2| = 1$, $|X_1 \cap X_3| = 2$, and $|X_2 \cap X_3| = 4$? Do you know the exact value of $|X_1 \cap X_2 \cap X_3|$? If not, what range could it hold? What other information would you need?

Figure 3: Comic from smbc

Let's be a bit more formal now.

Inclusion-Exclusion principle[1]

The basic idea here is that we can find the size of the union of the three sets by adding the size of each set, subtracting the intersection of each pair and re-adding the intersection of all three sets.



$|A| + |B| + |C|$

$|A| + |B| + |C|$
$-(|A \cap B| + |A \cap C| + |B \cap C|)$

$|A| + |B| + |C|$
$-(|A \cap B| + |A \cap C| + |B \cap C|)$
$+|A \cap B \cap C|$

[1] Figure and formula in this section from https://en.wikipedia.org/wiki/Inclusion%E2%80%93exclusion_principle.

Inclusion/Exclusion sample question #1

Now let's go back to the following collection of sets:

- Let $U = \{ x \in \mathbf{Z} \mid 1 \leq x \leq 30 \}$
- Let $S_n = \{x \in U \mid x = kn \text{ for some } k \in \mathbb{Z}\}$

What is the value of $S_2 \cup S_3 \cup S_5$?

Inclusion/Exclusion sample question #2

Describe the equation for finding the cardinality of all the union of four sets assuming you know the cardinality of any arbitrary intersections of those four sets.

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{i=1}^{n} |A_i| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j| + \sum_{1 \leq i < j < k \leq n} |A_i \cap A_j \cap A_k| - \ldots + (-1)^{n-1} |A_1 \cap \cdots \cap A_n| .$$

Can you parse the above formula?

Proofs with sets

Let's look at a proof involving sets. In particular, let's look at a proof of one of the distributive set laws. The key observation is that we can create a predicate which describes some element x that is an element of the set in question (though it does make us ask the question, what if there is no such element…)

- Consider: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
- Proof:

$A \cap (B \cup C)$

$= \{x : x \in A \cap (B \cup C)\}$ (definition of set)

$= \{x : (x \in A) \wedge (x \in (B \cup C))\}$ (defn. of intersection)

$= \{x : (x \in A) \wedge [(x \in B) \vee (x \in C)]\}$ (defn. of union)

$= \{x : [(x \in A) \wedge (x \in B)] \vee [(x \in A) \wedge (x \in C)]\}$ (distributive law for $\wedge$ over $\vee$)

$= \{x : (x \in A \cap B) \vee (x \in A \cap C)\}$ (defn. of intersection)

$= \{x : x \in (A \cap B) \cup (A \cap C)\}$ (defn. of union)

$= (A \cap B) \cup (A \cap C)$ (defn of set)

Doing that, we can jump back to predicate logic and just use the distributive law for predicate logic.

Sometimes that isn't a viable way forward.
Another, common way to prove A=B is to show that $A \subseteq B$ *and* $A \supseteq B$.

Using bit vectors to represent a set in a computer

Consider a case where the universal set U is finite and reasonably small. That is to say, we will only be considering sets which are subsets of U. In that case, we often find it helpful to represent sets as a series of bits. This can make set operations fairly trivial on a computer.

First, we specify an arbitrary ordering of the elements of U, for instance $a_1, a_2, \ldots, a_n$. We represent a subset A of U with a bit string of length n, where the ith bit in this string is 1 if a_i belongs to A and is 0 if a_i does not belong to A.

Consider the case where U={1, 2, 3, 4, 5, 6}. Say our "arbitrary" ordering of elements was in increasing order. We might use the bit string 100011 to represent the set {1, 5, 6}. How would we represent the set {2,3}?

This representation is really helpful because computers can quickly do "bitwise" logical operations on strings of bits. What would be the set operation performed by

- a bitwise OR?
- a bitwise AND?
- a bitwise NOT?

Example questions

If U={1, 2, 3, 4, 5, 6} and using the same ordering as above, provide bit-representations for the following:

- A={1, 3, 5}
- B={2, 3, 6}
- $A \cup B$
- $A \cap B$
- $\overline{A}$

Start on Functions (section 2.3)

As has been traditional in this class, we will start by defining a bunch of terms related to functions and then start using them.

- What is a function?
- A **mapping**
  - from **domain** A to **codomain** B $\quad f: A \to B$
  - y is the **image** of x $\quad f(x) = y$
  - x is the **pre-image** of y $\quad x \in A, y \in B$
  - the **range** is the image of the domain
    $f(A) = \{y \in B | y = f(x) \land x \in A\}$
- For every $x \in A$, there is a single value $f(x) \in B$.

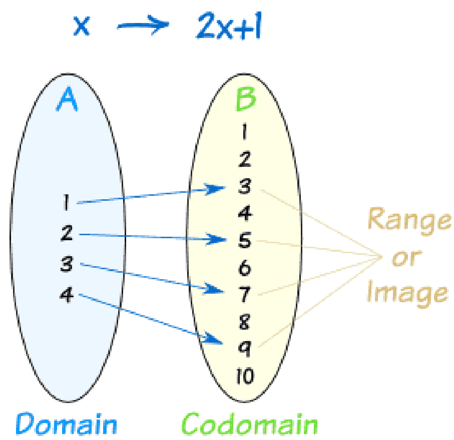


Figure 4: From http://www.mathsisfun.com

In figure 4, we are considering a function f(x)=2x+1 over the domain {1,2,3,4} and mapping to the codomain {1, 2, 3, 4, 5, 6, 7, 8, 9, 10}. The range, or image, is {3, 5, 7, 9}.

Questions

1. With domain and codomain of ***R***, say we define f such that f(x)=y iff $x=y^2$. Is f a function? Why or why not? If so, what is its range?

2. With domain and codomain of ***R***, say we define f such that $f(x)=1/x^2$. Is f a function? Why or why not? If so, what is its range?

3. With domain and codomain of ***R***, say we define f such that f(x)=y iff $y = \lceil x \rceil$. Is f a function? Why or why not? If so, what is its range?

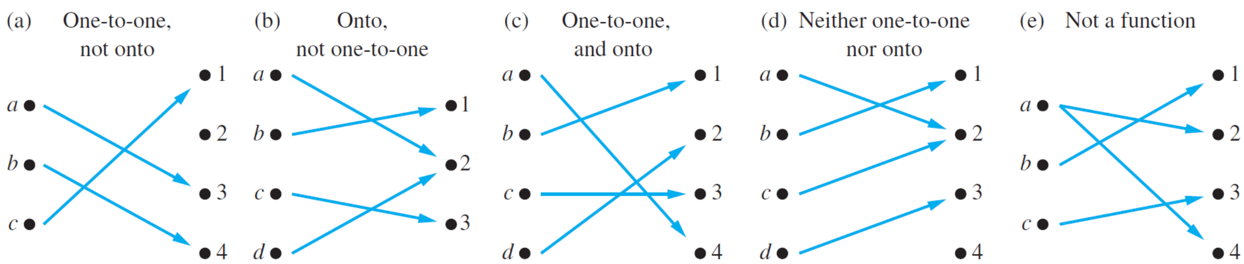
One-to-one and Onto

Obviously different functions have different properties. But there are two properties held by some functions that can be very useful.

- Given a function $f: A \rightarrow B$
- f is **one-to-one** (or "**injective**") iff
  $\forall a, b \in A\,[(f(b) = f(a)) \rightarrow (b = a)]$
- f is **onto** (or "**surjective**") iff
  $\forall b \in B, \exists a \in A\,[f(a) = b]$

- A function which never assigns the same value to two different domain elements is called "***one-to-one***".
- A function which has a range that is equal to its codomain is called "***onto***"

Below are some examples (from page 144 of the text) illustrating the one-to-one and onto properties.



Questions:

1. With domain and codomain of ***R***, say we define f such that f(x)=y iff $y = \lceil x \rceil$. Is f one-to-one? Onto?[2]

2. With domain and codomain of ***R***, say we define f such that f(x)=x^3. Is f one-to-one? Onto?

3. With domain and codomain of ***R***, say we define f such that f(x)=x^2. Is f one-to-one? Onto?

[2] This is the ceiling function and it is defined to be the next largest integer (basically rounding up).